# Understanding
# Vectra AI

Updated for Software Version 6.16
March 2022

VECTRA®

# Table of Contents


**The Vectra Kill Chain** 4
**Vectra Scoring** 5
**Detect for Network** 7
**Command & Control** 8
External Remote Access 9
Hidden DNS Tunnel 10
Hidden HTTP Tunnel 11
Hidden HTTPS Tunnel 12
Malware Update 13
Multi-home Fronted Tunnel 14
Peer-To-Peer 15
Stealth HTTP Post 16
Suspect Domain Activity 17
Suspicious HTTP 18
Suspicious Relay 20
TOR Activity 21
Threat Intelligence Match 22
Vectra Threat Intelligence Match 23
**Botnet Activity** 24
Brute-Force 25
Cryptocurrency Mining 26
Outbound DoS 27
Outbound Port Sweep 28
**Reconnaissance** 29
File Share Enumeration 30
Internal Darknet Scan 31
Kerberos Account Scan 32
Kerberos Brute-Sweep 33
RDP Recon 34
RPC Recon 35
RPC Targeted Recon 36
SMB Account Scan 37
Suspicious LDAP Query 38
Suspicious Port Scan 39
Suspicious Port Sweep 40
**Lateral Movement** 42
Automated Replication 43
Brute-Force 44
Privilege Anomaly: Unusual Account on Host 45
Privilege Anomaly: Unusual Host 47
Privilege Anomaly: Unusual Service 49
Privilege Anomaly: Unusual Service - Insider 51
Privilege Anomaly: Unusual Service from Host 53
Privilege Anomaly: Unusual Trio 55
Ransomware File Activity 57
SMB Brute-Force 58
Shell Knocker Client 59
Shell Knocker Server 61
SQL Injection Activity 63
Stage Loader 64
Suspicious Admin 65
Suspicious Remote Desktop 67
Suspicious Remote Execution 69
Threat Intelligence Match 71
**Exfiltration** 73
Data Gathering 74
Data Smuggler 75
Hidden DNS Tunnel 76
Hidden HTTP Tunnel 77
Hidden HTTPS Tunnel 78
Smash and Grab 79
Threat Intelligence Match 80

**Info** 81
**Network Detection Profiles** 83
Botnet 84
Cloud Services 85
External Adversary 86
Insider Threat: Admin 87
Insider Threat: User 88
IT Discovery 89
IT Services 90
Potentially Unwanted Program 91
Ransomware 92
Vulnerability Discovery 93
Worm 94
**Observed Privilege Scores** 95
**Detect for Azure AD and M365** 98
**Command & Control** 99
Azure AD Admin Account Creation 100
Azure AD MFA-Failed Suspicious Sign-On 101
Azure AD Redundant Access Creation 102
Azure AD Suspicious OAuth Application 103
Azure AD Suspicious Sign-on 104
Azure AD Suspected Compromised Access 105
Azure AD TOR Activity 106
O365 Power Automate HTTP Flow Creation 107
O365 Suspicious Power Automate Flow Creation 108
**Reconnaissance** 109
O365 Suspicious Compliance Search 110
O365 Unusual eDiscovery Search 111
O365 Suspect eDiscovery Usage 112
**Lateral Movement** 113
Azure AD Successful Brute-Force 114
O365 Suspicious Mailbox Manipulation 115
O365 Suspicious Mailbox Rule Creation 116
O365 Attacker Tool: Ruler 117
Azure AD Change to Trusted IP Configuration 118
O365 Disabling of Security Tools 119
O365 DLL Hijacking Activity 120
O365 External Teams Access 121
O365 Internal Spearphishing 122
O365 Log Disabling Attempt 123
O365 Malware Stage: Upload 124
Azure AD MFA Disabled 125
Azure AD Newly Created Admin Account 126
O365 Ransomware 127
O365 Risky Exchange Operation 128
Azure AD Privilege Operation Anomaly 129
O365 Suspicious SharePoint Operation 130
O365 Suspicious Teams Application 131
Azure AD Unusual Scripting Engine Usage 132
**Exfiltration** 133
O365 eDiscovery Exfil 134
O365 Exfiltration Before Termination 135
O365 Suspicious Download Activity 136
O365 Suspicious Exchange Transport Rule 137
O365 Suspicious Mail Forwarding 138
O365 Suspect Power Automate Activity 139
O365 Suspicious Sharing Activity 140

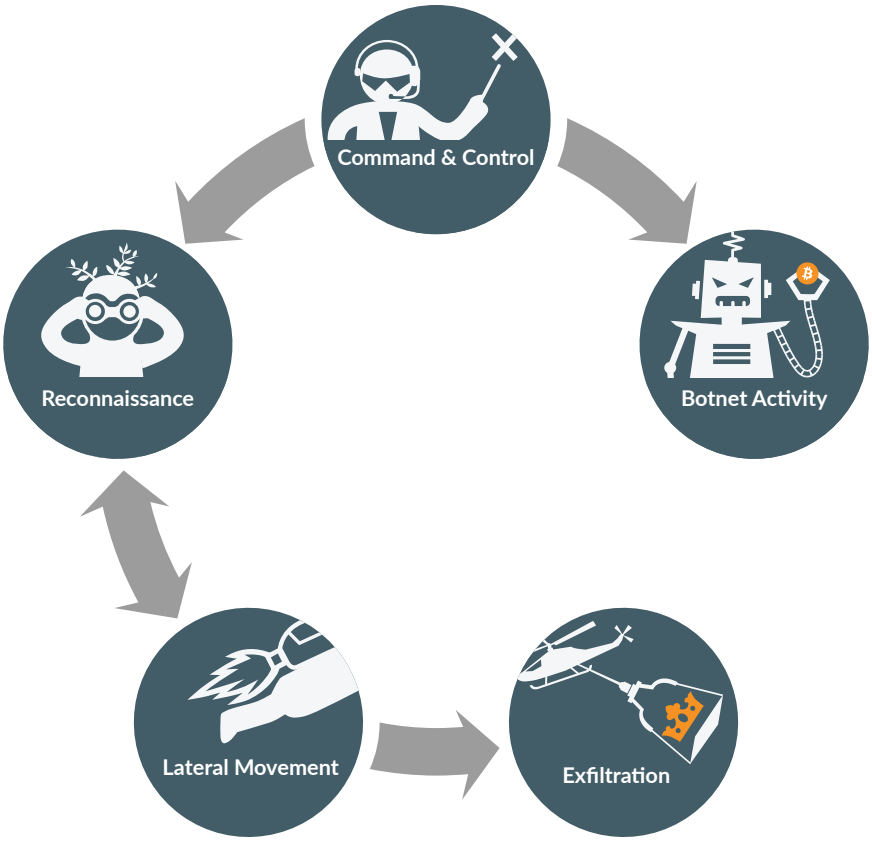
Info 141
Detect for AWS 143
Kingpin Technology 144
Command & Control 146
AWS Root Credential Usage 147
AWS Suspicious Credential Usage 148
AWS TOR Activity 149
Reconnaissance 150
AWS EC2 Enumeration 151
AWS Organization Discovery 152
AWS S3 Enumeration 153
AWS Suspect Credential Access from EC2 154
AWS Suspect Credential Access from ECS 155
AWS Suspect Credential Access from SSM 156
AWS Suspect Escalation Reconnaissance 157
AWS User Permissions Enumeration 158
Lateral Movement 159
AWS ECR Hijacking 160
AWS Lambda Hijacking 161
AWS Logging Disabled 162
AWS Ransomware S3 Activity 163
AWS Security Tools Disabled 164
AWS Suspect Admin Privilege Granting 165
AWS Suspect Console Pivot 166
AWS Suspect Login Profile Manipulation 167
AWS Suspect Privilege Escalation 168
AWS User Hijacking 169
Exfiltration 170
AWS Suspect External Access Granting 171
AWS Suspect Public EBS Change 172
AWS Suspect Public EC2 Change 173
AWS Suspect Public S3 Change 174
Botnet 175
AWS Cryptomining 176
Attack Campaigns 177

# The Vectra Kill Chain

After an initial exploit, the malware will contact its Command & Control server from which it will be remotely controlled in an automated fashion or by a human.

The attack usually progresses along the opportunistic path – the malware joins the host to a botnet and the bot herder steals information from the infected host and makes use of your resources to make money by attacking other systems across the Internet (Botnet Activity).

The attack may also have you as its intended target, something that is rarer, but also more threatening – in this case, the infected host will orient itself in your network (Reconnaissance), spread laterally to get closer to your crown jewels (Lateral Movement) and steal your data and send it to an outside system (Exfiltration).




- Top -

# Vectra Scoring


- Top -

## Vectra Scoring

Vectra's AI correlates threat behaviors to a host or account and prioritizes them into one of four severity rankings: Critical, High, Medium, and Low. This ranking is based on Vectra's scoring model's understanding of how aligned the collective attacker behaviors are to a real escalating attack.  Security teams monitoring the Vectra console should primarily base their judgment on which hosts or accounts to review first and based on the calculated severity ranking.

Hosts and accounts categorized as Critical or High severity have a high potential for doing damage to business operations and exhibit behaviors associated with actively unfolding attacks that warrant investigation. Accounts categorized as Low or Medium severity are exhibiting less directly observed risks and can be leveraged for starting points in threat hunting efforts rather than immediate investigation.

In addition to the severity ranking, threat and certainty scores are calculated for each prioritized account based on the correlated behaviors to enable finer-grain ordering.

Detections also receive threat and certainty scores that characterize detection-specific severities based on the threat of the associated behavior and certainty of the underlying detection models.  Details of how each detection's threat and certainty are calculated are presented on their respective detections one-pagers.

- Top -

# Detect for Network

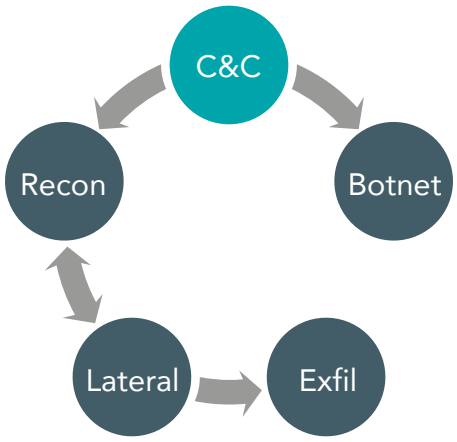


## Category

# Command & Control

- A host or account appears to be under control of an external entity
- Most often, the control is automated as the host or account is part of a botnet or has adware or spyware installed
- The host or account may be manually controlled from the outside – this is the most threatening case and makes it highly likely that this is a targeted attack

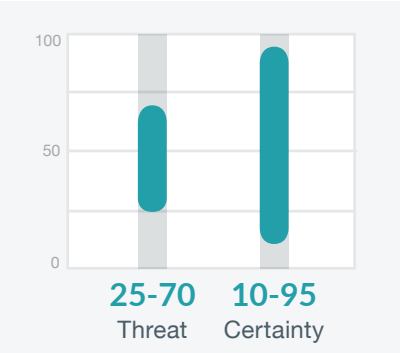


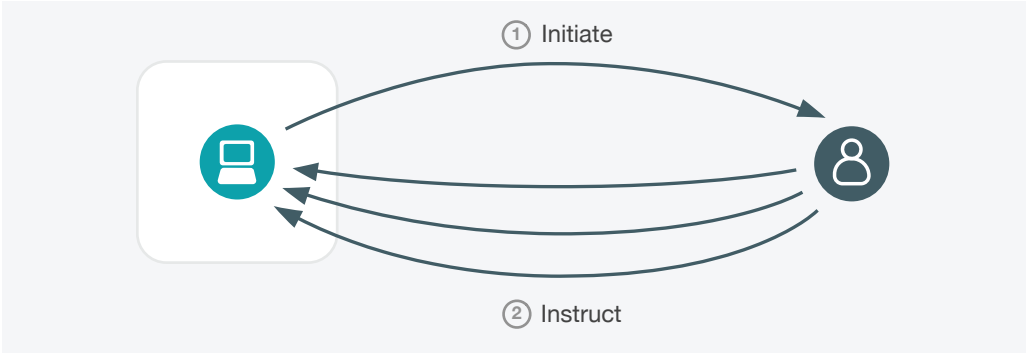



- Top -

# External Remote Access

## Command & Control




MITRE | ATT&CK®

T1005 Data from Local System
T1115 Clipboard Data
T1071 Application Layer Protocol
T1125 Video Capture
T1090 Proxy
T1113 Screen Capture
T1010 Application Window Discovery
T1037 Boot or Logon Initialization Scripts
T1111 Two-Factor Authentication Interception
T1572 Protocol Tunneling
T1573 Encrypted Channel
T1048 Exfiltration Over Alternative Protocol
T1204 User Execution
T1056 Input Capture
T1001 Data Obfuscation
T1571 Non-Standard Port
T1059 Command and Scripting Interpreter
T1518 Software Discovery
T1176 Browser Extensions
T1123 Audio Capture
T1008 Fallback Channels
T1219 Remote Access Software
T1105 Ingress Tool Transfer
T1133 External Remote Services
T1095 Non-Application Layer Protocol
T1132 Data Encoding

## Triggers

- An internal host is connecting to an external server and the pattern looks reversed from normal client to server traffic; the client appears to be receiving instructions from the server and a human on the outside appears to be controlling the exchange
- The threat score is driven by the quantity of data exchanged and longevity of the connection
- The certainty score is driven by the ratio of data sent by the internal host compared to data received from the server and the longevity of the connection

## Possible Root Causes

- A host includes malware with remote access capability (e.g. Meterpreter, Poison Ivy) that connects to its C&C server and receives commands from a human operator
- A user has intentionally installed and is using remote desktop access software and is accessing the host from the outside (e.g. GotoMyPC, RDP)
- This behavior can also be exhibited through very active use of certain types of chat software that exposes similar human-driven behavior

## Business Impact

- Presence of malware with human-driven C&C is a property of targeted attacks
- Business risk associated with outside human control of an internal host is very high
- Provisioning of this style of remote access to internal hosts poses substantial risks as compromise of the service provides direct access into your network

## Steps to Verify

- Look at the detection details and the PCAP to determine whether this may be traffic from chat software
- Check if a user has knowingly installed remote access software and decide whether the resulting risk is acceptable
- Scan the computer for known malware and potentially reimage it, noting that some remote access toolkits leave no trace on disk and reside entirely in memory

- Top -

# Hidden DNS Tunnel

## Command & Control


MITRE | ATT&CK®

T1005 Data from Local System

T1071 Application Layer Protocol

T1010 Application Window Discovery

T1037 Boot or Logon Initialization Scripts

T1572 Protocol Tunneling

T1573 Encrypted Channel

T1056 Input Capture

T1001 Data Obfuscation

T1059 Command and Scripting Interpreter

T1008 Fallback Channels

T1105 Ingress Tool Transfer

T1132 Data Encoding

### Triggers

- An internal host is communicating with an outside IP using DNS where another protocol is running over the top of the DNS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal DNS traffic
- The threat score is driven by the quantity of data sent and received via the tunnel
- The certainty score is driven by the similarity of the packet-level patterns to those of DNS tunnels

### Possible Root Causes

- A targeted attack may use hidden tunnels to hide communication with command and control servers
- A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible
- Intentionally installed software is using a hidden tunnel to bypass expected firewall rules

### Business Impact

- The use of a hidden tunnel by some software may be benign, but it represents significant risk as the intention is to bypass security controls
- Hidden tunnels used as part of a targeted attack are meant to slip by your perimeter security controls and indicate a sophisticated attacker
- Hidden tunnels are rarely used by botnets, though more sophisticated bot herders with more ambitious goals may utilize them

### Steps to Verify

- Check to see if the destination domain of the tunnel is an entity you trust for your network
- Ask the user of the host whether they are using hidden tunnel software for any purpose
- Before removing the offending software via antivirus or reimaging, take a memory snapshot for future analysis of the incident
- If the behavior reappears shortly after a reimaging, this may be a hardware/BIOS tunnel

- Top -

# Hidden HTTP Tunnel

## Command & Control


MITRE | ATT&CK®

T1005 Data from Local System

T1115 Clipboard Data

T1071 Application Layer Protocol

T1185 Man in the Browser

T1125 Video Capture

T1113 Screen Capture

T1010 Application Window Discovery

T1037 Boot or Logon Initialization Scripts

T1111 Two-Factor Authentication Interception

T1572 Protocol Tunneling

T1204 User Execution

T1056 Input Capture

T1001 Data Obfuscation

T1571 Non-Standard Port

T1059 Command and Scripting Interpreter

T1518 Software Discovery

T1176 Browser Extensions

T1123 Audio Capture

T1008 Fallback Channels

T1105 Ingress Tool Transfer

T1132 Data Encoding

## Triggers

- An internal host is communicating with an outside IP using HTTP where another protocol is running over the top of the HTTP sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal Web traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions

## Possible Root Causes

- A targeted attack may use hidden tunnels to hide communication with command and control servers
- A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible
- Intentionally installed software is using a hidden tunnel to bypass expected firewall rules

## Business Impact

- The use of a hidden tunnel by some software may be benign, but it represents significant risk as the intention is to bypass security controls
- Hidden tunnels used as part of a targeted attack are meant to slip by your perimeter security controls and indicate a sophisticated attacker
- Hidden tunnels are rarely used by botnets, though more sophisticated bot herders with more ambitious goals may utilize them

## Steps to Verify

- Check to see if the destination IP or domain of the tunnel is an entity you trust for your network
- Ask the user of the host whether they are using hidden tunnel software for any purpose
- Before removing the offending software via antivirus or reimaging, take a memory snapshot for future analysis of the incident
- If the behavior reappears shortly after a reimaging, this may be a hardware/BIOS tunnel

- Top -

# Hidden HTTPS Tunnel

## Command & Control


MITRE | ATT&CK®

T1005 Data from Local System

T1115 Clipboard Data

T1071 Application Layer Protocol

T1185 Man in the Browser

T1125 Video Capture

T1113 Screen Capture

T1010 Application Window Discovery

T1037 Boot or Logon Initialization Scripts

T1111 Two-Factor Authentication Interception

T1572 Protocol Tunneling

T1573 Encrypted Channel

T1204 User Execution

T1056 Input Capture

T1001 Data Obfuscation

T1571 Non-Standard Port

T1059 Command and Scripting Interpreter

T1518 Software Discovery

T1176 Browser Extensions

T1123 Audio Capture

T1008 Fallback Channels

T1132 Data Encoding

## Triggers

- An internal host is communicating with an outside IP using HTTPS where another protocol is running over the top of the HTTPS sessions
- This represents a hidden tunnel involving one long session or multiple shorter sessions over a longer period of time mimicking normal encrypted Web traffic
- When it can be determined whether the tunneling software is console-based or driven via a graphical user interface, that indicator will be included in the detection
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the combination of the persistence of the connection(s) and the degree to which the observed volume and timing of requests matches up with training samples

## Possible Root Causes

- A targeted attack may use hidden tunnels to hide communication with command and control servers over SSL on port 443
- A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible
- Intentionally installed software is using a hidden tunnel to bypass expected firewall rules

## Business Impact

- The use of a hidden tunnel by some software may be benign, but it represents significant risk as the intention is to bypass security controls
- Hidden tunnels used as part of a targeted attack are meant to slip by your perimeter security controls and indicate a sophisticated attacker
- Hidden tunnels are rarely used by botnets, though more sophisticated bot herders with more ambitious goals may utilize them

## Steps to Verify

- Check to see if the destination IP or domain of the tunnel is an entity you trust for your network
- Ask the user of the host whether they are using hidden tunnel software for any purpose
- Before removing the offending software via antivirus or reimaging, take a memory snapshot for future analysis of the incident
- If the behavior reappears shortly after a reimaging, this may be a hardware/BIOS tunnel

- Top -

# Malware Update

## Command & Control



MITRE | ATT&CK®

T1105 Ingress Tool Transfer

### Triggers

- An internal host is downloading and installing software from the Internet
- The downloads are over HTTP, appear to be machine- driven, and follow a suspicious pattern of checking for availability of files before downloading them
- The threat score is driven by the number of executable files being downloaded
- The certainty score is driven by the pattern of machine- generated HTTP requests

### Possible Root Causes

- The initial exploit on this host may be loading malware to continue the attack
- Malware installed on the host may be updating itself to enhance its functionality
- Malware installed on the host may be updating itself to a new version of its software

### Business Impact

- An infected host can attack other organizations (e.g. spam, DoS, ad clicks) thus causing harm to your organization's reputation, potentially causing your IP addresses to be black listed and impacting the performance of business-critical applications
- If this is a targeted attack, it can spread further into your network and ultimately exfiltrate data from it
- The malware which infected the host can create nuisances and affect user productivity

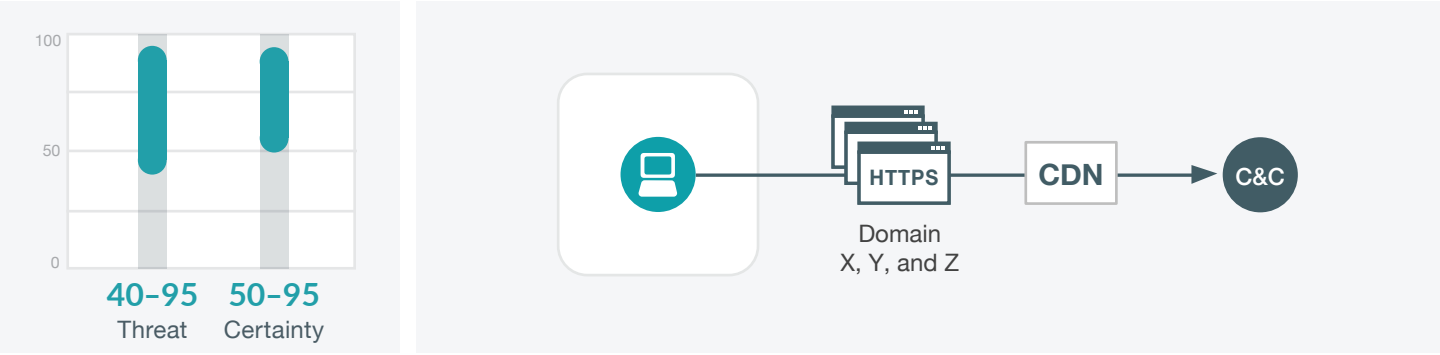
### Steps to Verify

- Look up the domain and IP address to which the communication is being sent via reputation services to see if this is known malware; such lookups are supported directly within the UI
- Search for the domain + "virus" via a search engine; this is effective for finding references to known adware or spyware
- Download the supplied PCAP and look at the HTTP payload being sent to see if any data is being leaked in clear text or whether the identity of the program is visible

- Top -

# Multi-home Fronted Tunnel

## Command & Control




MITRE | ATT&CK®

T1005 Data from Local System

T1115 Clipboard Data

T1071 Application Layer Protocol

T1125 Video Capture

T1113 Screen Capture

T1010 Application Window Discovery

T1037 Boot or Logon Initialization Scripts

T1111 Two-Factor Authentication Interception

T1572 Protocol Tunneling

T1573 Encrypted Channel

T1204 User Execution

T1056 Input Capture

T1001 Data Obfuscation

T1571 Non-Standard Port

T1059 Command and Scripting Interpreter

T1518 Software Discovery

T1176 Browser Extensions

T1123 Audio Capture

T1008 Fallback Channels

T1132 Data Encoding

### Triggers

- An internal host is communicating with an outside IP using HTTPS where another protocol is running over the top of the HTTPS sessions. The sessions appear to go to different domains but are all served by a single Content Delivery Network (CDN) and all utilize a JA3 hash which is only used by this host with this one CDN.
- This represents a hidden tunnel involving multiple shorter sessions over a longer period of time mimicking normal encrypted Web traffic
- The threat score is driven by the amount of data transfer spikes over the baseline beacon and the number of unique second-level domains contacted
- The certainty score is driven by the communication persistence, the total connection volume, and how the traffic is spread across the different domains

### Possible Root Causes

- A targeted attack may use hidden tunnels to hide communication with command and control servers over TLS on port 443 and other ports
- Intentionally installed software is using a domain-fronted hidden tunnel utilizing multiple benign domains to bypass expected firewall rules

### Business Impact

- The use of a hidden tunnel with multi-domain fronting is quite unusual, and it represents significant risk as the intention is to bypass security controls
- Hidden tunnels used as part of a targeted attack are meant to slip by your perimeter security controls and indicate a sophisticated attacker

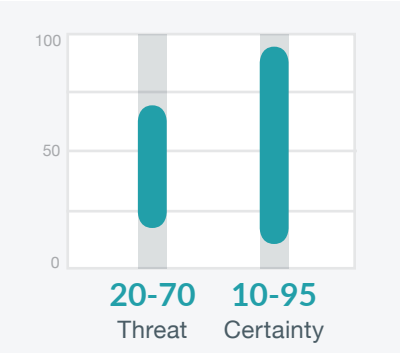
### Steps to Verify

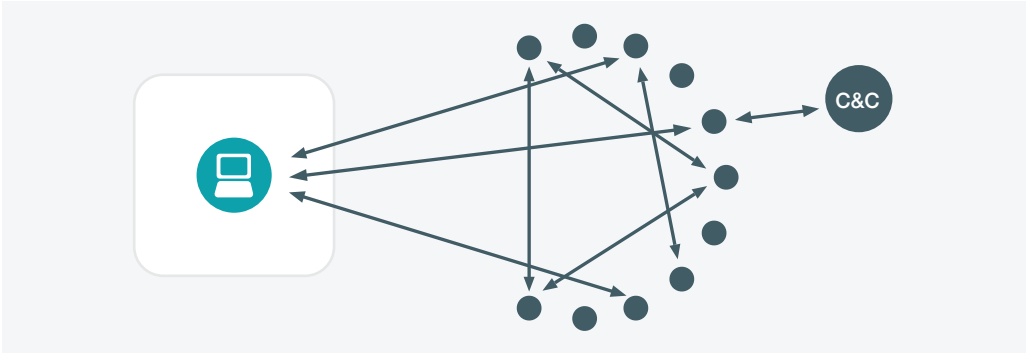
- Ask the user of the host whether they are using hidden tunnel software for any purpose and if not, whether they intentionally connected to the list of domains in the detection (the JA3-hash in the detection may provide a clue to the software utilized)
- Before removing the offending software via antivirus or reimaging, take a memory snapshot for future analysis of the incident
- If the behavior reappears shortly after a reimaging, this may be a hardware/BIOS tunnel

- Top -

# Peer-To-Peer

## Command & Control




MITRE | ATT&CK®

T1090 Proxy

### Triggers

- An internal host is communicating with a set of external IP addresses with a pattern and low data rate common to peer-to-peer command and control
- The threat score is driven by the length of time over which communication with peers occurs
- The certainty score is driven by the number of reachable and unreachable peers

### Possible Root Causes

- The internal host is infected with malware which is using peer-to-peer communication for its command and control; some botnets utilize this form of command and control as it is more resilient to attempts at disrupting or sink holing it
- Legitimate peer-to-peer software is running idle in the background without any data (e.g. Bittorrent) or voice (e.g. Skype) transfer activity and as such exhibits patterns similar to command and control traffic

### Business Impact

- An infected host can attack other organizations (e.g. spam, DoS, ad clicks) thus causing harm to your organization's reputation, potentially causing your IP addresses to be black listed and impacting the performance of business-critical applications
- The host can also be instructed to spread further into your network and ultimately exfiltrate data from it
- Software which infected the host can create nuisances and affect user productivity

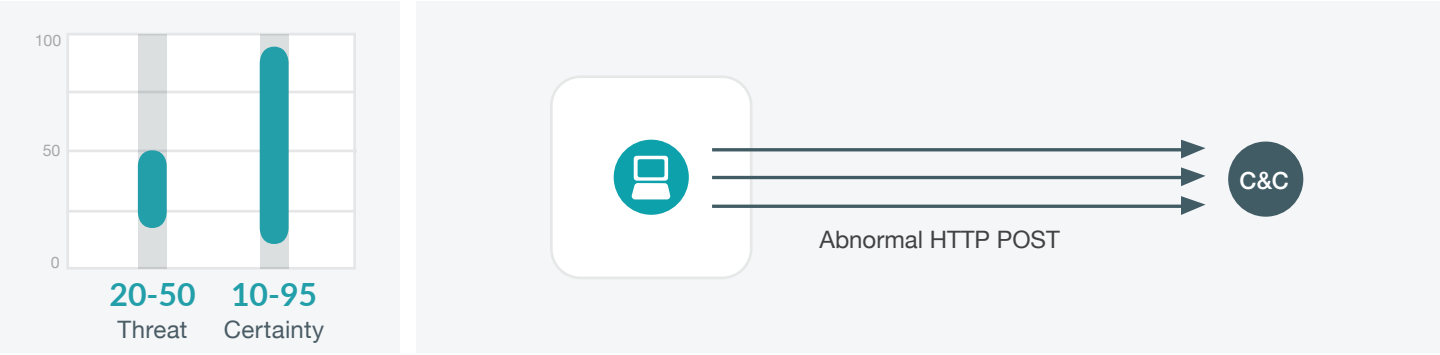
### Steps to Verify

- If the detection is generated as a result of a purposely installed peer-to-peer application, make sure the software complies with IT security policy
- If the detection cannot be attributed to such an application, the host is likely infected with a malware and should be fixed through the use of AV software or reimaged

- Top -

# Stealth HTTP Post

## Command & Control




MITRE | ATT&CK®

T1071 Application Layer Protocol

### Triggers

- An internal host is sending data to an external system in multiple HTTP Post requests without being referred and without software identification
- These posts appear to be machine generated since they occur with a regular timing pattern
- The threat score is driven by the number of overall sessions and length of their duration
- The certainty score is driven by the number and persistence of HTTP Post requests

### Possible Root Causes

- Adware, spyware or malware installed on an internal host is communicating back to its command and control server
- The communication may include some data leakage from the local host, which is particularly common with spyware

### Business Impact

- An infected host can attack other organizations (e.g. spam, DoS, ad clicks) thus causing harm to your organization's reputation, potentially causing your IP addresses to be black listed and impacting the performance of business-critical applications
- The host can also be instructed to spread further into your network and ultimately exfiltrate data from it
- Software which infected the host can create nuisances and affect user productivity

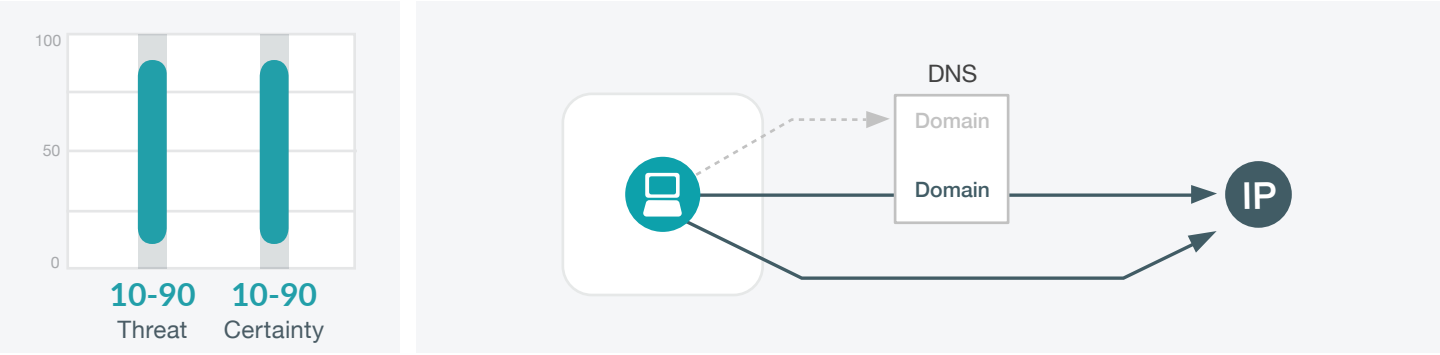
### Steps to Verify

- Look up the domain and IP address to which the communication is being sent via VirusTotal or other reputation services to see if this is known malware; such lookups are supported directly within the UI
- Search for the domain + "virus" via a search engine – this is effective for finding references to known adware or spyware
- Download the supplied PCAP and look at the HTTP payload being sent to see if any data is being leaked in clear text or whether the identity of the program is visible in the payload

- Top -

# Suspect Domain Activity

## Command & Control




MITRE | ATT&CK®

T1568 Dynamic Resolution

### Triggers

- An internal host is looking up suspicious external domains
- Suspicious activity may involve looking up machine-generated domain names or non-existent domain names in rapid succession
- The threat score is driven by successful lookups
- The certainty score is driven by the breadth of domain lookups and the characteristics of successful lookups

### Possible Root Causes

- An infected host which is part of a botnet is using a domain generation algorithm (DGA) to locate its command & control servers
- An infected host or adware installed by the user is accessing newly generated domains to present ad impressions to the user
- An internal user visits newly registered domains with unusual names (e.g., letter sequences not normally found in domains)

### Business Impact

- An infected host can attack other organizations (e.g. spam, DoS, ad clicks) thus causing harm to your organization's reputation, potentially causing your IP addresses to be black listed and impacting the performance of business-critical applications
- The host can also be instructed to spread further into your network and ultimately exfiltrate data from it
- Software which infected the host can create nuisances and affect user productivity

### Steps to Verify

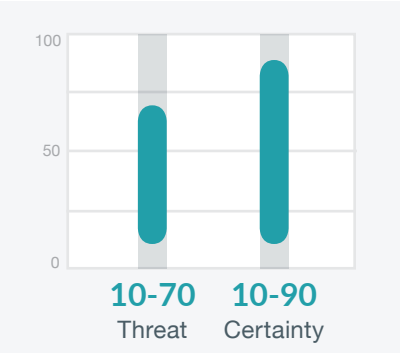
- Do not go directly to the listed domain as it is likely to be malicious
- Look up the domain and IP address to which the communication is being sent via reputation services to see if this is known malware; such lookups are supported directly from the UI
- Inquire whether the user of the host would likely have gone to the listed domain
- Check to see if the host is also exhibiting other detected behaviors to understand the intent of the malware

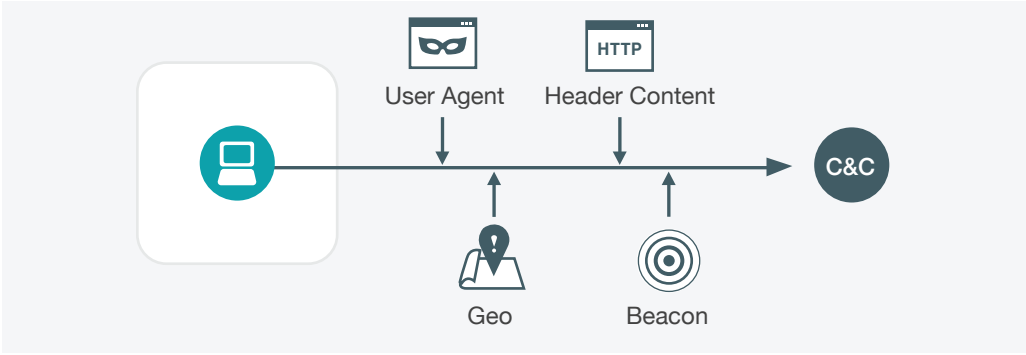
- Top -

# Suspicious HTTP

## Command & Control




MITRE | ATT&CK®

T1071 Application Layer Protocol

## Triggers

- Software on an internal host is initiating one or more suspicious HTTP requests which form a pattern typically observed in command and control communications in recent malware samples
- The suspicious pattern may be the result of any combination of the following: (a) incorrect or malformed User-Agent, (b) absence or presence and order of a variety of HTTP headers, (c) presence and regularity of beaconing of the request and (d) connections to geographies which have a higher likelihood of hosting command and control servers
- While beaconing is a key driver of the threat score, the presence of all four factors causes the threat score to be at the top of the range. Combinations with fewer factors will score successively lower with combinations that don't include beaconing being at the very low end of the range.
- Suspicious User-Agent and suspicious HTTP header contribute strongly to the certainty score while geo and beaconing contribute weakly. Suspicious HTTP communication to multiple domains further increases the certainty score.

## Possible Root Causes

- Malware installed on the host may be communicating back to its command and control server(s)
- Adware or spyware installed on the host may be communicating to its command and control server(s) or may be leaking data acquired on the host
- Software installed on the host is emitting HTTP requests that share two or more patterns with recent known malware samples: (a) malformed User-Agent, (b) unusual collection of HTTP headers, (c) communicating in an automated pattern and (d) communicating to out-of-the-ordinary geographies

## Business Impact

- An infected host can attack other organizations (e.g. spam, DoS, ad clicks) thus causing harm to your organization's reputation, potentially causing your IP addresses to be black listed and impacting the performance of business-critical applications
- The host can also be instructed to spread further into your network and ultimately exfiltrate data from it
- Software which infected the host can create nuisances and affect user productivity

- Top -

## Steps to Verify

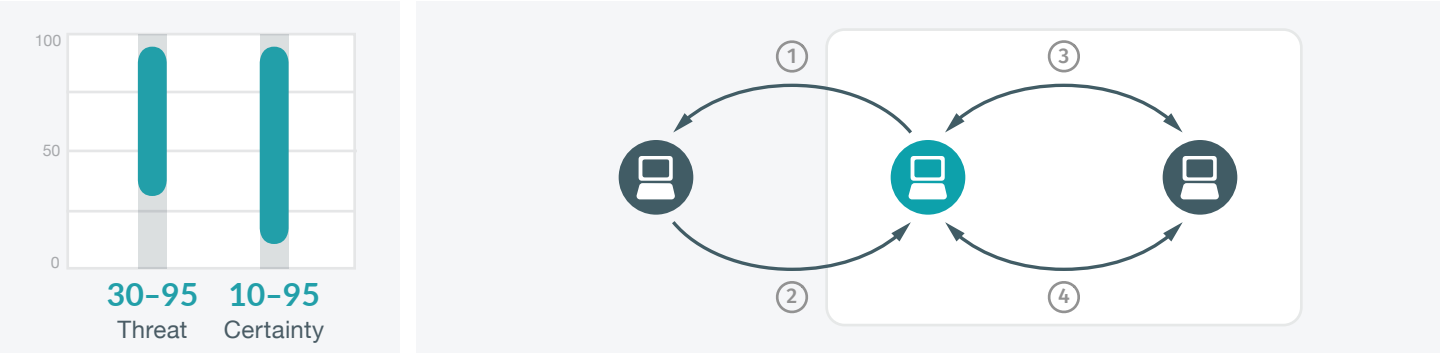
- Look up the domain and IP address to which the communication is being sent via reputation services to see if this is known malware; such lookups are supported directly within the UI
- Search for the domain + “virus” via a search engine; this is effective for finding references to known adware or spyware
- Download the supplied PCAP and look at the HTTP payload being sent to see if any data is being leaked in clear text or whether the identity of the program is visible
- If there is no known reason why the user of the system would communicate to the geography in question, ask the end-user for a possible reason for the communication

- Top -

# Suspicious Relay

## Command & Control




MITRE | ATT&CK®

T1090 Proxy

T1104 Multi-Stage Channels

### Triggers

- This host appears to be acting as a relay for communication between an external system to another internal host—relays of this type involve a first (external) leg and a second (internal) leg
- This host also has another active command and control detection
- The threat score is driven by how close the durations of the connections involved in relay activity are on the two legs of the relay
- The certainty score is driven by how close the ratio of sent to received bytes are in the two legs of the relay

### Possible Root Causes

- A host is compromised and is being used to relay information to and from a host deeper inside the network
- An internal host is hosting some form of approved proxy (e.g. SOCKS) to allow other internal hosts to communicate with the Internet through it

### Business Impact

- An infected host which is enabling another internal host to hide its communication with the Internet by acting as a relay represents a high risk as this may allow a host which normally is not allowed to communicate with the outside to do so
- For hosts that have approved proxy software installed, ensure all the necessary security controls are in place to prevent unauthorized use

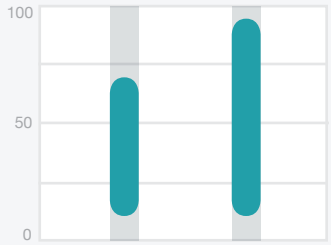
### Steps to Verify

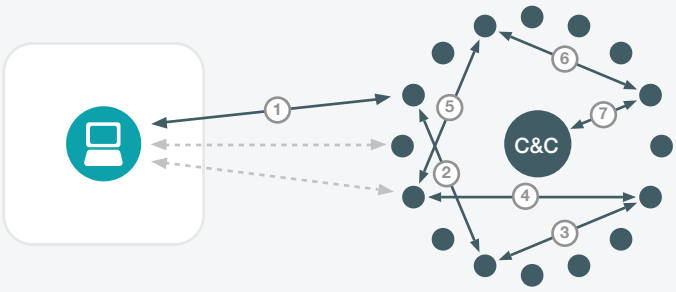
- Determine whether this host should be providing relay services to other internal hosts; if not, this is likely malicious behavior
- Look at the outside destination of the traffic and the payload of traffic, available in the PCAP, to determine what it being sent and where it is going; this will help further calibrate the risk

- Top -

# TOR Activity

## Command & Control



The Onion Router (TOR)

MITRE | ATT&CK®

T1090 Proxy

### Triggers

- An internal host establishes connections with outside servers where protocol usage approximates communicating via The Onion Router (TOR)
- The algorithm inspects the protocol handshake of each session and triggers if characteristics of the session setup are similar to those observed in TOR connections
- The threat score is driven by volume and similarity to command and control traffic; it is low for browsing, high for command and control or when there is a significant amount of outbound data observed
- The certainty score is driven by the similarity of the session characteristics to those observed in TOR sessions

### Possible Root Causes

- A targeted attack is utilizing TOR to hide communications with command and control servers or to exfiltrate your organization's data
- An infected host which is part of a botnet is utilizing TOR to communicate with its command and control servers or to leak small amounts of stolen data
- A user is utilizing a TOR-enabled program to anonymously communicate with servers available on the Internet or ones available only through TOR

### Business Impact

- The use of TOR as part of a targeted attack is meant to slip by most standard perimeter defenses and indicates attacker sophistication
- The use of TOR as part of a botnet is relatively rare and would indicate a more sophisticated botnet
- The intentional use of TOR by employees may be allowed, but it does represent significant risk as the intention of TOR is to mask traffic source and destination

### Steps to Verify

- Ask the user of the host whether they are using TOR for any purpose
- Check to see if any TOR-enabled software is installed on the host
- Check the TOR entry nodes listed in the detection against lists of known TOR entry nodes (e.g., search for "tor entry node list"), but note that these lists are seldom complete and shift over time

- Top -

# Threat Intelligence Match

## Command & Control


### Triggers

- An internal host is connecting to an external system and the connection has met criteria specified in one or more configured threat feeds
- The threat score is driven by the combination of the indicator type in the STIX file (with watchlist and anonymization being lowest, malware artifacts being medium, and C2 channel and exfiltration being highest) and the quantity of data received on the flagged connections
- The certainty score is specified as part of the threat feed configuration and ranges from low (30) to medium (60) and high (90)

### Possible Root Causes

- A host includes malware which is initiating the connection that triggered the detection
- A user on the host manually initiated the connection which triggered the detection

### Business Impact

- Presence of command & control is a property of most attacks that originate from the outside
- The threat intel feed may have included additional context tied to the specific criteria that the connection met
- Business risk associated with outside control of an internal host is very high

### Steps to Verify

- Refer to the information accompanying your threat feed as it may include verification and remediation instructions
- Determine which process on the internal host is sending the traffic which was flagged; in Windows systems, this can be done using a combination of netstat and tasklist commands
- Check if a user has knowingly installed remote access software and decide whether the resulting risk is acceptable
- Scan the computer for known malware and potentially reimage it, noting that some infections leave no trace on disk and reside entirely in memory

- Top -

# Vectra Threat Intelligence Match

## Command & Control


MITRE | ATT&CK®

T1008 Fallback Channels

T1041 Exfiltration Over C2 Channel

T1048 Exfiltration Over Alternative Protocol

T1059 Command and Scripting Interpreter

T1071 Application Layer Protocol

T1095 Non-Application Layer Protocol

T1105 Ingress Tool Transfer

T1132 Data Encoding

T1189 Drive-by Compromise

T1219 Remote Access Software

T1571 Non-Standard Port

T1573 Encrypted Channel

### Triggers

- An internal host has been observed either generating DNS activity or making direct connections associated with malicious external IPs or Domains identified by Vectra Threat Intelligence.
- The threat score is driven by the quantity of data received on the flagged connection
- The certainty score is related to Vectra's confidence in active use of the indicator and ranges from low (30) to medium (60) and high (90)

### Possible Root Causes

- A host is communicating with a confirmed malicious IP or Domain that may be associated with staged malware, command and control, or client-side attacks.
- A user has been redirected to a site associated with phishing or credential compromise.
- A host is communicating with a benign service co-hosted on an IP or Domain with a poor or malicious reputation.

### Business Impact

- Compromised assets or user credentials provide adversaries with the internal foothold necessary to begin to stage an attack.
- The identification of internal connections to known bad IP addresses or domains demonstrates positive risk to organizational assets and users and may indicate active attack progression.

### Steps to Verify

- Investigate the host and accounts associated for further indications of compromise.
- Using appropriate operational security and safeguards, verify the risk posed by this known bad IP or Domain by consulting external third party sources.
- Verify if supplemental preventative security controls protected the asset from full communication.
- In the case of phishing, verify with the user if credentials may have been compromised or take appropriate risk-based containment activities to include session revocation and password resets.
- Verify host integrity, the presence of new, unauthorized, or malicious software, and take appropriate incident handling or response activities.

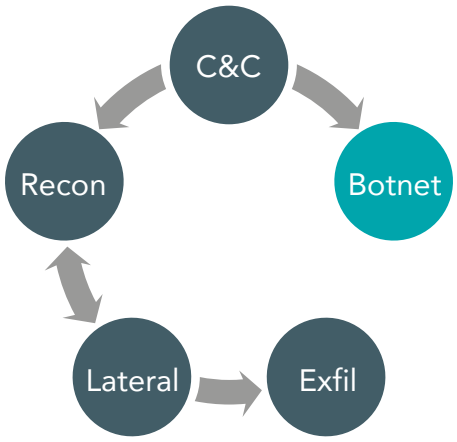
- Top -

## Category

# Botnet Activity

- A host is making money for its bot herder
- The ways in which an infected host can be used to produce value can range from mining bitcoins to sending spam emails to producing fake ad clicks
- The bot herder is utilizing the host computer, its network connection and, most of all, the unsullied reputation of the assigned IP to turn a profit

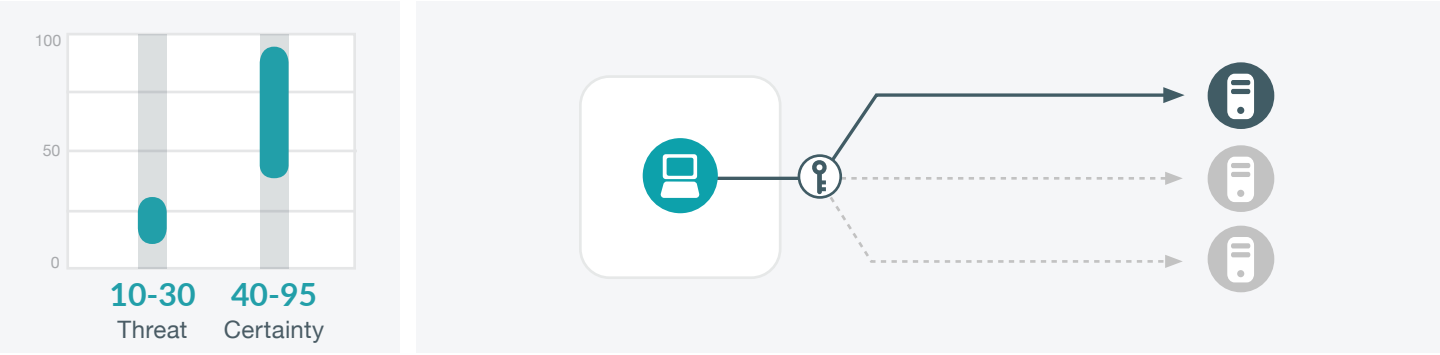





- Top -

# Brute-Force

## Botnet Activity




MITRE | ATT&CK®

T1110 Brute Force

### Triggers

- An internal host is making an unusually high number of login attempts, a behavior which is consistent with a brute-force password-guessing attack on one or more external servers
- Such attacks can be performed via a number of different protocols
- The threat score is driven by the rate of attempts and timing at which the attack is performed
- The certainty score is driven by total number of sessions in the attack

### Possible Root Causes

- An infected host is trying to guess passwords on one or more external systems; this is common botnet behavior where the host is instructed to breach internet-accessible systems that can be used as way points for command and control and data leakage
- A misconfigured internal host is constantly trying to connect to one or more external systems

### Business Impact

- Botnet activity presents several risks to the organization: (1) it creates noise which may hide more serious issues; (2) there is a chance your organization's IP will end up on black lists; and (3) the compromised host can always be instructed to perform a direct attack on the organization
- Even if triggered due to a misconfiguration, the identified behavior is creating significant noise that may mask more serious issues and should be cleaned up

### Steps to Verify

- If the internal host should not even be connecting to the external servers, this is likely malicious behavior
- Determine which process on the internal host is sending traffic to the external IP address(es) and ports; in Windows systems, this can be done using a combination of netstat and tasklist commands
- Verify that the process on the infected host should even be running and whether the process is configured correctly

- Top -

# Cryptocurrency Mining

## Botnet Activity



MITRE | ATT&CK®

T1496 Resource Hijacking

### Triggers

- An internal host is mining units of cryptocurrency of which Bitcoin, Litecoin, Ethereum, and Monero are some of the most common variants
- Cryptocurrency mining is a common way for botnet operators to make money
- Cryptocurrency mining may involve communication via HTTP or via the Stratum mining protocol
- The threat score is driven by the rate at which cryptocurrency mining activity is performed

### Possible Root Causes

- An infected host is mining cryptocurrency for its bot herder
- Some cryptocurrency mining can occur in the user's browser as a side effect of visiting compromised or low-reputation websites
- The user of the host on which the behavior has been detected has installed cryptocurrency mining software and is making money using your organization's systems, power, and network resources

### Business Impact

- Botnet activity presents several risks to the organization: (1) it creates noise which may hide more serious issues; (2) there is a chance your organization's IP will end up on black lists; and (3) the compromised host can always be instructed to perform a direct attack on the organization
- If the user of the host intentionally installed cryptocurrency mining software, the risk may be minimal, though such a user may also be prone to installing other "money making" software which may not prove to be as benign

### Steps to Verify

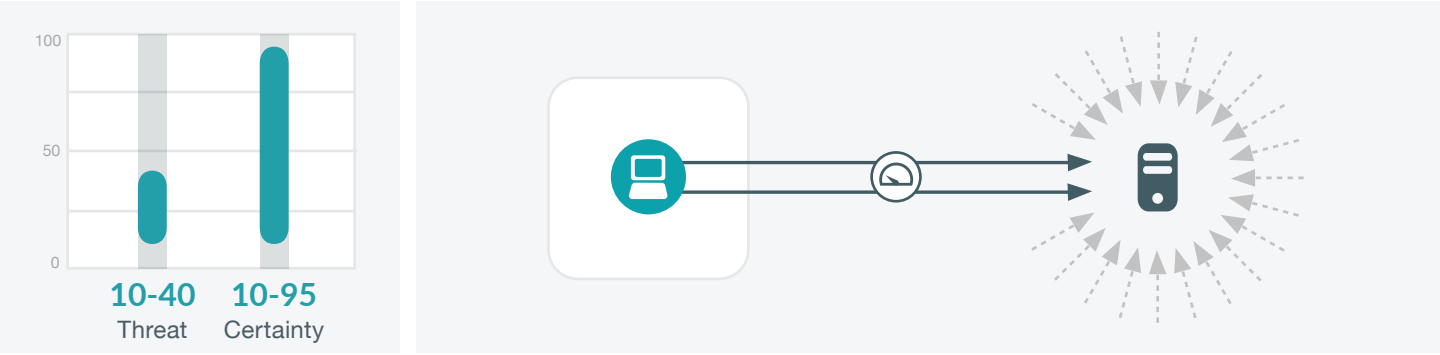
- If the user intentionally installed cryptocurrency mining software, decide whether it should be removed
- If the user did not install cryptocurrency mining software, the host is likely infected and part of a botnet that performs "silent mining"
- Use anti-virus software or reimage the host to remove the malware

- Top -

# Outbound DoS

## Botnet Activity




MITRE | ATT&CK®

T1498 Network Denial of Service

### Triggers

- An internal host appears to be taking part in a Denial- of-Service (DoS) campaign on an external IP address
- The form of DoS detection has two types: “SYN Flood” and “Slowloris”
- The threat score is driven by the volume of data sent in the detected DoS sessions
- The certainty score is driven by the volume of DoS sessions and the length of period the attack is sustained

### Possible Root Causes

- The internal host is infected and has become part of a botnet and is being instructed by its bot herder to perform a DoS attack on an external system, which is a relatively common way for a botnet to make money
- An internal host is misconfigured and continually, in high volume, tries to connect to an external IP address

### Business Impact

- Botnet activity presents several risks to the organization: (1) it creates noise which may hide more serious issues; (2) there is a chance your organization’s IP will end up on black lists; and (3) the compromised host can always be instructed to perform a direct attack on the organization
- The sheer volume of flood attacks may materially affect the amount of bandwidth available for legitimate functions which need to access the Internet

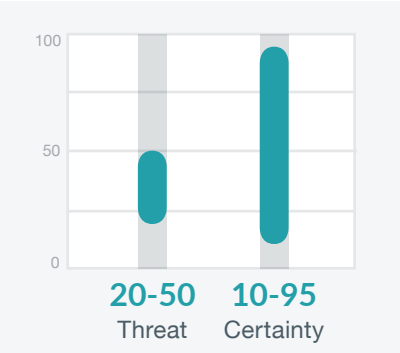
### Steps to Verify

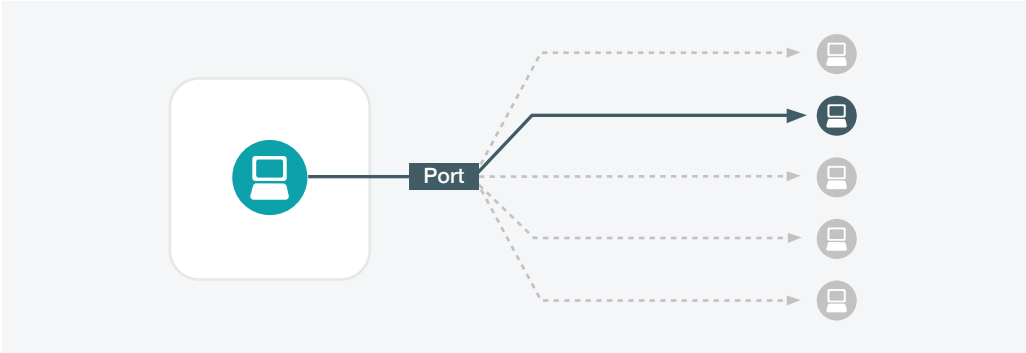
- Explore if there is a legitimate reason for the host to be connecting to the suspected victim of the attack
- Contact the user of the host to see whether they are trying to perform some unusual task which might trigger the DoS detection
- Check the host for presence of malware that is participating in a DoS attack

- Top -

# Outbound Port Sweep

## Botnet Activity




MITRE | ATT&CK®

T1018 Remote System Discovery

### Triggers

- An internal host is generating many more unsuccessful attempts to connect to external services than successful ones
- The threat score is driven by the breadth of IP addresses scanned and the pace at which the scan occurs
- The certainty score is driven by the failure rate of outbound connection attempts

### Possible Root Causes

- An internal host is part of a botnet and is being used by its bot herder to find other external services that could subsequently be attacked
- An internal host is misconfigured and is making many connection attempts to different IP addresses on the Internet

### Business Impact

- Botnet activity presents several risks to the organization: (1) it creates noise which may hide more serious issues; (2) there is a chance your organization's IP will end up on black lists; and (3) the compromised host can always be instructed to perform a direct attack on the organization
- A misconfigured internal host may be using unnecessary bandwidth and slowing down both the host itself and other applications as a result of the traffic it is sending

### Steps to Verify

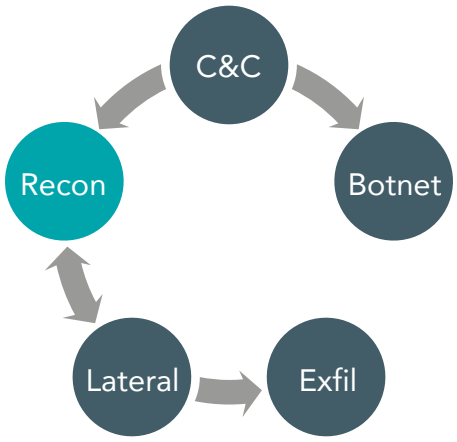
- Look at the pattern of IP addresses being scanned to determine the intent of the scan
- Verify whether there is misconfigured software on the host which is causing the scan
- If the behavior cannot be explained by user action or known software behavior, the host is likely infected and should be remediated

- Top -

## Category

# Reconnaissance

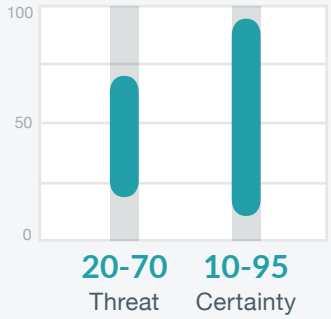
- A host or account is mapping out the inside of your network or cloud environment
- The activity may indicate that this is a targeted attack
- Detection types cover fast scans and slow scans – your vulnerability scanner will show up here as it performs much the same activity as an attacker

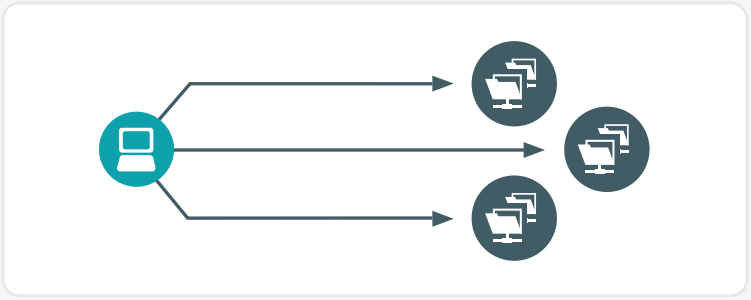



- Top -

# File Share Enumeration

## Reconnaissance



MITRE | ATT&CK®

T1039 Data from Network Shared Drive

T1119 Automated Collection

T1135 Network Share Discovery

### Triggers

- A host accesses a number of file shares significantly in excess of the number of file shares normally accessed in the network
- The threat score is proportional to the diversity of shares being mounted with a higher threat score for larger number of shares across a few file servers vs. a small number of shares across many file servers
- The certainty score is driven by the volume of shares mounted

### Possible Root Causes

- An attacker is looking for data to exfiltrate or is looking for files which provide additional information necessary for achieving the goals of the attack
- The host is accessing a large number of file shares as an end user attempts to find a particular file or directory

### Business Impact

- An enumeration of the available file shares in a network is an effective way for an attacker to find data to exfiltrate or data that helps further the attack
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep or a port scan so attackers feel they can use it with relatively little risk of detection

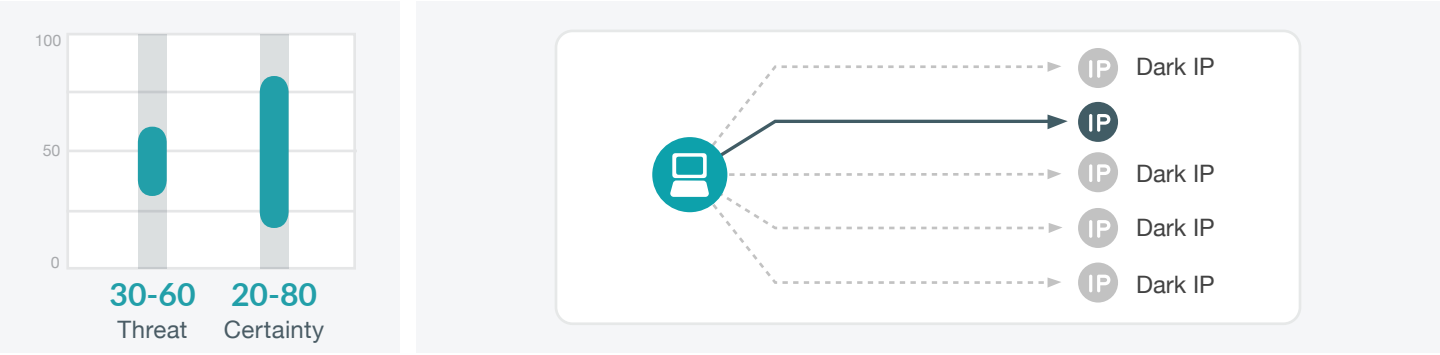
### Steps to Verify

- Ask the user of the host whether they have any knowledge of accessing the listed file shares
- Check the file server logs to see what files were accessed on the shares
- If the file share access continues and remains unexplained, determine which process on the internal host is accessing the file shares; in Windows systems, this can be done using a combination of netstat and tasklist commands

- Top -

# Internal Darknet Scan

## Reconnaissance




MITRE | ATT&CK®

T1082 System Information Discovery

T1018 Remote System Discovery

T1072 Software Deployment Tools

T1046 Network Service Scanning

T1016 System Network Configuration Discovery

### Triggers

- An internal host has contacted a number of internal IPs that have not been active in the recent past
- Darknet detections cover longer periods than port scans and ignore contact to systems which do not respond to this host, but which are otherwise active
- The threat score places large weight on the spread of IPs, medium for spread of ports and low for the total number of dark IPs contacted
- The certainty score places equal weight on the spread of IPs, spread of ports and number of dark IPs contacted

### Possible Root Causes

- An infected internal system that is part of targeted attack is performing slow reconnaissance of your network by reaching out to different IP addresses in your network
- A vulnerability scanner or asset discovery system is mapping systems in your network
- A host has been moved to a new network and is unsuccessfully attempting to connect to many previously available services

### Business Impact

- Slow reconnaissance of your systems may represent the beginning of a targeted attack in your network
- Authorized reconnaissance by vulnerability scanners and asset discovery systems should be limited to a small number of hosts which can be whitelisted for this behavior

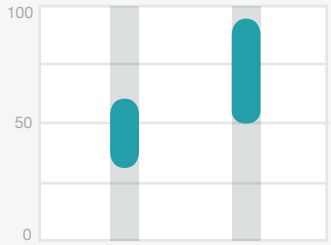
### Steps to Verify

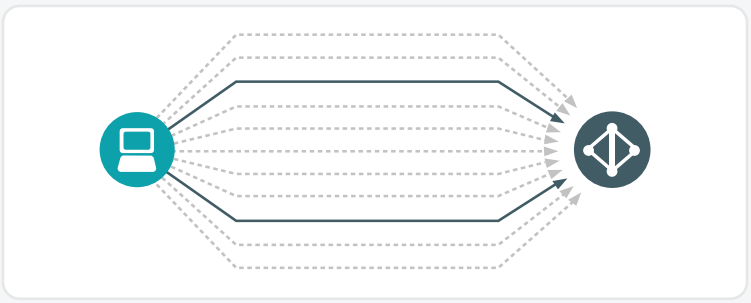
- Check to see if the detected host should be authorized for network scans
- Look at the pattern of IP addresses being scanned to determine the intent of the scan
- If the pattern appears random and distributed over time, determine which software on the host could be causing the connection requests

- Top -

# Kerberos Account Scan

## Reconnaissance



MITRE | ATT&CK®

T1087 Account Discovery

### Triggers

- A Kerberos client attempts a suspicious amount of authentication requests using a large number of user accounts with many of them failing as a result of non-existent accounts
- The threat score is driven by the number of unique non-existent accounts used in authentication attempts during the scan
- The certainty score is highest when each non-existent account is used only once and gets progressively lower the more times each non-existent account is used during the scan

### Possible Root Causes

- The internal Kerberos client is part of targeted attack which aims to spread horizontally within the network by first discovering the existence of user accounts and then stealing the account's credentials or Kerberos tickets
- A client is initiating a large number of authentication attempts with many of them failing

### Business Impact

- An account scan to a Kerberos or Active Directory server is an effective way for an attacker to determine what accounts are available inside an organization's network
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep or a port scan so attackers feel they can use it with relatively little risk of detection

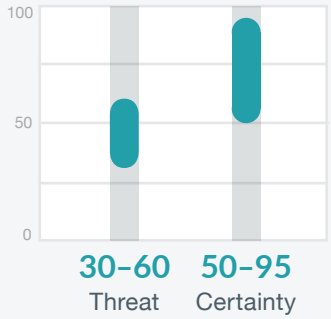
### Steps to Verify

- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this host
- Inquire whether the host should be utilizing the user accounts listed in the detection
- Verify that the host on which authentication is attempted is not a shared resource as this could generate a sufficient variety of authentications to resemble an account scan

- Top -

# Kerberos Brute-Sweep

## Reconnaissance




MITRE | ATT&CK®

T1110 Brute Force

### Triggers

- A host attempts a suspicious amount of authentication requests using a large number of user accounts with some of them failing because the accounts don't exist and others failing because the password is incorrect
- The threat score is driven by the number of failed authentications for accounts that exist
- The certainty score is driven by the regularity in the frequency of failed authentications for accounts that exist

### Possible Root Causes

- The host is part of targeted attack which aims to spread horizontally within the network by first discovering the existence of user accounts and simultaneously attempting to login to them using credentials from a common set of passwords
- The host may be a portal (a shared resource) and the authentication requests are being performed on behalf of other systems inside or outside the organization

### Business Impact

- An account brute sweep to a Kerberos or AD server is an effective way for an attacker to determine what accounts are available inside an organization's network and to simultaneously try to guess the accounts' passwords
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep, a port scan, or even the widespread use of RPCs to many hosts, so attackers feel they can use it with relatively little risk of detection

### Steps to Verify

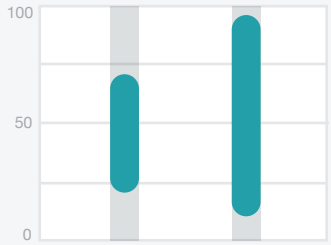
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this host
- Inquire whether the host should be utilizing the user accounts listed in the detection
- Verify that the host on which authentication is attempted is not a shared resource as this could generate a sufficient variety of authentications to resemble an account brute sweep

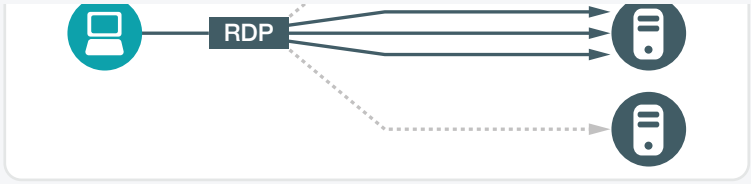
- Top -

# RDP Recon

## Reconnaissance




MITRE | ATT&CK®

T1033 System Owner/User Discovery

T1018 Remote System Discovery

## Triggers

- A host is making multiple RDP connection attempts with most of the connections failing to complete
- The connection attempts can target one or more RDP servers
- Even when a single RDP server is targeted, multiple accounts may still be involved in the encrypted part of the RDP connection setup
- The threat score is driven by the connection failure rate, which is the ratio of failed connections to total connection attempts, and the time window over which the failures are reported
- The certainty score is driven by the total number of failed connection attempts

## Possible Root Causes

- An attacker is trying to determine the existence of accounts in order to progress to the next step in the attack
- The attacker is working through a list of accounts with well-known default passwords in an attempt to find a working account/password combination
- This host is a jump server and several users are unsuccessfully attempting to RDP to other servers from it

## Business Impact

- A scan via RDP is an effective way for an attacker to determine what accounts are available inside an organization's network and which RDP servers accept logins via the accounts
- If one of the targets has not been normally accessed via RDP, the nature of the target server will provide additional guidance regarding the potential business impact
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep or a port scan so attackers feel they can use it with relatively little risk of detection

## Steps to Verify

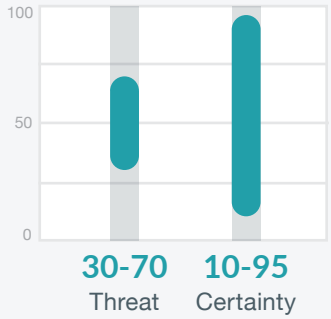
- Inquire whether the target of the RDP connection attempts should even be setup to accept RDP connections
- Inquire whether this host should be initiating the number of RDP connections to the targets listed in the detection
- If this host is a jump server, retrieve the logs of the jump server to see what upstream connections are the originators of the large number of failed RDP connections

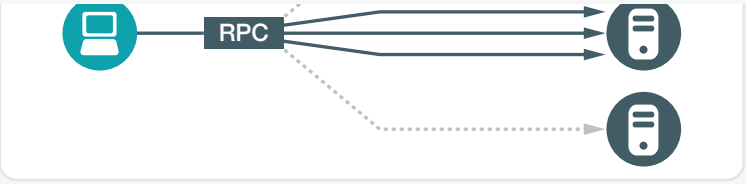
- Top -

# RPC Recon

## Reconnaissance




MITRE | ATT&CK®

T1082 System Information Discovery

T1201 Password Policy Discovery

T1087 Account Discovery

T1124 System Time Discovery

T1049 System Network Connections Discovery

T1007 System Service Discovery

T1057 Process Discovery

T1069 Permission Groups Discovery

T1033 System Owner/User Discovery

T1135 Network Share Discovery

## Triggers

- This host is making RPC calls to a large number of other hosts
- The number of hosts being contacted far exceeds the number of hosts normally contacted as observed on this network
- The threat score is driven by how commonly the UUIDs used in the RPCs are seen in reconnaissance tools and how useful they are to creating a map of the network
- The certainty score is driven by how much the number of hosts contacted exceeds locally learned normal threshold and how useful the observed UUIDs used in the RPCs are in performing reconnaissance tasks

## Possible Root Causes

- An attacker is active inside the network and is mining information from individual hosts in order to build a better map of assets in the network
- The information mined can include what accounts have recently logged into which hosts and can be used in deciding where to steal privileged account credentials
- An admin is completing authorized system management activity
- Endpoint management software installed on a central server is performing periodic system management activity
- Specialized hardware, including IoT, is utilizing RPC for peer discovery and identification

## Business Impact

- A scan of neighboring hosts' information is an effective way for an attacker to complete a detailed map of what happens where inside the target organization's network
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep or a port scan so attackers feel they can use it with relatively little risk of detection

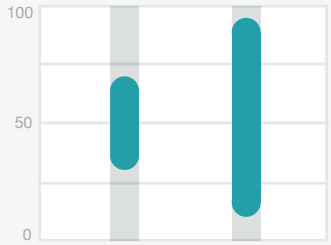
## Steps to Verify

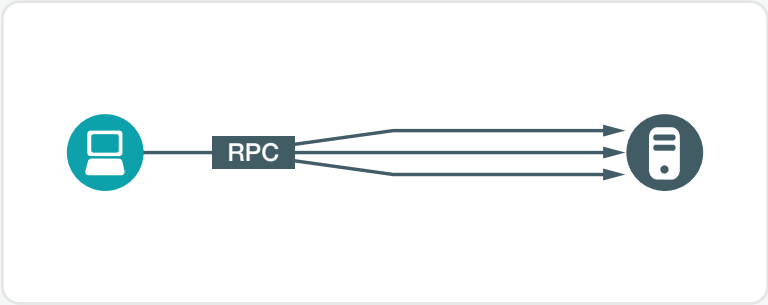
- Examine the local logs on the host making the RPC queries for a more detailed view of activity by this host
- Inquire whether the host should be contacting the hosts listed in the detection
- If the behavior continues and remains unexplained, determine which process on the internal host is establishing the connections over which the RPC requests are made; in Windows systems, this can be done using a combination of netstat and tasklist commands

- Top -

# RPC Targeted Recon

## Reconnaissance




MITRE | ATT&CK®

T1007 System Service Discovery

T1082 System Information Discovery

T1124 System Time Discovery

T1077 Windows Admin Shares

T1049 System Network Connections Discovery

T1057 Process Discovery

T1069 Permission Groups Discovery

T1087 Account Discovery

T1135 Network Share Discovery

T1201 Password Policy Discovery

## Triggers

- This host is making one or more RPC function calls indicative of information gathering to one or more other hosts
- The RPC function calls related to information gathering being made differ from ones normally made by this host or received by the target host
- The threat score is driven by the number of recon functions used during a single connection made by this host and the score is boosted if some of the functions are in the list of functions associated with known attacker techniques
- The certainty score is driven by how far the list of RPC functions used during a connection diverges from the list of RPC recon function that were previously observed in use by this host

## Possible Root Causes

- An attacker is active inside the network and is mining information from individual hosts in order to better understand the usefulness of the target host to furthering the attack
- The information mined may include recently logged on accounts, running services, available network shares, or password hashes
- An admin is completing authorized system management activity
- Endpoint management software installed on a central server is performing periodic system
- management activity
- Specialized hardware, including IoT, is utilizing RPC for peer discovery and identification

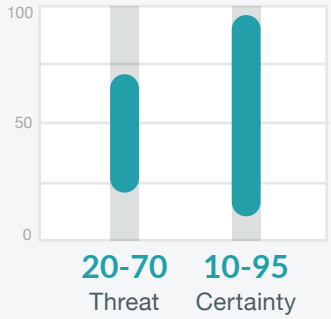
## Business Impact

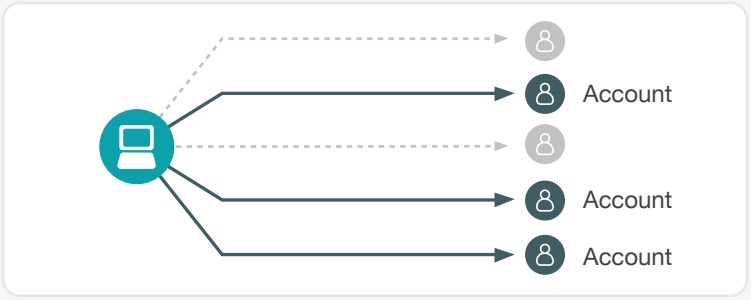
- Retrieval of a key host's information is an effective way for an attacker to further a "low-and-slow" attack on an organization's network
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep, a port scan, or even the widespread use of RPCs to many hosts, so attackers feel they can use it with relatively little risk of detection

- Top -

# SMB Account Scan

## Reconnaissance




MITRE | ATT&CK®

T1087 Account Discovery

### Triggers

- A host rapidly makes use of multiple accounts via the SMB protocol which can be used for file sharing, RPC and other activity
- The threat score is driven by the number of unique IPs or accounts scanned relative to the total number of accounts scanned
- The certainty score is driven by the number of accounts scanned

### Possible Root Causes

- An attacker is trying to determine the existence of accounts in order to progress to the next step in the attack
- The attacker is working through a list of accounts with well-known default passwords in an attempt to find a working account/password combination
- This host provides services through a portal and many users are using the portal by logging in and requesting services which require an SMB connection to fulfill

### Business Impact

- An account scan is an effective way for an attacker to determine what accounts are available inside an organization's network
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep or a port scan so attackers feel they can use it with relatively little risk of detection

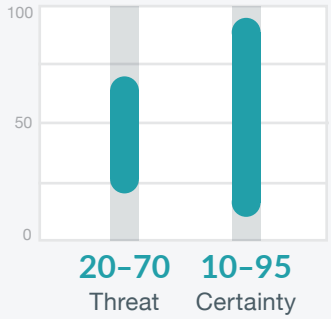
### Steps to Verify

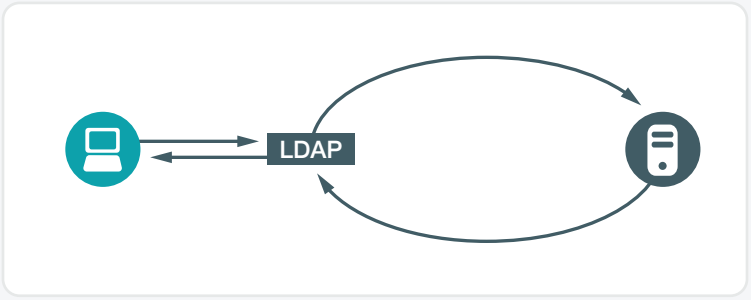
- If logs of user session activity are available, examine the logs for a more detailed view of activity by this host
- Inquire whether the host should be utilizing the user accounts listed in the detection
- Verify that the host from which authentication is attempted is not a shared resource as this could generate a sufficient variety of account usage to resemble an account scan

- Top -

# Suspicious LDAP Query

## Reconnaissance




MITRE | ATT&CK®

T1087 Account Discovery

T1018 Remote System Discovery

T1482 Domain Trust Discovery

## Triggers

- This host is querying Active Directory using the LDAP protocol in a manner that appears like reconnaissance behavior
- The LDAP queries are either unusually broad in scope or are specifically targeting accounts and groups that have names which imply administrative privilege
- The threat score is driven by the volume of returned objects across the suspicious queries observed: a high volume of returned objects leads to a higher score and a low volume leads to a lower score
- The certainty score is driven by the number of suspicious queries observed: hosts that make multiple suspicious queries will have a higher certainty

## Possible Root Causes

- An attacker is active inside the network and is mining information from one or more Active Directory servers in order to build a better map of assets in the network
- An admin is retrieving information from AD in order to complete a certain task or create a report
- An auditing application installed on this host is retrieving information from AD as part of its core functionality

## Business Impact

- A scan of information in an Active Directory server is an effective way for an attacker to determine what accounts are privileged inside an organization's network and what the names of servers and infrastructure components are
- Reconnaissance within a network is a precursor to active attacks which ultimately exposes an organization to substantial risk of data acquisition and exfiltration
- This form of reconnaissance is often a lot less noticeable than a port sweep or a port scan so attackers feel they can use it with relatively little risk of detection

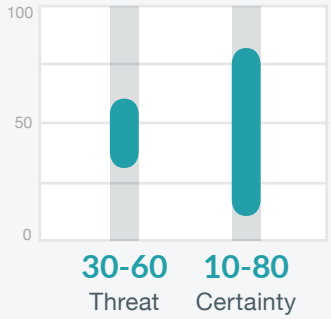
## Steps to Verify

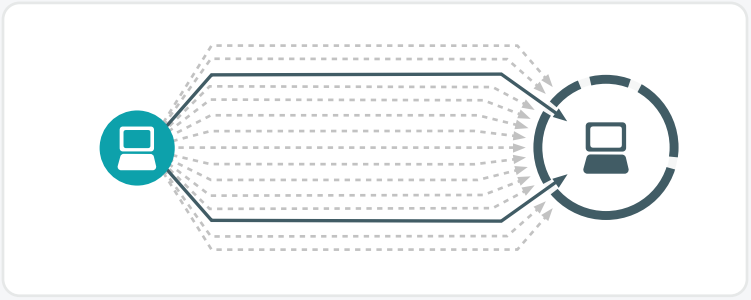
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this host
- Inquire whether the host should be making the queries listed in the detection
- If the LDAP queries continue and remain unexplained, determine which process on the internal host is making the queries; in Windows systems, this can be done using a combination of netstat and tasklist commands

- Top -

# Suspicious Port Scan

## Reconnaissance



MITRE | ATT&CK®

T1082 System Information Discovery

T1018 Remote System Discovery

T1072 Third Party Software

T1046 Network Service Scanning

T1016 System Network Configuration Discovery

## Triggers

- An internal host has attempted contact with many ports on a small number of internal IP addresses
- The threat score is driven by the number of ports being scanned
- The certainty score is driven by the number and frequency of scanning attempts

## Possible Root Causes

- An infected internal system that is part of a targeted attack is trying to locate any services which may be active on a small number of hosts by attempting connections on different ports on one or more IP addresses
- An IT-run vulnerability scanner or asset discovery system is mapping out system services on a host
- The detected host is communicating with another host using a peer-to-peer protocol and the traffic configuration on the switch is only supplying one direction of the traffic to the Vectra sensor

## Business Impact

- Reconnaissance of individual systems may represent the beginning of a targeted attack in your network
- If the system being scanned is an important or critical asset, any unauthorized scan should be treated with utmost suspicion
- Authorized reconnaissance by vulnerability scanners and asset discovery systems should be limited to a small number of hosts which can be whitelisted for this behavior using triage filters

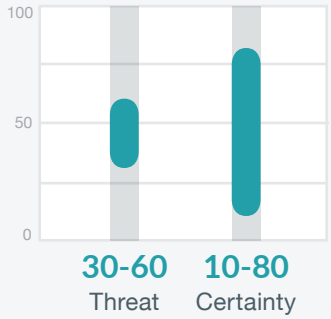
## Steps to Verify

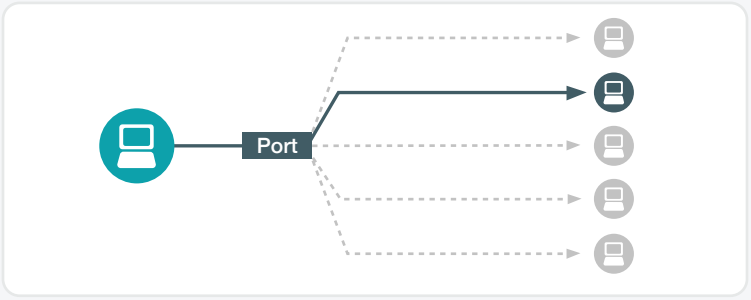
- Check to see if the detected host is authorized to perform port scans on the target hosts
- Look at the pattern of ports being scanned to try to determine what the detected host may be searching for
- If the pattern appears random and distributed over time, it is likely some form of reconnaissance and should be dealt with before the attack progresses further

- Top -

# Suspicious Port Sweep

## Reconnaissance




MITRE | ATT&CK®

T1082 System Information Discovery

T1018 Remote System Discovery

T1072 Third Party Software

T1046 Network Service Scanning

T1016 System Network Configuration Discovery

## Triggers

- An internal host has attempted contact with a large number of internal IP addresses on a small number of ports
- The threat score is lower for scattered scans and higher when a single port is scanned across many IP addresses
- The certainty score is driven by the number and frequency of scanning attempts

## Possible Root Causes

- An infected internal system that is part of a targeted attack is contacting a large number of internal IP addresses on a small number of ports to find systems which are running particular software that may be vulnerable to an attack
- An IT-run vulnerability scanner or asset discovery system is mapping out system services in your network
- A host with an unusual discovery mechanism is looking for a service on its local subnet
- Alarm equipment or IP cameras are performing large-scale scans due to misconfiguration or firmware bugs

## Business Impact

- Reconnaissance of your systems may represent the beginning of a targeted attack in your network
- Authorized reconnaissance by vulnerability scanners and asset discovery systems should be limited to a small number of hosts which can be whitelisted for this behavior using triage filters

## Steps to Verify

- Check to see if the detected host is authorized to perform port sweeps
- Look at the pattern of ports being scanned to determine the intent of the scan
- If the pattern appears random and distributed over time, it is likely some form of reconnaissance and should be dealt with before the attack progresses further

- Top -

## Steps to Verify

- Examine the local logs on the host making the RPC queries for a more detailed view of activity by this host
- Inquire whether the host should be contacting the hosts listed in the detection
- If the behavior continues and remains unexplained, determine which process on the internal
- host is establishing the connections over which the RPC requests are made; in Windows systems, this can be done using a combination of netstat and tasklist commands

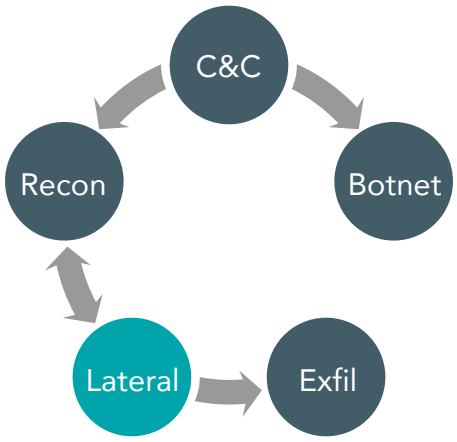


## Category

# Lateral Movement

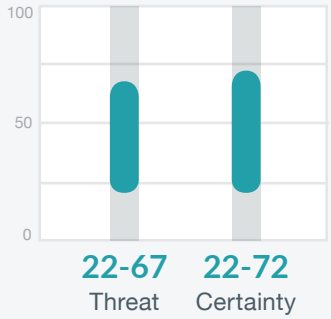
- Covers scenarios of lateral action meant to further a targeted attack
- This can involve attempts to steal account credentials or to steal data from another resource
- It can also involve compromising another host or account to make the attacker's foothold more durable or to get closer to target data

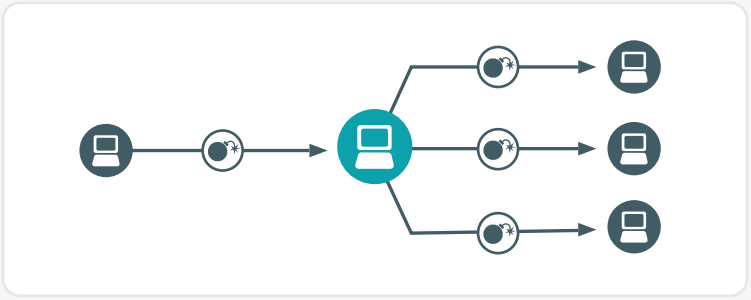



- Top -

# Automated Replication

## Lateral Movement



MITRE | ATT&CK®

T1072 Software Deployment Tools

T1210 Exploitation of Remote Services

### Triggers

- An internal host is sending very similar payloads to several internal targets
- This may be the result of an infected host sending one or more exploits to other hosts in an attempt to infect them
- The certainty score is driven by the number of targeted hosts and the detection of an upstream propagator
- The threat score is driven by the number of targeted hosts and number of different exploits, particularly exploits on different ports

### Possible Root Causes

- An infected host which is part of a botnet is trying to expand the botnet's footprint by infecting additional hosts
- An infected host which is taking part in a targeted attack is trying to spread laterally in an effort to get closer to data it wants to exfiltrate
- An agent on the host is utilizing unusual techniques to discover an available service

### Business Impact

- Internal spreading of botnet-related malware often is repeated by the next infected host, thus mimicking a computer worm and rapidly infecting all possible hosts
- A wide scale spread of botnet-related malware will incur significant remediation costs
- Lateral spread which is part of a targeted attack makes the attack more resilient and gets it closer to your crown jewels

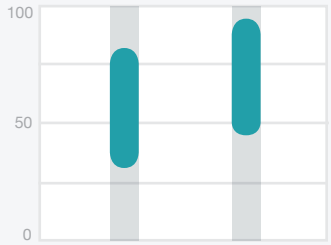
### Steps to Verify

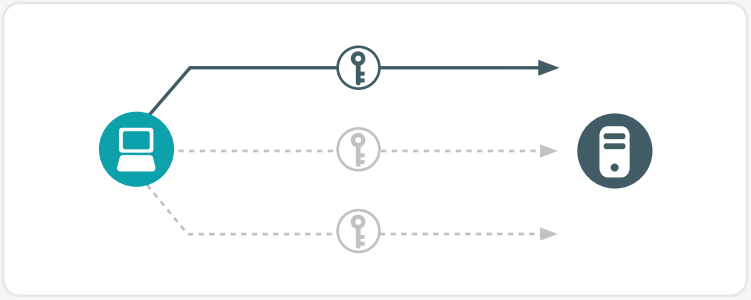
- Look at the protocol and port listed in the detection to determine what network service is being exploited
- Determine if there's any reason for this host to be communicating these services on the listed targets
- Try to ascertain what software on this host would emit the traffic being seen
- Examine the packet capture file to see if this appears to be a network discovery attempt

- Top -

# Brute-Force

## Lateral Movement



MITRE | ATT&CK®

T1110 Brute Force

### Triggers

- An internal host is making many login attempts on an internal system, behavior which is consistent with a brute-force password attack
- Such attacks can be performed via different protocols (e.g. RDP, VNC, SSH) and may also be a Heartbleed attack (e.g. memory scraping)
- The threat score is driven by the number of attempts and timing with which the attack is performed
- The certainty score is driven by the total number of sessions in the attack

### Possible Root Causes

- An infected host or a malicious insider in control of the host is trying to guess passwords on another internal system
- A misconfigured host is constantly trying to connect to one or more other internal systems

### Business Impact

- Successful harvesting of account credentials (usernames and password) of other accounts, particularly more privileged accounts, is a classic progression of a targeted attack
- Even if triggered due to a misconfiguration, the identified misconfiguration is creating significant stress on the target system and should be cleaned up

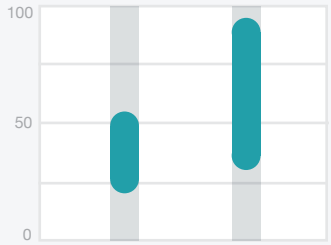
### Steps to Verify

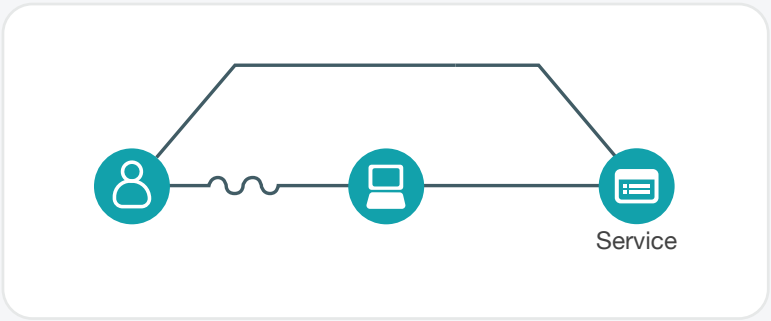
- Determine whether the internal host in question should be connecting to the target host; if not, this is likely malicious behavior
- Determine which process on the internal host is sending traffic to the internal IP address(es) and ports; in Windows systems, this can be done using a combination of netstat and tasklist commands
- Verify that the process should be running on the infected host and whether the process is configured correctly

- Top -

# Privilege Anomaly: Unusual Account on Host

## Lateral Movement




MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

T1552 Unsecured Credentials

T1555 Credentials from Password Stores

T1040 Network Sniffing

T1033 System Owner/User Discovery

T1212 Exploitation for Credential Access

T1484 Group Policy Modification

T1556 Modify Authentication Process

T1558 Steal or Forge Kerberos Tickets

T1550 Use Alternate Authentication Material

T1539 Steal Web Session Cookie

T1003 OS Credential Dumping

T1136 Create Account

## Triggers

- A privileged account is used to access a privileged service, but is doing so from a host which the account has not been observed on but where the host (using other accounts) has been seen accessing the service
- The threat score is driven by the privilege scores of the three entities (account, host, and service)
- The certainty score is driven by the observed stability of the account, host, and service clusters and the extent of the abnormality of the access and is inversely affected by the number of hosts on which the account is used

## Possible Root Causes

- The privileged account has been compromised and is being used to access a privileged service normal for the account, but from a host that the account is typically not used from; additionally, the host used for the access is itself a normal place from which to connect to the privileged server, just not with this account
- A privileged employee has borrowed another privileged user's machine (either due to their primary laptop crashing or because they are away from their desk) to perform what is otherwise normal work for the account

## Business Impact

- Lateral movement within a network involving privileged accounts, hosts, or services exposes an organization to substantial risk of data acquisition and exfiltration
- Unexplained unusual patterns of use of privileged accounts, hosts, and services are involved in almost all major breaches
- Attacks carried out by rogue insiders will often exhibit unusual patterns of use as well
- The accounts and hosts used and the services accessed provide a possible perspective on the potential business impact

- Top -

## Steps to Verify

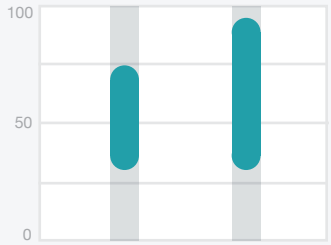
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this account since, if it has been compromised, all hosts the account has been on must be considered to be compromised as well
- Carefully inquire into whether the owner of the host in question would expect the account listed in the detection to be used on this host
- Verify that the host from which authentication is attempted is not a shared resource as this could mean that the attacker is using it as a pivot point

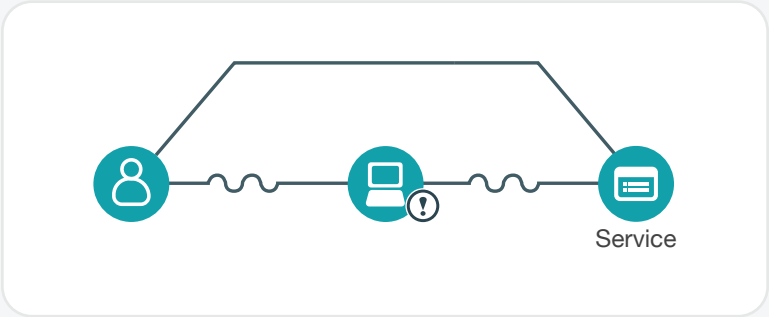


# Privilege Anomaly: Unusual Host

## Lateral Movement




MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

T1552 Unsecured Credentials

T1555 Credentials from Password Stores

T1040 Network Sniffing

T1033 System Owner/User Discovery

T1212 Exploitation for Credential Access

T1484 Group Policy Modification

T1556 Modify Authentication Process

T1558 Steal or Forge Kerberos Tickets

T1550 Use Alternate Authentication Material

T1539 Steal Web Session Cookie

T1003 OS Credential Dumping

T1136 Create Account

## Triggers

- An account is used to access a service from a host which the account is not usually on and from which the service is not usually accessed and at least the service (and likely the account) has a high privilege score OR the privilege score of the host is suspiciously low in comparison to the privilege levels of the account and service
- The threat score is driven by the privilege scores of the three entities (account, host and service) OR the closeness of the privilege score of the most privileged entity to the threshold denoting high privilege
- The certainty score is driven by the observed stability of the account, host and service clusters and the number of entities in each relationship (e.g. the number of services the account has been observed to access) and the extent of the abnormality of the host compared to the hosts typically used with the account and the service OR the number of times the anomaly is triggered

## Possible Root Causes

- The account is under the control of an attacker and is being used from an unusual host to connect to one or more services which are normal for the account but abnormal from the host
- An employee or contractor with approved access to the network who pretty consistently works from a particular set of hosts has been assigned a new host or has temporarily decided to work from another host

## Business Impact

- Lateral movement within a network involving privileged accounts, hosts or services exposes an organization to substantial risk of data acquisition and exfiltration
- Unexplained unusual patterns of use of privileged accounts, hosts and services are involved in almost all major breaches
- Attacks carried out by rogue insiders will often exhibit unusual patterns of use as well
- The accounts and hosts used and the services accessed provide a possible perspective on the potential business impact

- Top -

## Steps to Verify

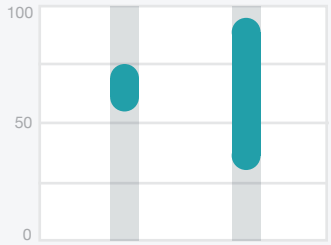
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this account across all hosts
- Carefully inquire into whether the owner of the host in question should be using the specified accounts to access the listed services
- Verify that the host from which authentication is attempted is not a shared resource as this could mean that the attacker is using it as a pivot point

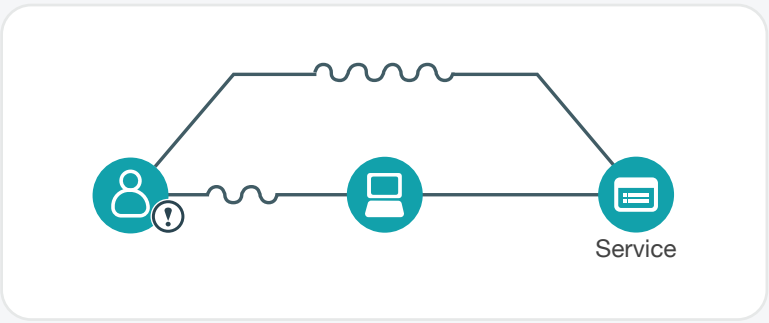


# Privilege Anomaly: Unusual Service

## Lateral Movement




MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

T1552 Unsecured Credentials

T1555 Credentials from Password Stores

T1040 Network Sniffing

T1033 System Owner/User Discovery

T1212 Exploitation for Credential Access

T1484 Group Policy Modification

T1556 Modify Authentication Process

T1558 Steal or Forge Kerberos Tickets

T1550 Use Alternate Authentication Material

T1539 Steal Web Session Cookie

T1003 OS Credential Dumping

T1136 Create Account

### Triggers

- An account which is typically used from this host is accessing a service which the account has not been observed accessing from any host and at least two entities (account and service) have high privilege scores
- The threat score is driven by the privilege scores of the three entities (account, host and service)
- The certainty score is driven by the observed stability of the account, host and service clusters and the number of entities in each relationship (e.g. the number of services the account has been observed to access) and the extent of the abnormality of the service compared to the services typically used with the account and the host

### Possible Root Causes

- The host is under the control of an attacker and the account on the host is being used to connect to one or more services which are abnormal for the account and may or may not be abnormal for the host
- An employee or contractor with approved access to the network has been assigned a new project or job which involve new privileged services which are quite abnormal given their prior role

### Business Impact

- Lateral movement within a network involving privileged accounts, hosts or services exposes an organization to substantial risk of data acquisition and exfiltration
- Unexplained unusual patterns of use of privileged accounts, hosts and services are involved in almost all major breaches
- Attacks carried out by rogue insiders will often exhibit unusual patterns of use as well
- The accounts and hosts used and the services accessed provide a possible perspective on the potential business impact

- Top -

## Steps to Verify

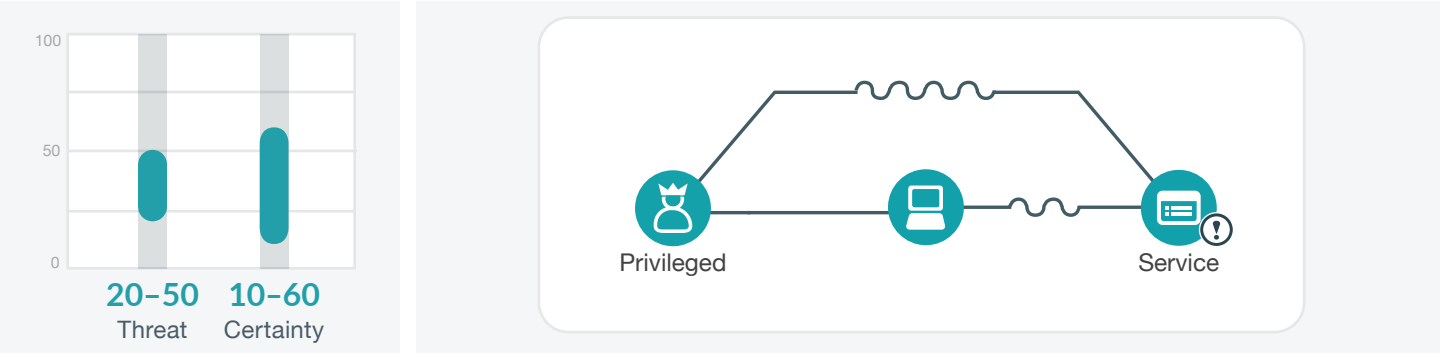
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this host and account since if the host is compromised, the account must be considered to be compromised as well
- Carefully inquire into whether the owner of the host in question should be using the specified accounts to access the listed services
- Verify that the host from which authentication is attempted is not a shared resource as this could mean that the attacker is using it as a pivot point



# Privilege Anomaly: Unusual Service - Insider

## Lateral Movement




MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

T1552 Unsecured Credentials

T1555 Credentials from Password Stores

T1040 Network Sniffing

T1033 System Owner/User Discovery

T1212 Exploitation for Credential Access

T1484 Group Policy Modification

T1556 Modify Authentication Process

T1558 Steal or Forge Kerberos Tickets

T1550 Use Alternate Authentication Material

T1539 Steal Web Session Cookie

T1003 OS Credential Dumping

T1136 Create Account

## Triggers

- An account with a low privilege score is used from a host that has a low privilege score to access a service which has a substantially higher privilege score
- The threat score is driven by the privilege scores of the three entities (account, host and service) when the service privilege is high; for medium privilege services being accessed from low privileged hosts and accounts, the threat score is driven by the degree of mismatch in the privilege scores
- The certainty score is driven by the observed stability of the account, host and service clusters and the number of entities in each relationship (e.g. the number of services the account has been observed to access) and the extent of the abnormality of the service compared to the services typically used with the account and the host; for medium privilege services being accessed from low privileged hosts and accounts, the certainty score is driven by the number of anomalous transactions observed

## Possible Root Causes

- The host is under the control of an attacker and the account on the host is being used to connect to one or more higher privileged services
- The account is under the control of an attacker and is being used from multiple hosts to connect to one or more higher privileged services
- A new admin has been hired and as the account used by the admin is new and the machine assigned to the admin is new, both have low privilege scores; when the admin then begins to perform legitimate work, detections are triggered until the privilege scores of the admin's account and host are raised based on observed activity
- A new service is being rolled out and it was initially only used by higher privileged admin accounts (and thus considered to be a high privilege service) but then release for use by a broader set of lower privileged accounts
- A rarely used service is generally accessed by higher privileged accounts, but is technically also available to lower privileged accounts is accessed by one such low privileged accounts

- Top -

## Business Impact

- Lateral movement within a network involving privileged accounts, hosts or services exposes an organization to substantial risk of data acquisition and exfiltration
- Unexplained unusual patterns of use of privileged accounts, hosts and services are involved in almost all major breaches
- Attacks carried out by rogue insiders will often exhibit unusual patterns of use as well
- The accounts and hosts used and the services accessed provide a possible perspective on the potential business impact

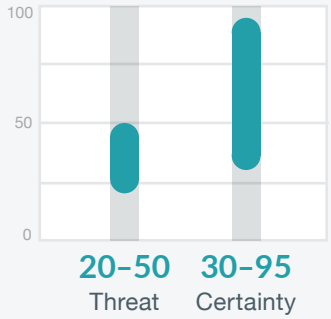
## Steps to Verify

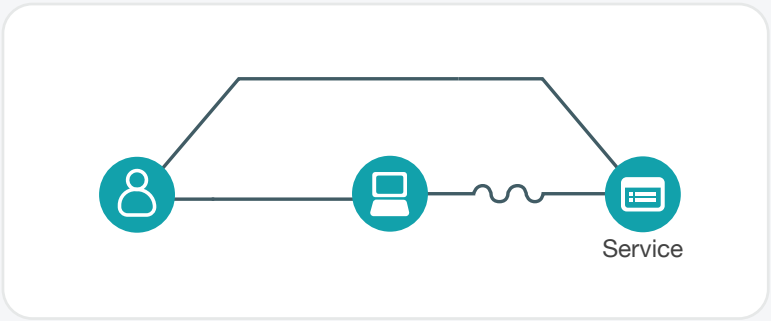
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this host and account since if the host is compromised, the account must be considered to be compromised as well
- Carefully inquire into whether the owner of the host in question should be using the specified accounts to access the listed services
- Verify that the host from which authentication is attempted is not a shared resource as this could mean that the attacker is using it as a pivot point

- Top -

# Privilege Anomaly: Unusual Service from Host

## Lateral Movement




MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

T1552 Unsecured Credentials

T1555 Credentials from Password Stores

T1040 Network Sniffing

T1033 System Owner/User Discovery

T1212 Exploitation for Credential Access

T1484 Group Policy Modification

T1556 Modify Authentication Process

T1558 Steal or Forge Kerberos Tickets

T1550 Use Alternate Authentication Material

T1539 Steal Web Session Cookie

T1003 OS Credential Dumping

T1136 Create Account

## Triggers

- A privileged account is used to access a privileged service, and is doing so from a host which the account has been observed on but where the host has not been seen accessing the service
- The threat score is driven by the privilege scores of the three entities (account, host, and service)
- The certainty score is driven by the observed stability of the account, host, and service clusters and the extent of the abnormality of the access and is inversely affected by the number of hosts on which the service is used

## Possible Root Causes

- The privileged account has been compromised and is being used to access a privileged service normal for the account, but from a host that the service is typically not accessed from; additionally, the host used for the access is itself a normal place for this account, but not a place from which this service is accessed by any account
- A privileged employee has decided to use their backup/secondary machine (either due to their primary laptop crashing or because they are away from their desk) to perform what is otherwise normal work for the account

## Business Impact

- Lateral movement within a network involving privileged accounts, hosts, or services exposes an organization to substantial risk of data acquisition and exfiltration
- Unexplained unusual patterns of use of privileged accounts, hosts, and services are involved in almost all major breaches
- Attacks carried out by rogue insiders will often exhibit unusual patterns of use as well
- The accounts and hosts used and the services accessed provide a possible perspective on the potential business impact

- Top -

## Steps to Verify

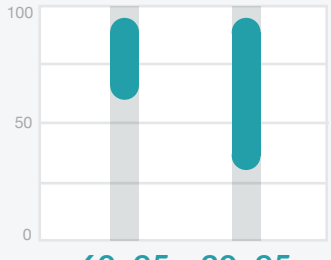
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this account since if it has been compromised, all hosts the account has been on must be considered to be compromised as well
- Verify that the host in question is a secondary machine owned by the account owner
- Verify that the host from which authentication is attempted is not a shared resource as this could mean that the attacker is using it as a pivot point

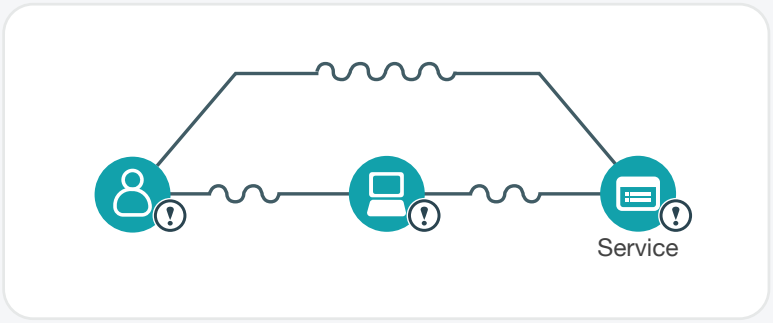


# Privilege Anomaly: Unusual Trio

## Lateral Movement




MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

T1552 Unsecured Credentials

T1555 Credentials from Password Stores

T1040 Network Sniffing

T1033 System Owner/User Discovery

T1212 Exploitation for Credential Access

T1484 Group Policy Modification

T1556 Modify Authentication Process

T1558 Steal or Forge Kerberos Tickets

T1550 Use Alternate Authentication Material

T1539 Steal Web Session Cookie

T1003 OS Credential Dumping

T1136 Create Account

## Triggers

- An account is used from a host to request access to a service where none of the pairings (account-host, account-service and host-service) are consistent with prior observed behavior and at least the service is considered privileged
- The threat score is driven by the privilege scores of the three entities (account, host and service)
- The certainty score is driven by the observed stability of the account, host and service clusters and the number of entities in each relationship (e.g. the number of services the account has been observed to access) and the extent of the abnormality of the transaction with regards to each of the three entities involved

## Possible Root Causes

- The account or host (or both) are under the control of an attacker and are being used to in a manner which is abnormal for all three entities (account, host and service) involved
- An employee or contractor with approved access to the network is attacking the organization by using their account on an unusual host or someone else's account on their host to access a service which neither the account nor the host usually connects to

## Business Impact

- Lateral movement within a network involving privileged accounts, hosts or services exposes an organization to substantial risk of data acquisition and exfiltration
- Unexplained unusual patterns of use of privileged accounts, hosts and services are involved in almost all major breaches
- Attacks carried out by rogue insiders will often exhibit unusual patterns of use as well
- The accounts and hosts used and the services accessed provide a possible perspective on the potential business impact

- Top -

## Steps to Verify

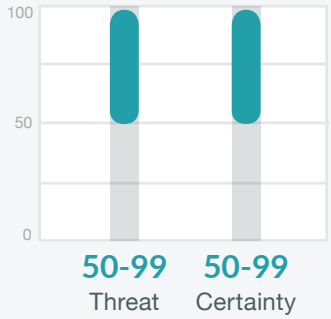
- Examine the Kerberos or Active Directory server logs for a more detailed view of activity by this host and account and requests made for the service
- Carefully inquire into whether the owner of the host in question should be using the specified accounts to access the listed services
- Verify that the host from which authentication is attempted is not a shared resource as this could mean that the attacker is using it as a pivot point

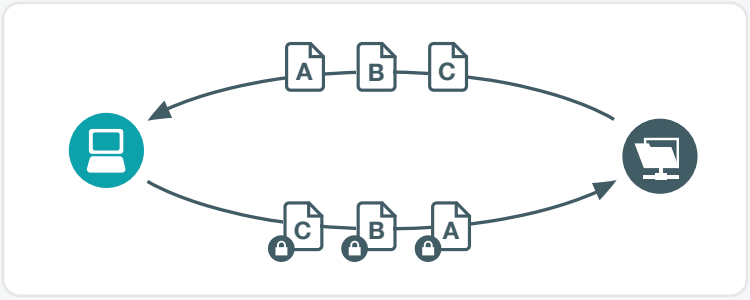


# Ransomware File Activity

## Lateral Movement




MITRE | ATT&CK®

T1486 Data Encrypted for Impact

### Triggers

- An internal host is connected to one or more file servers via the SMB protocol and is rapidly reading files and writing files of roughly the same size and with roughly the same file name
- This pattern is highly correlated with how ransomware interacts with file servers
- Given the potential for damage, the threat score for detections of this type is high
- The certainty score is driven by the volume and persistence of the observed activity

### Possible Root Causes

- The internal host is infected with a variant of ransomware
- A benign application on the host is rapidly reading files from and writing files to a networked file share
- A user is compiling a large set of source files located on a file share, causing a pattern of reading and writing files that exhibits a similar pattern

### Business Impact

- Ransomware encrypts files and transmits the encryption key to the attacker
- The attacker then attempts to extract a ransom (typically payable in an untraceable cyber currency) from the organization in return for a promise to release the encryption key which allows the files to be recovered
- Even if your organization is willing to pay the ransom, there is no guarantee that the encryption key will be provided by the attacker
- Absent the encryption key, files will have to be restored from a backup and any changes since the last backup will be lost

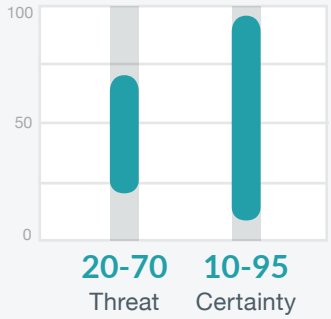
### Steps to Verify

- Examine the sample files referenced in the detection and see if the original files are missing and the files that have replaced them carry strange but similar file names or file extensions
- Check the directory in which the files reside for ransom notes with instructions on how to pay the ransom and retrieve the encryption key

- Top -

# SMB Brute-Force

## Lateral Movement




MITRE | ATT&CK®

T1110 Brute Force

### Triggers

- An internal host is utilizing the SMB protocol to make many login attempts using the same account(s), behavior which is consistent with a brute-force password attack
- Many, though not necessarily all, of these authentications are observed to fail
- The threat score is driven by the rate of login attempts
- The certainty score is driven by the overall number of login attempts

### Possible Root Causes

- An infected host or a malicious insider in control of the host is trying to guess passwords for an account on another internal system
- A misconfigured host is constantly trying to connect to one or more other internal systems using an incorrect password or trying to log into an account which no longer exists or is locked out

### Business Impact

- Successful harvesting of account credentials (usernames and passwords) of other accounts, particularly more privileged accounts, is a classic progression of a targeted attack
- Even if triggered due to a misconfiguration, the identified behavior is creating significant stress on the target system and should be cleaned up

### Steps to Verify

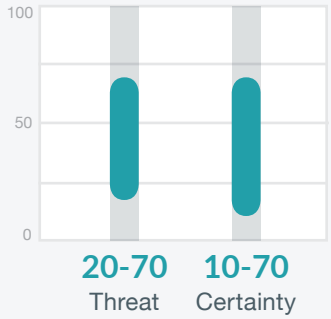
- Determine whether the internal host in question should be connecting to the target host using the indicated account(s); if not, this is likely malicious behavior
- Determine which process on the internal host is initiating the SMB requests; in Windows systems, this can be done using a combination of netstat and tasklist commands
- Verify that the process should be running on the internal host and whether the process is configured correctly

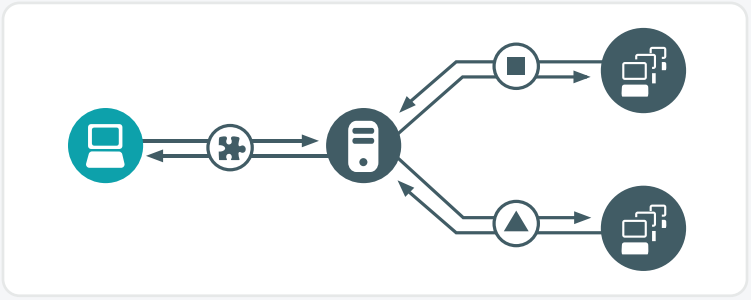
- Top -

# Shell Knocker Client

## Lateral Movement



MITRE | ATT&CK®

T1205 Traffic Signaling

### Triggers

- The host is communicating in an unusual manner with an internal server on a port that has previously shown a stable pattern for requests and responses
- The request sent to the internal server and the response received from it don't conform to any of the previously observed patterns
- The threat score is driven by either the duration of the connection between the client and the server; if the server returns a null response, the threat score is driven by the size of the client request
- The certainty score is driven by the level of dissimilarity between normal patterns of communication and the flagged communication

### Possible Root Causes

- The server has been compromised and the port has been hijacked to enable communication to the compromised part of the system without requiring a new port to be utilized for the communication
- The client or the server has been recently upgraded and the pattern of use on the server port has changed
- This client has an unusual configuration in that it communicates with the port on the server in a manner unlike all the other observed communication on that port

### Business Impact

- Port hijacking is a technique attackers use to enable communication to a compromised server without raising alarms which may go off when a new port is used on an existing server
- Compromised servers are often more valuable than compromised laptops as they remain on the network at all times and are often located in the data center where most of an organization's important data resides

- Top -

## Steps to Verify

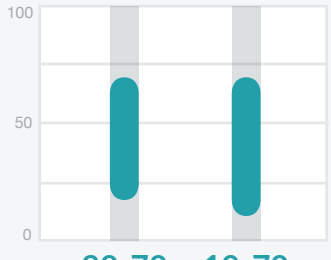
- See if the pattern of the flagged request and response represent acceptable deviations from the normal patterns or are significant departures such as binary data in an otherwise character-based protocol
- Inquire whether the software which emitted the request on this host has recently been updated as this may cause detections for a short period of time after the update
- Inquire whether the software on the server which responded to the request has recently been updated as this may cause detections for a short period of time after the update
- If the changed pattern remains unexplained, boot the client and server using a known good image on a USB device, then mount the local drive and scan it for signs of compromise

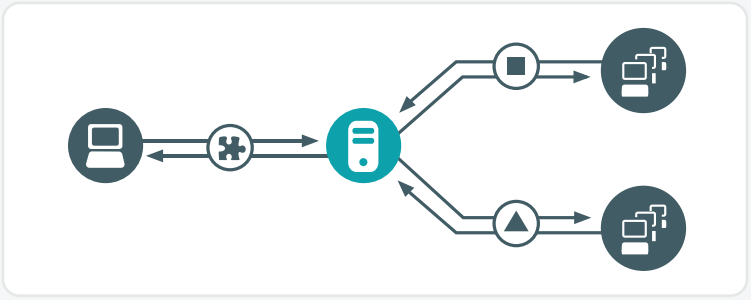


# Shell Knocker Server

## Lateral Movement



MITRE | ATT&CK®

T1205 Traffic Signaling

### Triggers

- The server is communicating in an unusual manner with an internal client on a port that has previously shown a stable pattern for requests and responses
- The request received by the server and the response sent by it don't conform to any of the previously observed patterns
- The threat score is driven by either the duration of the connection between the client and the server; if the server returns a null response, the threat score is driven by the size of the client request
- The certainty score is driven by the level of dissimilarity between normal patterns of communication and the flagged communication

### Possible Root Causes

- The server has been compromised and the port has been hijacked to enable communication to the compromised part of the system without requiring a new port to be utilized for the communication
- The client or the server has been recently upgraded and the pattern of use on the server port has changed
- The client which triggered the detection has an unusual configuration in that it communicates with the port on this server in a manner unlike all the other observed communication on the port

### Business Impact

- Port hijacking is a technique attackers use to enable communication to a compromised server without raising alarms which may go off when a new port is used on an existing server
- Compromised servers are often more valuable than compromised laptops as they remain on the network at all times and are often located in the data center where most of an organization's important data resides

- Top -

## Steps to Verify

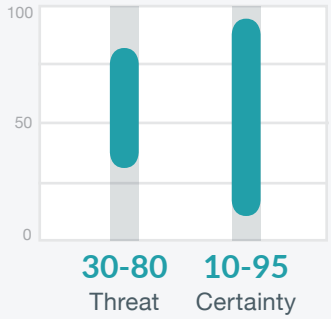
- See if the pattern of the flagged request and response represent acceptable deviations from the normal patterns or are significant departures such as binary data in an otherwise character-based protocol
- Inquire whether the software which emitted the request on the client has recently been updated as this may cause detections for a short period of time after the update
- Inquire whether the software on this server which responded to the request has recently been updated as this may cause detections for a short period of time after the update
- This type of backdoor is most likely to be in a kernel module, so produce a list of all installed kernel modules and verify against list of good known kernel modules
- If the changed pattern remains unexplained, boot the client and server using a known good image on a USB device, then mount the local drive and scan it for signs of compromise

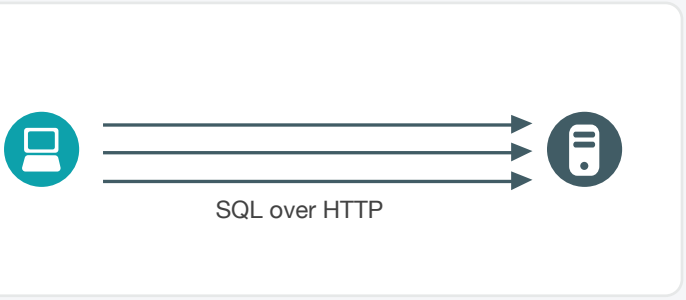


# SQL Injection Activity

## Lateral Movement




MITRE | ATT&CK®

T1190 Exploit Public Facing Application

### Triggers

- An internal host sends requests to a Web server and embeds SQL fragments into HTTP Post data or the URL to gain access to the backend database; the requests appear machine-generated due to the large volume and rate of arrival
- The threat score is driven by the volume of HTTP requests containing SQL fragments and the size of the returned data
- The certainty score is driven by the number of requests sent and their classification as SQL fragments

### Possible Root Causes

- An infected system that is part of targeted attack is looking for vulnerabilities in an internal Web app through which to access the database integrated into it, or is harvesting information for later exfiltration
- An IT-operated vulnerability scanner is scanning for Web app vulnerabilities
- A software application on the host uses the unsafe practice of passing passes SQL statements in HTTP Post data or in a URL

### Business Impact

- Probing and potentially exploiting an internal Web application's vulnerabilities can be a prelude to a targeted attack getting access to data and then exfiltrating it
- Application software that passes SQL statements in HTTP Post data or as part of a URL may be vulnerable to attackers as they can send very different input than the application writer expects

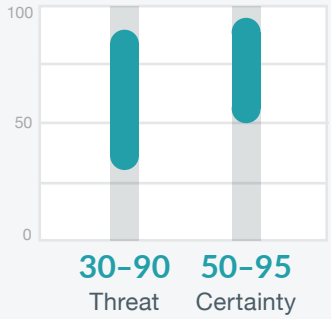
### Steps to Verify

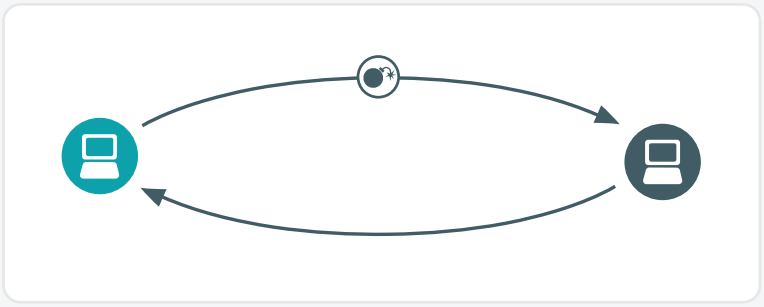
- Verify systems identified as the source of SQL injection attacks should be communicating directly with SQL servers; download the PCAP to see the entire HTTP Post data or the URL to determine if its behaving as expected
- If this pattern is coming from neither an IT-run vulnerability scanner nor from software that by design sends SQL statements in requests, check for presence of malware on the host

- Top -

# Stage Loader

## Lateral Movement



MITRE | ATT&CK®

T1210 Exploitation of Remote Services

T1570 Lateral Tool Transfer

## Triggers

- The detection results from the observation of two closed sessions where an internal host is attacking another internal host by uploading a payload which causes the destination host to connect back to the initial host to download additional stages of software
- The threat score is higher if the count of connections made back to the initial host's callback port is low; it is also higher the smaller the time-gap is between the initial payload upload connection and the connection made to download the stage; and callback ports of 4444 or 1337 (commonly used in post-exploit command and control) further boosts the threat score
- The certainty score is driven by the similarity of the exchange to a model trained on malicious samples—the model includes bytes sent, bytes received, time-gap between initial payload and callback, protocol-difference between the two connections, and the durations for both first and second connection

## Possible Root Causes

- The initial host is transmitting an exploit to a destination host which runs a stage loader and connects back to the initial host to load the rest of the malware necessary for the attacker to make progress toward their goal
- Bidirectional transaction-based protocols where commands or requests are issued over one port/protocol and data is returned shortly thereafter over another port/protocol can also trigger the detection—common protocols which behave in this manner include the WinRM 2.0 Framework (used for Windows remote management), PostgreSQL, and SNPP (Simple Network Paging Protocol)

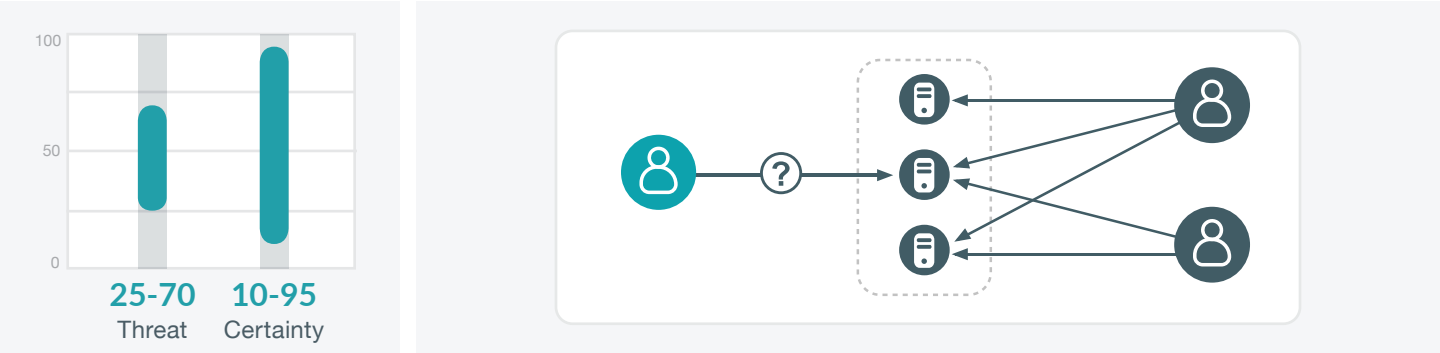
## Business Impact

- Lateral movement within a network expands an attacker's footprint and exposes an organization to substantial risk of data acquisition and exfiltration
- Lateral movement through exploits or leveraging stolen credentials is involved in almost all high-profile breaches
- The destination host which is attacked provides a possible perspective on the potential business impact

- Top -

# Suspicious Admin

## Lateral Movement




MITRE | ATT&CK®

T1003 OS Credential Dumping

T1078 Valid Accounts

T1212 Exploitation For Credential Access

T1552 Unsecure Credentials

T1555 Credentials From Password Stores

T1021 Remote Services

T1563 Remote Service Session Hijacking

## Triggers

- The host is using protocols correlated with administrative activity (RDP, SSH, IPMI, iDRAC, etc.) in ways which are considered suspicious
- The threat score is driven by the number of other administrative connections made by this host
- The certainty score is driven by the number of other recognized administrators of the target systems using the same administrative protocol

## Possible Root Causes

- The host has begun using an administrative protocol to connect to a system for which one or more other hosts have already been observed to be regular administrators using the same protocol
- Administrative connections via a particular administrative protocol to a system which has no known regular administrators using that protocol will not result in a detection
- Administrative connections to a system which has a known regular administrator host using the chosen protocol will also not result in a detection if there is significant overlap in administrative connections to other systems between this host and the other known administrator host
- If such an administrative connection recurs over a period of several days, it is considered normal and no longer will trigger a detection
- The detection may be benign when it involves a host assigned to a new employee authorized to administrate the target systems or when the role of the employee has undergone a significant change

## Business Impact

- Administrative protocols are a primary tool for attackers to move laterally inside a network in which they have already established a toehold
- Given that administrative connections are typically used in conjunction with administrative credentials, the attacker may have almost unconstrained access to systems and data that are the organization's key assets
- Unexpected and unexplained administrative connections represent a huge potential risk in the lifecycle of a major breach

- Top -

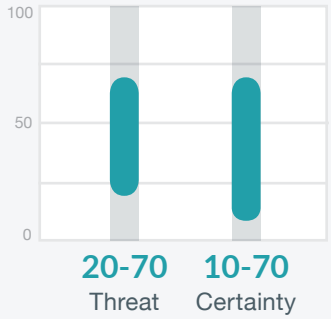
## Steps to Verify

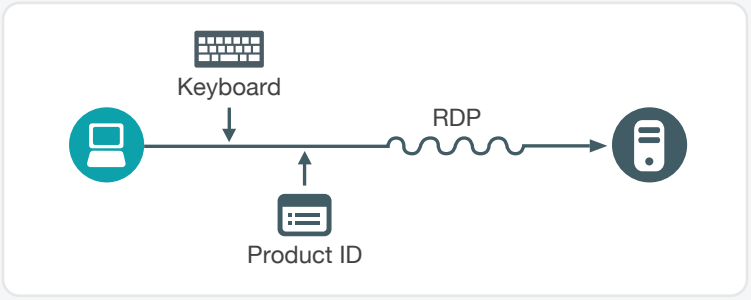
- Verify whether the host belongs to an employee whose job function requires administrative access to other systems
- Verify whether the employee who has been assigned the host should be using the particular administrative protocol to administer the identified system
- Inquire whether the owner of the host actually initiated the administrative connection in order to determine whether the host has been compromised
- Check the logs on the administered target for the creation of new accounts, the launch of abnormal processes and the modification of registry key
- If employee associated with this host was not the originator of the admin session, reset all domain and local admin credentials belonging to the employee across the local machine and the network
- If the credentials of the employee whose machine was compromised had domain administrative privileges, the secret key of the domain controller may have been compromised and may need to be reset – search for “krbtgt account password change” to find instructions on how to do this
- Verify that the host from which the administrative connection was originated is a jump system as this may mean that the originator of the administrative connection is an upstream host which connected to the jump system

- Top -

# Suspicious Remote Desktop

## Lateral Movement




MITRE | ATT&CK®

T1003 OS Credential Dumping

T1078 Valid Accounts

T1212 Exploitation For Credential Access

T1552 Unsecure Credentials

T1555 Credentials From Password Stores

T1021 Remote Services

## Triggers

- A host connects to an internal RDP server with a keyboard layout or a product ID different than the one usually seen in conjunction with the specified RDP client token
- A host connects to an internal RDP server with a keyboard layout that is unusual for that RDP server
- The threat score is driven by the types of anomalies observed with keyboard anomalies scoring higher and product ID anomalies scoring lower
- The certainty score is driven by the duration an RDP client token or server has been monitored for construction of the baseline with a higher quality baseline resulting in a higher certainty
- A host connects to an internal RDP server with a keyboard layout that is different from those usually seen on the network

## Possible Root Causes

- An external foreign attacker who has taken over control of an internal host is using it with unusual keyboard layouts to connect to RDP servers to move laterally in the network
- An external attacker who has taken over control of an internal host has brought along their own RDP stack and is using it to connect to internal RDP servers to move laterally in the network
- An employee has switched to their native keyboard layout while accessing an RDP server
- An employee has installed a new RDP client with a new product ID and is accessing an RDP server

## Business Impact

- Along with SSH, RDP is one of the most useful lateral movement protocols for attackers as it allows remote control of the target as well as the copying of files across the connection
- This type of control and data acquisition may happen well in advance of actual exfiltration attempts and represents a great chance to head off attacks before any substantial damage occurs

- Top -

## Steps to Verify

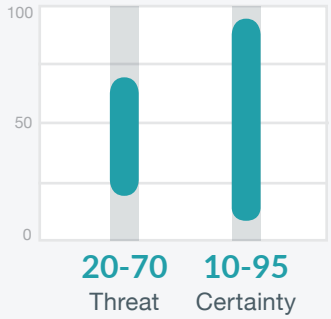
- For keyboard layout anomalies, inquire whether the user of the internal host is fluent in the language of the flagged keyboard layout
- For an RDP product id anomaly, inquire whether IT has installed new RDP client software or ask the user of the host whether they have done so

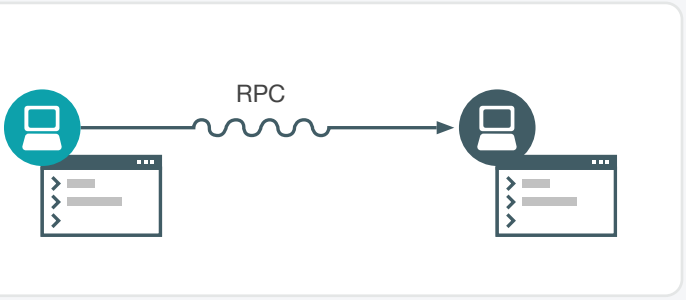


# Suspicious Remote Execution

## Lateral Movement




MITRE | ATT&CK®

T1569 System Services

T1021 Remote Services

T1047 Windows Management Instrumentation

T1053 Scheduled Task/Job

T1078 Valid Accounts

T1570 Lateral Tool Transfer

T1571 Non-Standard Port

T1572 Protocol Tunneling

### Triggers

- An internal host is utilizing the SMB or DCE RPC protocol to make one or more suspicious RPC requests and referencing functions related to remote execution of code
- The combination of source host, destination host, user account and RPC UUID has not previously been observed
- The threat score is driven by the number of destinations that received suspicious RPC requests
- The certainty score is lower if the RPC UUID is broadly used and higher when it is not commonly used

### Possible Root Causes

- An infected host, a malicious insider or a red team participant who is in control of the host is trying to spread laterally by executing code on systems to which it has connected
- Newly installed software or software that is infrequently used is legitimately making use of remote execution RPCs; this behavior is relatively common for system management software

### Business Impact

- Lateral movement via remote execution is a key element of many different attacks and the SMB channel allows both for the copying of executables and the use of RPCs to execute them
- Even systems which are permitted to perform remote execution should be monitored because those systems are the most valuable for an attacker to compromise

- Top -

## Steps to Verify

- Determine whether the internal host in question should be using remote execution RPCs
- Determine whether the user account flagged in the detection is one with administrative privileges and whether that administrator logged into the host which triggered the detection
- Determine whether the user account flagged in the detection is a service account associated with a specific product and whether that product should be running on the host which triggered the detection
- Determine which process on the internal host is initiating the SMB requests that includes the RPC request; in Windows systems, this can be done using a combination of netstat and tasklist commands
- Verify that the process should be running on the internal host and whether the process is configured correctly



# Threat Intelligence Match

## Lateral Movement


### Triggers

- An internal host has initiated communications with another internal host and the connection has met criteria specified in one or more configured threat feeds
- The threat score is driven by the combination of the indicator type in the STIX file (with watchlist and anonymization being lowest, malware artifacts being medium and C2 channel and exfiltration being highest) and the quantity of data sent and received on the flagged connections
- The certainty score is specified as part of the threat feed configuration and ranges from low (30) to medium (60) and high (90)

### Possible Root Causes

- A host includes malware which is initiating the connection that triggered the detection
- A user on the host manually initiated the connection which triggered the detection

### Business Impact

- The internal connection may be used by the originating host to compromise the target host or to maintain communication with a previously compromised host
- If the connection is to a target host which contains important data, this may represent an attempt to acquire data for later exfiltration
- The threat intel feed may have included additional context tied to the specific criteria that the connection met
- Lateral movement and data acquisition are present in almost all large-scale breaches

### Steps to Verify

- Refer to the information accompanying your threat feed as it may include verification and remediation instructions
- Determine which process on the internal host is sending the traffic which was flagged; in Windows systems, this can be done using a combination of netstat and tasklist commands
- Check if a user has knowingly installed remote access software and decide whether the resulting risk is acceptable
- Scan the computer for known malware and potentially reimage it, noting that some infections leave no trace on disk and reside entirely in memory

- Top -

## Steps to Verify

- Determine whether there is any reason for the two hosts involved in a stage loading sequence to be communicating with each other
- Check to see whether any connections between the initial and destination host (in either direction) persist after the stage loading sequence
- Run all available endpoint checks on both the initial and the destination host to check for unwanted malware, but realize that fileless malware will typically escape detection

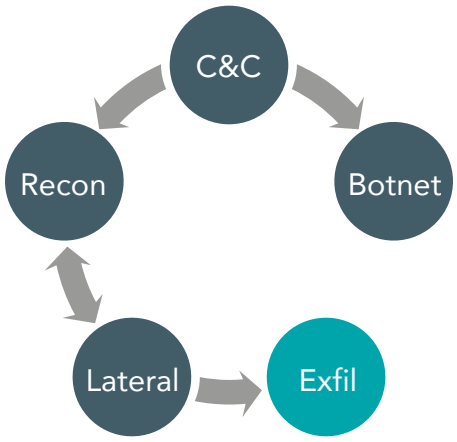


## Category

# Exfiltration

- Covers scenarios where data is being sent outside or collected in a way meant to hide the data transfer
- While data is constantly being sent out of the network or cloud environment, it usually does not involve the use of techniques meant to hide the transfer
- The host or account transmitting the data, where it is transmitting the data, the amount of data and the technique used to send it all provide indicators of exfiltration

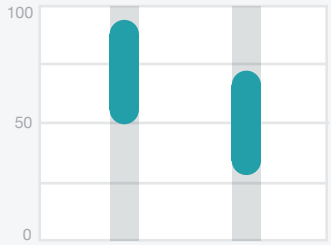


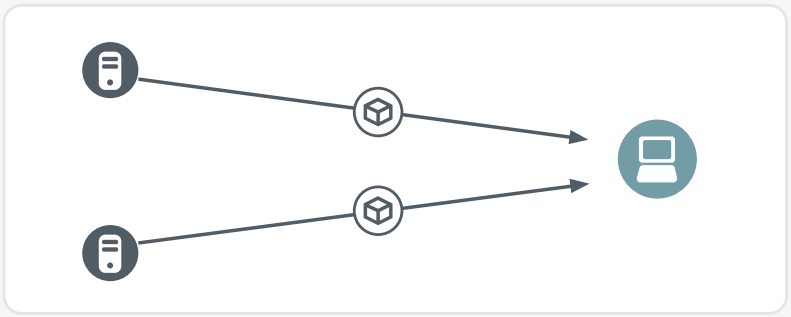

- Top -

# Data Gathering

## Exfiltration



MITRE | ATT&CK®

T1213 Data From Information Repositories

T1074 Data Staged

T1119 Automated Collection Alternative Protocol

T1039 Data from Network Shared Drive

### Triggers

- Pre-exfiltration behaviors have been observed on a host that has received abnormally high amounts of data from one or more hosts within a short period of time.
- The certainty score is based on a combination of how abnormal the data gathered volume and the relative data gathered versus data sent volume is from the host's baselines.
- The threat score is based on the total volume of data gathered and the number of hosts from which data was gathered from.

### Possible Root Causes

- An attacker has pivoted to a host to use for dumping/staging data prior to exfiltrating, likely taking advantage of the trusted nature of this host to bypass security controls and evade detection.
- A malicious insider is collecting data they intend to steal from a position of trust.
- A user has joined a new team, changed organizational roles, or otherwise been given reason to significantly depart from their typical data access and retrieval activities.
- An application has been observed on an unusual or infrequent backup or update cycle.

### Business Impact

- Failure to identify and respond to pre-exfiltration activities in an organization increases the likelihood of data loss.
- When successful, data exfiltration places an organization at the risk of the loss of intellectual property, financial data, or other regulated or sensitive data sources.

### Steps to Verify

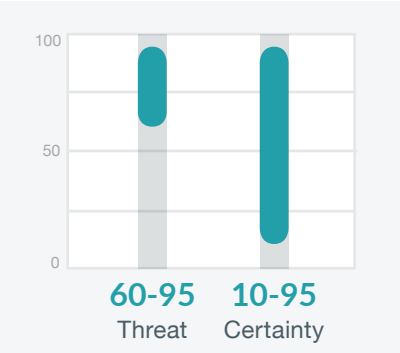
- Verify if the data gathered supports valid and authorized business activities.
- Investigate the host and associated accounts for other signs of compromise.

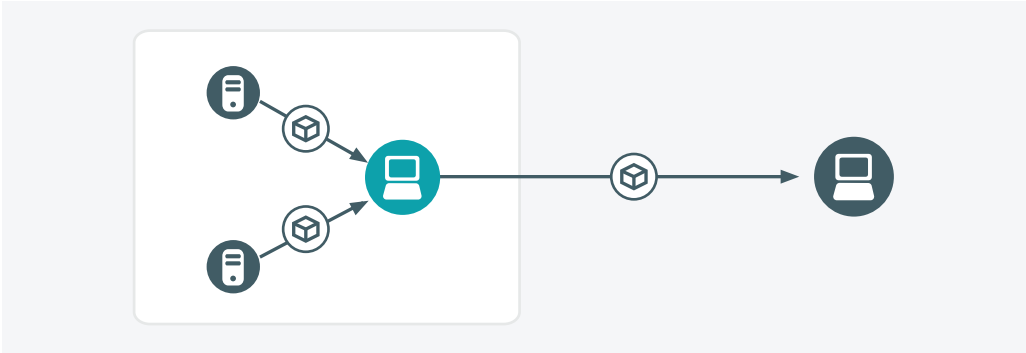
- Top -

# Data Smuggler

## Exfiltration



MITRE | ATT&CK®

T1041 Exfiltration Over C2 Channel

T1213 Data From Information Repositories

T1560 Archive Collected Data

T1074 Data Staged

T1048 Exfiltration Over Alternative Protocol

T1020 Automated Exfiltration

T1030 Data Transfer Size Limits

T1567 Exfiltration Over Web Service

### Triggers

- An internal host is acquiring a large amount of data from one or more internal servers and is subsequently sending a significant amount of data to an external system
- The threat score is driven by the amount of data transmitted
- The certainty score is driven by the relationship between the time and size of the data acquired and the time and size of the data sent

### Possible Root Causes

- A host infected with malware as part of a targeted attack or a malicious insider may be acquiring and exfiltrating company data
- While acquiring and transmitting a large quantity of data to the outside within a short period of time may be pure coincidence, the outbound data transfer is significant enough to warrant further examination

### Business Impact

- The detection signals possible exfiltration of company data
- The internal servers from which the data was retrieved provides some indication of the data which was acquired; if those servers contain valuable information and the external service to which data was uploaded is not an IT- sanctioned service, the potential business risk is high

### Steps to Verify

- Decide whether this may be a malicious insider or an infected host
- If the signs point to an infected host, contact the user to inquire if they initiated the uploading behavior in question
- For potential malicious insiders, perform a complete analysis of recent behavior
- Look up the external system IP addresses and domain names on sites that maintain reputation lists as this may provide a clear indication that the internal host is infected; such lookups are supported directly within the UI

- Top -

# Hidden DNS Tunnel

## Exfiltration


MITRE | ATT&CK®

T1005 Data from Local System

T1115 Clipboard Data

T1071 Application Layer Protocol

T1125 Video Capture

T1113 Screen Capture

T1572 Protocol Tunneling

T1123 Audio Capture

T1041 Exfiltration Over C2 Channel

## Triggers

- An internal host is communicating with an outside IP using DNS where another protocol is running over the top of the DNS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal DNS traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the distinctness of the names being looked up, with more distinctness resulting in higher certainty

## Possible Root Causes

- A targeted attack may use hidden tunnels to hide exfiltration activity
- A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible
- Intentionally installed software is using a hidden tunnel to bypass expected firewall rules

## Business Impact

- The use of a hidden tunnel by some software may be benign, but it represents significant risk as the intention is to bypass security controls
- Hidden tunnels used as part of a targeted attack are meant to slip by your perimeter security controls and indicate a sophisticated attacker
- Hidden tunnels are rarely used by botnets, though more sophisticated bot herders with more ambitious goals may utilize them

## Steps to Verify

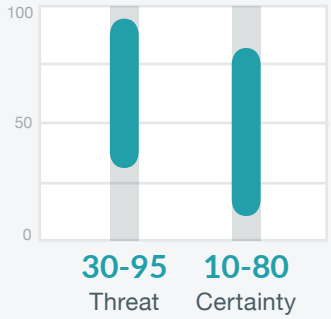
- Check to see if the destination domain of the tunnel is an entity you trust for your network
- Ask the user of the host whether they are using hidden tunnel software for any purpose
- Before removing the offending software via antivirus or reimaging, take a memory snapshot for future analysis of the incident
- If the behavior reappears shortly after a reimaging, this may be a hardware/BIOS tunnel

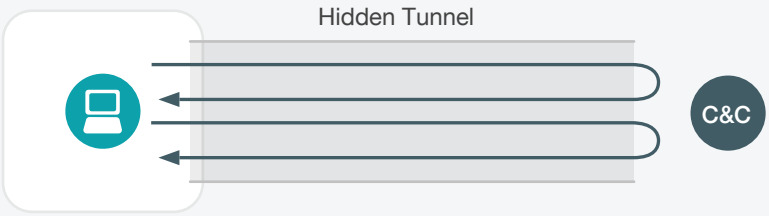
- Top -

# Hidden HTTP Tunnel

## Exfiltration




MITRE | ATT&CK®

T1005 Data from Local System

T1115 Clipboard Data

T1071 Application Layer Protocol

T1125 Video Capture

T1113 Screen Capture

T1572 Protocol Tunneling

T1123 Audio Capture

T1041 Exfiltration Over C2 Channel

### Triggers

- An internal host is communicating with an outside IP using HTTP where another protocol is running over the top of the HTTP sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal Web traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions

### Possible Root Causes

- A targeted attack may use hidden tunnels to hide exfiltration activity
- A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible
- Intentionally installed software is using a hidden tunnel to bypass expected firewall rules

### Business Impact

- The use of a hidden tunnel by some software may be benign, but it represents significant risk as the intention is to bypass security controls
- Hidden tunnels used as part of a targeted attack are meant to slip by your perimeter security controls and indicate a sophisticated attacker
- Hidden tunnels are rarely used by botnets, though more sophisticated bot herders with more ambitious goals may utilize them

### Steps to Verify

- Check to see if the destination IP address or domain of the tunnel is an entity you trust for your network
- Ask the user of the host whether they are using hidden tunnel software for any purpose
- Before removing the offending software via antivirus or reimaging, take a memory snapshot for future analysis of the incident
- If the behavior reappears shortly after a reimaging, this may be a hardware/BIOS tunnel

- Top -

# Hidden HTTPS Tunnel

## Exfiltration


MITRE | ATT&CK®

T1005 Data from Local System

T1115 Clipboard Data

T1071 Application Layer Protocol

T1125 Video Capture

T1113 Screen Capture

T1572 Protocol Tunneling

T1123 Audio Capture

T1041 Exfiltration Over C2 Channel

## Triggers

- An internal host is communicating with an outside IP using HTTPS where another protocol is running over the top of the HTTPS sessions
- This represents a hidden tunnel involving one long session or multiple shorter sessions over a longer period of time mimicking normal encrypted Web traffic
- When it can be determined whether the tunneling software is console-based or driven via a graphical user interface, that indicator will be included in the detection
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the combination of the persistence of the connection(s) and the degree to which the observed volume and timing of requests matches up with training samples

## Possible Root Causes

- A targeted attack may use hidden tunnels over SSL on port 443 to hide exfiltration activity
- A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible
- Intentionally installed software is using a hidden tunnel to bypass expected firewall rules

## Business Impact

- The use of a hidden tunnel by some software may be benign, but it represents significant risk as the intention is to bypass security controls
- Hidden tunnels used as part of a targeted attack are meant to slip by your perimeter security controls and indicate a sophisticated attacker
- Hidden tunnels are rarely used by botnets, though more sophisticated bot herders with more ambitious goals may utilize them

## Steps to Verify

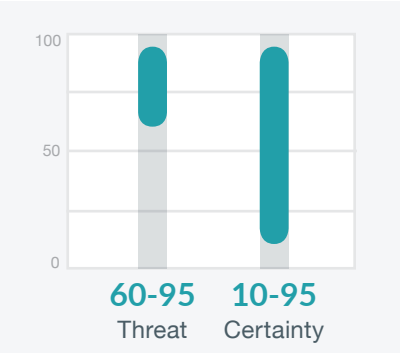
- Check to see if the destination IP or domain of the tunnel is an entity you trust for your network
- Ask the user of the host whether they are using hidden tunnel software for any purpose
- Before removing the offending software via antivirus or reimaging, take a memory snapshot for future analysis of the incident
- If the behavior reappears shortly after a reimaging, this may be a hardware/BIOS tunnel

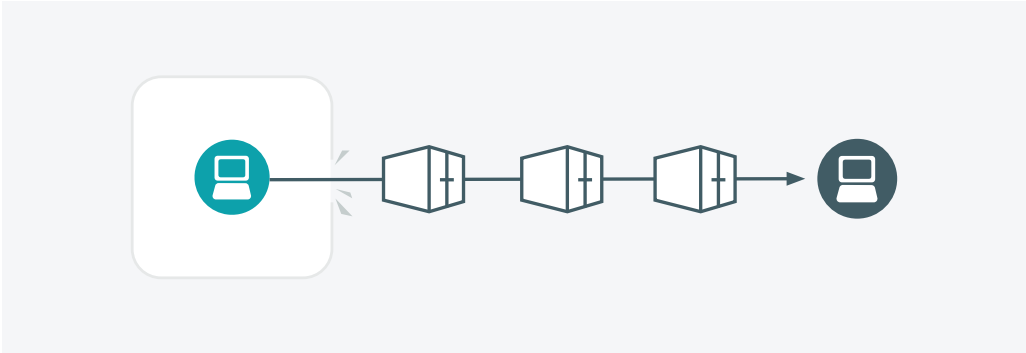
- Top -

# Smash and Grab

## Exfiltration



MITRE | ATT&CK®

T1041 Exfiltration Over C2 Channel

T1213 Data From Information Repositories

T1560 Archive Collected Data

T1029 Scheduled Transfer

T1119 Automated Collection

T1048 Exfiltration Over Alternative Protocol

T1020 Automated Exfiltration

T1030 Data Transfer Size Limits

T1567 Exfiltration Over Web Service

### Triggers

- A host transmits unusually large volumes of data to destinations which are not considered normal for this network
- The threat score is driven by the number of IPs the destination domain maps to and if this host is on a public IP also takes into account whether the destination is in another country
- The certainty score is driven by the rate of data being exfiltrated

### Possible Root Causes

- An attacker is rapidly exfiltrating large volumes of data from your network
- The host is sending large volumes of data to destinations that have not been previously used for large data transfers

### Business Impact

- The detection signals possible exfiltration of company data
- The host from which the data was sent, the destination to which the data was sent and the volume of data transmitted may provide some clues to what data was transmitted
- If the external service to which data was uploaded is not an IT-sanctioned service, the potential business risk is high

### Steps to Verify

- Check to see if the destination IP or domain to which data was moved is an entity you trust for your network
- Ask the user of the host whether they have any knowledge of the data transfer
- If the data transfer is unexplained and your endpoint security solution logs such things, determine what software on the host was responsible for the data transfer

- Top -

# Threat Intelligence Match

## Exfiltration


### Triggers

- An internal host is connecting to an external system and the connection has met criteria specified in one or more configured threat feeds
- The threat score is driven by the combination of the indicator type in the STIX file (with watchlist and anonymization being lowest, malware artifacts being medium, and C2 channel and exfiltration being highest) and the quantity of data transmitted on the flagged connections
- The certainty score is specified as part of the threat feed configuration and ranges from low (30) to medium (60) and high (90)

### Possible Root Causes

- A host includes malware which is initiating the connection that triggered the detection
- A user on the host manually initiated the connection which triggered the detection

### Business Impact

- The detection signals exfiltration of company data
- The host from which the data was sent, the destination to which the data was sent and the volume of data transmitted may provide some clues to what data was transmitted
- The threat intel feed may have included additional context tied to the specific criteria that the connection met
- If the external service to which data was uploaded is not an IT-sanctioned service, the potential business risk is high

### Steps to Verify

- Refer to the information accompanying your threat feed as it may include verification and remediation instructions
- Determine which process on the internal host is sending the traffic which was flagged; in Windows systems, this can be done using a combination of netstat and tasklist commands
- Check if a user has knowingly installed remote access software and decide whether the resulting risk is acceptable
- Scan the computer for known malware and potentially reimage it, noting that some infections leave no trace on disk and reside entirely in memory

- Top -

## Category
# Info

- Reports on new and novel events without directly impacting scoring
- New and novel events occur normally in most network and cloud environments and in most cases are not directly linked to threats
- Awareness of new and novel events support better situational awareness and provide additional context when observed with kill chain alerts





- Top -

## New Host

- Reports on the first time a host was seen on the internal network.

## New Host Role

- Reports when a host began operating with a particular infrastructure role.

## Novel MAC Vendor

- Reports when a host appears with an unusual MAC vendor for the network.

## Novel Admin Protocol Usage

- Reports when a host uses an administrative protocol (e.g., SSH) for the first time.

## Novel External Destination Port

- Reports when a host is seen making an outbound connection on a destination port that is rare for the environment and lasted longer than 5 minutes.

## Novel Access to SMB Admin Share

- Reports when a host is seen connecting to another host's SMB admin share and it is unusual for this host to connect to other systems in this way.

## Vectra Indicator Match

- A host was seen with network artifacts that are sometimes associated with attacker infrastructure. These events should be reviewed in the context of other threat detections.



# Network Detection Profiles



# Botnet

## Detection Profile

### General Behavioral Profile

- Programmatic discovery and asset monetization techniques
- External, persistent Command and Control behaviors

### Possible Root Causes

- A host has been infected and is participating in a botnet
- SaaS enabled asset discovery services have been observed

### Business Impact

- Investigations of entities matching this profile should be prioritized in alignment with malware remediation procedures and urgency
- Failure to take timely steps to respond to entities that match this profile may allow crypto-mining activities to persist, or open the door to more aggressive attacks from the compromised host over time

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# Cloud Services

## Detection Profile

### General Behavioral Profile

- Complex, active external Command and Control and/or Data Exfiltration Services
- NOT PRESENT: Lateral movement focused behaviors

### Possible Root Causes

- Entities are leveraging unauthorized cloud services

### Business Impact

- Investigations of entities matching this profile may generally be prioritized in alignment with addressing the presence of unauthorized IT Services, or with risks associated with data exfiltration and data loss

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.



# External Adversary

## Detection Profile

### General Behavioral Profile

- Technically sophisticated, objective-oriented activities
- Advanced discovery and lateral movement techniques
- External, persistent Command and Control and/or Data Exfiltration

### Possible Root Causes

- Advanced Persistent Threat
- Full scope Red Team / Penetration Test

### Business Impact

- Investigation of entities matching this profile should be considered urgent
- Failure to take timely steps to respond to entities that match this profile may increase the risk of a breach

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# Insider Threat: Admin

## Detection Profile

### General Behavioral Profile

- Technically sophisticated, objective-oriented activities
- Advanced discovery and lateral movement techniques
- NOT PRESENT: External Command and Control and/or Data Exfiltration

### Possible Root Causes

- Technically sophisticated insider threat with local network access
- Emerging External Adversary with out-of-band communication
- An Admin has begun performing authorized activities that were previously unknown to the system

### Business Impact

- Investigations of entities matching this profile should be prioritized above less critical severity tasks
- Failure to take timely steps to respond to entities that match this profile may increase the risk of unauthorized or malicious activities

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# Insider Threat: User

## Detection Profile

### General Behavioral Profile

- Low-sophistication, human-based network reconnaissance and objectives
- Data Exfiltration

### Possible Root Causes

- A user is collecting and exfiltrating data outside of the organized authorized storage
- A user has been granted additional roles and privileges not previously known, or is moving data to previously unauthorized cloud storage locations

### Business Impact

- Investigations of entities matching this profile should be prioritized in alignment with organizational tolerance to data loss
- Failure to take timely steps to respond to entities that match this profile may allow for the loss of intellectual property, competitive advantage, legally protected, or regulated data

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# IT Discovery

## Detection Profile

### General Behavioral Profile

- Low-sophistication discovery and reconnaissance techniques

### Possible Root Causes

- Asset Management or Change Management Infrastructure
- IP Address Management (IPAM) Infrastructure

### Business Impact

- Investigations of entities matching this profile may generally be prioritized after more urgent activities are complete
- Failure to take timely steps to investigate may allow the perpetuation of unauthorized IT Discovery Services

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# IT Services

## Detection Profile

### General Behavioral Profile

- Low-sophistication reconnaissance and discovery
- Lateral machine-to-machine communication
- Simple external data exfiltration services

### Possible Root Causes

- IT Services are exhibiting machine-to-machine communication patterns

### Business Impact

- Investigations of entities matching this profile may generally be prioritized after more urgent activities are complete
- Failure to take timely steps to investigate may allow the perpetuation of unauthorized IT Services

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# Potentially Unwanted Program

## Detection Profile

### General Behavioral Profile

- External, persistent Command and Control behaviors
- Programmatic Discovery behaviors
- NOTE PRESENT:  Asset monetization techniques

### Possible Root Causes

- Adware or Potentially Unwanted Programs (PUP) are active.
- SaaS enabled asset discovery services have been observed

### Business Impact

- Investigations of entities matching this profile may generally be prioritized in alignment with addressing the presence of unauthorized IT Services, or Unwanted or Unauthorized Software, or Policy and Acceptable Use violations.

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# Ransomware

## Detection Profile

### General Behavioral Profile

- Behavioral patterns associated with ransomware

### Possible Root Causes

- Malicious ransomware activity
- Technical services exhibiting behaviors similar to ransomware

### Business Impact

- Investigation of entities matching this profile should be considered urgent
- Failure to take timely steps to respond to entities that match this profile may increase risk of loss of data and system availability

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.



# Vulnerability Discovery

## Detection Profile

### General Behavioral Profile

- Discovery, Reconnaissance, Lateral movement, and/or Exploitation
- NOT PRESENT: External, persistent Command and Control and/or Data Exfiltration

### Possible Root Causes

- An adversary that has yet to exhibit the full range of malicious behaviors, or a limited scope penetration testing activity
- Vulnerability discovery and management infrastructure behaviors observed

### Business Impact

- Investigations of entities matching this profile should be prioritized in alignment with procedures associated with unauthorized vulnerability discovery or limited scope penetration testing
- Failure to take timely steps to investigate may allow additional dwell time for an adversary with unobserved, persistent command and control or allow the presence of unauthorized, rogue vulnerability discovery infrastructure

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# Worm

## Detection Profile

### General Behavioral Profile

- Wide-but-shallow network recon, searching for specific services.
- Lateral machine-to-machine communication.
- NOT PRESENT:  Deep, thorough network enumeration of many services on individual targets.

### Possible Root Causes

- Malicious software is actively performing worm-like spreading behaviors across network
- Authorized IT software is leveraging risky, rare machine-to-machine discovery and update functionality

### Business Impact

- Investigations of entities matching this profile may generally be prioritized in alignment with addressing the presence of destructive malware, ransomware, and worms.

### About Detection Profiles

Cognito supports security analyst investigative workflows by classifying the behavioral profile of an entity based on the active detections it has exhibited – the assignment of these profiles are useful for quickly wrapping context around the types of real world profiles that exhibit similar behaviors to the one under investigation.

When determining a behavioral profile for a host, only active detections are considered – this means that if detections on a host are triaged as marked-as-custom, marked-as-fixed, or become inactive, that host's behavioral profile may change.

- Top -

# Observed Privilege Scores

- Top -

Cognito displays observed privilege scores for accounts, hosts, and services in some host and detection pages. The concept of “observed privilege” is distinct from that of “granted privilege”. A user may be given an account that has been granted a lot of privilege, but if the user only makes very modest use of that privilege, the observed privilege of the account will be low. Cognito focuses on observed privilege as it provides a clearer basis for implementing effective detection strategies related to advanced attackers’ use of stolen credentials.

All observed privilege scores, regardless of the object (account, host, or service) to which they refer, are expressed on the same scale. Each privilege score consists of two components: a numerical score from 1 to 10 (ranging from low to high privilege) and a label (low, medium, or high). Scores of 1 and 2 are labeled “low”, scores of 3 to 7 are labeled “medium”, and scores of 8-10 are labeled “high”. Cognito detection algorithms that are part of the Privileged Access Analytics (PAA) feature make extensive use of these privilege scores.

## Account Scores

Observed privilege scores for accounts derive from the number of services an account connects to, either exclusively or in partnership with a small number of other accounts. An account that connects to 200 services, each of which is used by only a small number of other accounts, will score high. An account which connects to 5 services, each of which is used by a large number of other accounts, will score low.

Using this approach, service accounts tend to score high as they usually connect to many services that only the service account can access. Privileged users (aka admins) are typically given a normal account (to be used for normal non-privileged activity such as getting onto WiFi, requesting vacations, etc.) and a privileged account (to be used only for activities which require privileges). The first of these accounts will typically have a low score, the second a high score.

## Service Scores

Let’s begin by defining what a “service” is. Given that PAA is constructed on Kerberos traffic and Active Directory data, a service is any distinct place (server) to which a system (client) can connect to request a service. Using this definition, RDP is not a service, but RDP to a particular system (e.g. RDP to serverA) *is* a service. Given such a methodology, it’s easy to see how a network can contain many services.

Observed privilege scores for services derive from the scores of the accounts that are used to connect to the service. Thus, if a service is only accessed via accounts that predominantly have high privilege scores, the service will also have a high privilege score. This can, for instance, happen when a small number of privileged accounts belonging to admins are used from each admin’s laptop to exclusively connect to a particular service. Another example is when a service account for a backup server connects to an agent running on 1,000 laptops. In both instances, the accounts used are high privilege—in the latter example, there is only single account in use. Conversely, a vacation request portal used by everyone in an organization (each logging in with their user accounts) will rate low on the privilege scale. And a service used exclusively by a low privilege account will also have a low privilege score.

- Top -

## Host Scores

Observed privilege scores for hosts derive from the scores of the accounts that are seen on the host. If a particular host has only high-privileged accounts on it, the host will have a high privilege. A jump system from which only privileged users initiate connections to downstream servers is an example of a high-privileged host. A laptop on which a privileged user uses both their normal account and their privileged account will score quite high (though not as high as the jump system described above).

Privilege scores for hosts often indicate how interesting the hosts would be to an attacker. If an attacker compromises a high privilege host, they can harvest the credentials of one or more high-privilege accounts on that host. In a scenario where an attacker wants to move laterally through the use of stolen credentials, this is exactly their goal. After all, stealing credentials which have little or no privilege won't get the attacker closer to their goal.



# Detect for Azure AD and M365

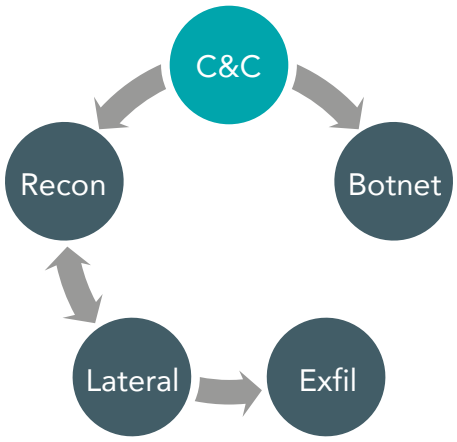


## Category

# Command & Control

- A host or account appears to be under control of an external entity
- Most often, the control is automated as the host or account is part of a botnet or has adware or spyware installed
- The host or account may be manually controlled from the outside – this is the most threatening case and makes it highly likely that this is a targeted attack

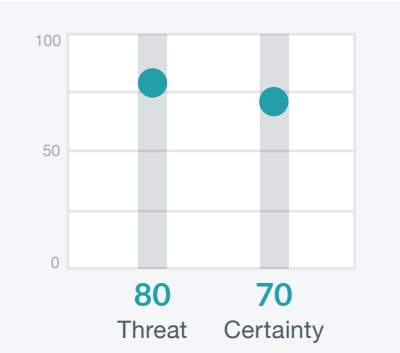


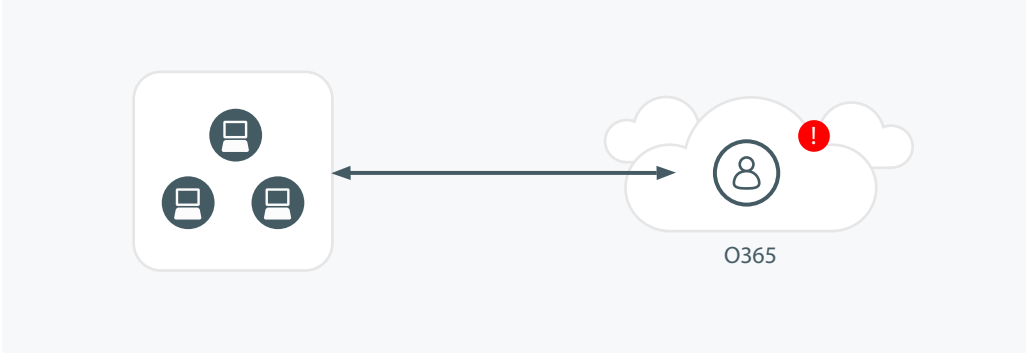



- Top -

# Azure AD Admin Account Creation

## Command & Control




MITRE | ATT&CK®

T1528 Steal Application Access Token

T1550 Use Alternate Authentication Material

## Triggers

- An account has been created with administrative privileges (TenantAdmins, PrivilegedRoleAdmins, ApplicationAdministrators) that provide broad access to the environment.
- The threat score is statically assigned.
- The certainty score is statically assigned.

## Possible Root Causes

- An attacker that has gained administrative rights has added additional administrative accounts to the environment as a back-up access method if their existing access is disabled or otherwise removed at a future date.
- Existing legitimate administrators may add additional administrative users unintentionally or via social engineering.
- A new, legitimate, administrative account was added.

## Business Impact

- Unauthorized administrative users have complete control within the environment, creating significant on-going risk to a broad range of resources.
- Attackers with access to the identified administrative rights will be able to operate unfettered within the environment.
- Attackers using multiple administrative accounts improve their resilience to an incident response and are able to silo operations to prevent the detection of a single compromised admin account from affecting access and actions undertaken from other compromised admin accounts.

## Steps to Verify

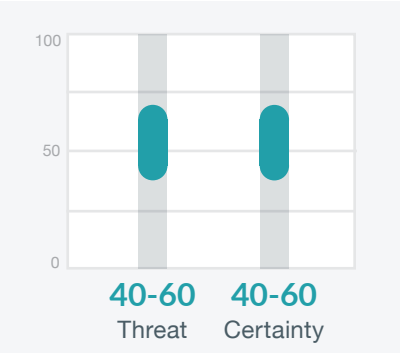
- Validate the administrative account was created according to organizational change control policies and that the access granted is appropriate and necessary.

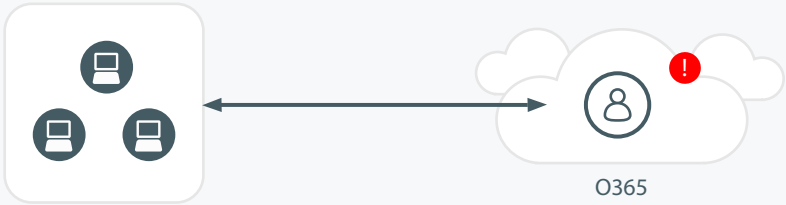
- Top -

# Azure AD MFA-Failed Suspicious Sign-On

## Command & Control




MITRE | ATT&CK®

T1078 Valid Accounts

### Triggers

- A login attempt occurred to an account where both conditional access policies were not met and where sign-on attributes (such as location, device, etc.) that are unusual for the account.

### Possible Root Causes

- An adversary has stolen a valid account and is attempting to use it as part of an attack but had not yet succeeded in circumventing MFA or other conditional access policies.
- A user has moved and performed a full refresh of their devices and failed to pass MFA or other conditional access policies.

### Business Impact

- Adversaries will continue to attempt to bypass security controls until successful unless directly stopped.
- The compromise of a valid account may lead to the loss of confidentiality and integrity of any data and services that the account may access, and it may be used in service of additional lateral movement or attacks against other internal users.

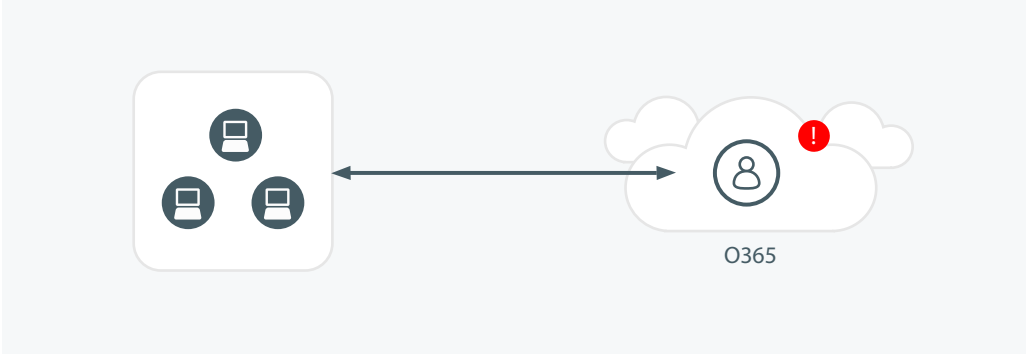
### Steps to Verify

- Investigate irregularities associated with this user's login events for indications of a successful compromise.
- Validate whether these attempts were performed by the account's proper owner.

- Top -

# Azure AD Redundant Access Creation

## Command & Control


MITRE | ATT&CK®

T1098 Account Manipulation

### Triggers

- A service principal, application, or user has been provisioned membership into to the 'Privileged Role Administrator' AzureAD role.

### Possible Root Causes

- An adversary has provisioned access into a sensitive role to create redundant access into the network.
- In some cases, administrators performing deployment testing will grant permissions associated with this role to the app or related service principal.

### Business Impact

- Adversaries will create redundant access mechanisms so that they are able to continue to maintain persistence despite their primary access method being discovered and remediated.
- Redundant access allows malicious activities to continue well beyond initial discovery and response phases, increasing risks to enterprise services or data.

### Steps to Verify

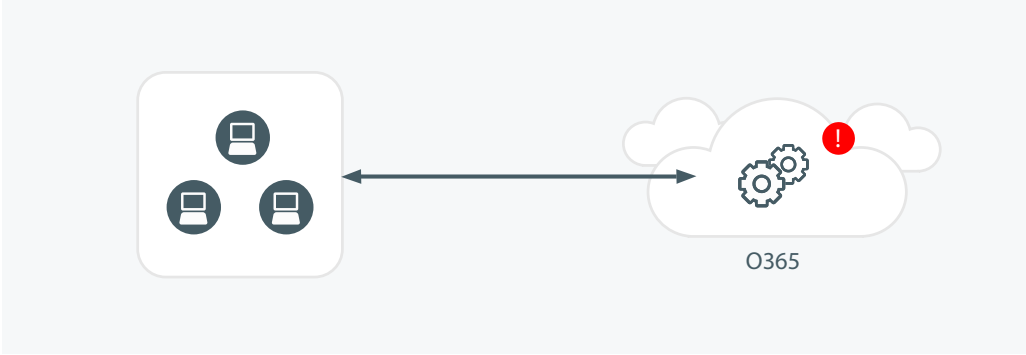
- Validate that this activity is not associated with authorized administrative testing activities.

- Top -

# Azure AD Suspicious OAuth Application

## Command & Control


MITRE | ATT&CK®

T1550 Use Alternate Authentication Material

T1528 Steal Application Access Token

### Triggers

- A third-party cloud application has requested excessive or risky access, which may allow malicious activities to be performed on behalf of the granter of the permission.

### Possible Root Causes

- An attacker is trying to trick the user into delegating permissions to them which will enable further malicious activities.
- A new legitimate 3rd party application is installed in the organization which requires elevated permissions from users.

### Business Impact

- Malicious applications are able to perform actions with delegated permissions without a user's knowledge and may be difficult to detect.
- Depending on the delegated privileges involved, the impact may range from single account takeover to full subscription compromise.

### Steps to Verify

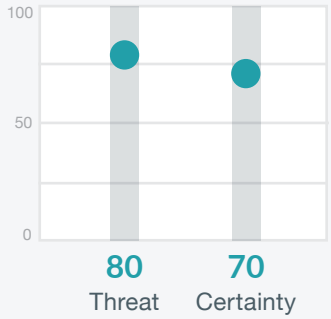
- Validate that this is an authorized application which has been vetted for risk by the security team.

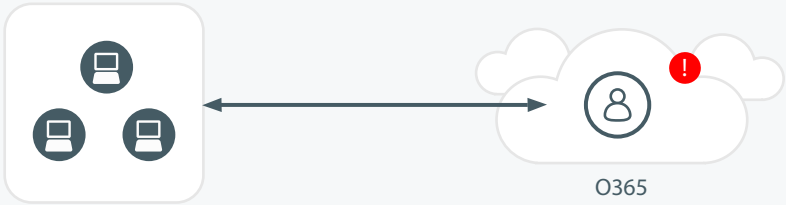
- Top -

# Azure AD Suspicious Sign-on

## Command & Control




MITRE | ATT&CK®

T1078 Valid Accounts

### Triggers

- A successful login has occurred to an account with sign-on attributes (such as location, device, etc.) that are unusual for the account.
- The threat score is statically assigned.
- The certainty score is statically assigned.

### Possible Root Causes

- An adversary has stolen a valid account and is using it as part of an attack.
- A user has moved and performed a full refresh of their devices and performed login activities across these devices with new sign-on attributes.

### Business Impact

- Adversaries frequently bypass security controls through the malicious, unauthorized use of valid credentials.
- The compromise of a valid account may lead to the loss of confidentiality and integrity of any data and services that account may access, and it may be used in service of additional lateral movement or attacks against other internal users.

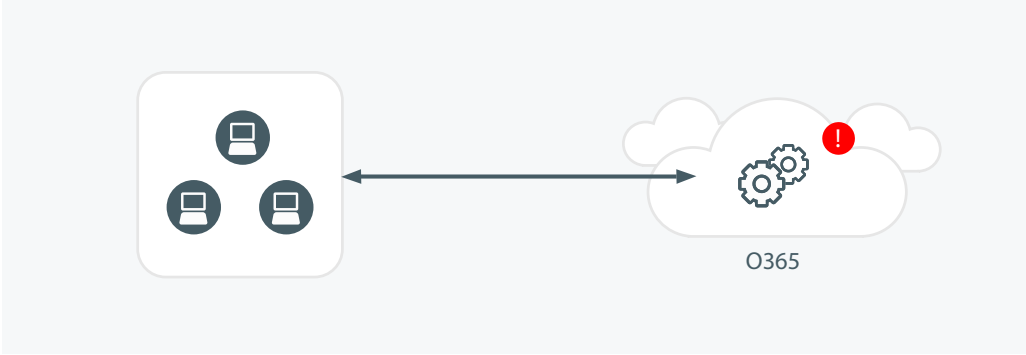
### Steps to Verify

- Investigate irregularities associated with these login events for indications of compromise.
- Validate the login activities have been performed in accordance with organizational MFA policies, enforcing re-login with MFA if required.

- Top -

# Azure AD Suspected Compromised Access

## Command & Control


MITRE | ATT&CK®

T1078 Valid Accounts

### Triggers

- A successful login has occurred to an account with many characteristics that are both unusual for the account and highly correlated with account compromise.
- The threat score is statically assigned.
- The certainty score is statically assigned.

### Possible Root Causes

- An adversary has stolen a valid account and is using it as part of an attack.
- A user has shifted multiple aspects of their normal sign-on behavior which match multiple behaviors associated with malicious account takeovers.

### Business Impact

- Adversaries frequently bypass security controls through the malicious, unauthorized use of valid credentials.
- The compromise of a valid account may lead to the loss of confidentiality and integrity of any data and services that the account may access, and it may be used in service of additional lateral movement or attacks against other internal users.

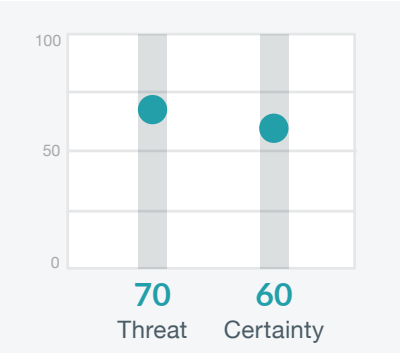
### Steps to Verify

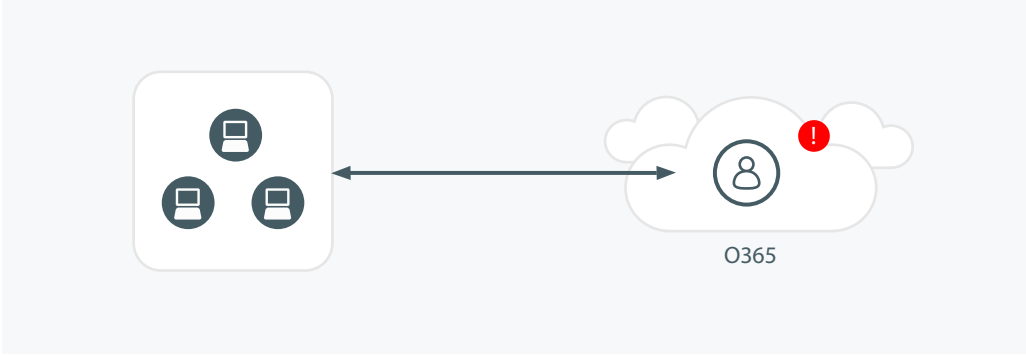
- Investigate irregularities associated with these login events for indications of compromise.
- Validate the login activities have been performed in accordance with organizational MFA policies, enforcing re-login with MFA if required.

- Top -

# Azure AD TOR Activity

## Command & Control




MITRE | ATT&CK®

T1090 Proxy

### Triggers

- A user was observed accessing the environment from a known anonymized (TOR) exit node, post authentication.
- The threat score is statically assigned.
- The certainty score is statically assigned.

### Possible Root Causes

- An attacker is using an anonymizing proxy like TOR to obfuscate details of their source connection or make investigation more difficult by using multiple source IP addresses.
- A user may be intentionally using TOR to circumvent restrictions preventing access to the resources in question, such as those applied by the country they are accessing from.

### Business Impact

- Attackers identified under this detection are actively operating within the environment while maintaining some level of operational security by obfuscating their source details.
- Attackers operating using TOR will reduce the ability of teams to connect identified attacker behavior with other behaviors not yet identified since it enables the attacker to regularly change the source detail of their connections while undertaking operations within the environment.

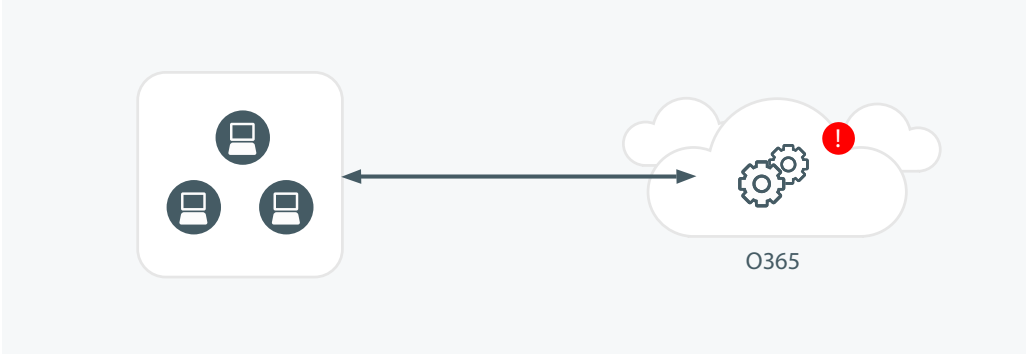
### Steps to Verify

- Review the actions being undertaken by the user during and just before the identified activity to determine resources accessed and potential risk posed by that access.
- Review security policy to determine if use of TOR is allowed.
- Discuss with user to determine if use of TOR is known and legitimate.
- If review determines there is a high risk to data or the environment, disable the account and perform a comprehensive investigation.

- Top -

# O365 Power Automate HTTP Flow Creation

## Command & Control


MITRE | ATT&CK®

T1041 Exfiltration Over C2 Channel

T1008 Fallback Channels

T1105 Ingress Tool Transfer

T1059 Command and Scripting Interpreter

T1020 Automated Exfiltration

### Triggers

- An account has congured an internal resource for remote interaction through the use of a Power Automate HTTP Connector.

### Possible Root Causes

- An attacker is leveraging Power Automate HTTP connectors to extend malicious access into internal resources.
- In rare cases, a Power Automate HTTP connector is used to enable legitimate external connectors which trigger approved internal actions.

### Business Impact

- Adversaries using this technique may gain malicious access to a wide range of internal resources including forms, pages, files, and emails.
- Use of this technique allows an adversary to bypass login and MFA requirements once the Power Automate flow is installed.

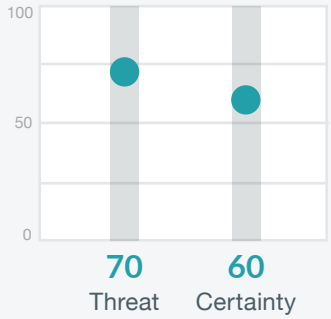
### Steps to Verify

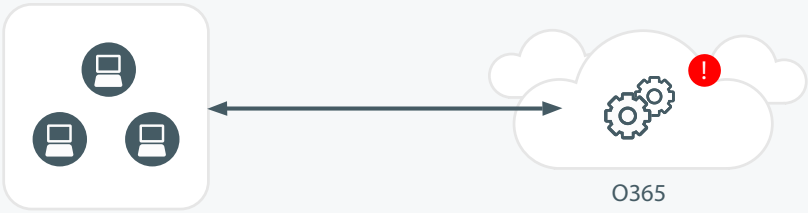
- Given the risk and relative rarity associated with Power Automate HTTP connectors, the legitimacy of associated flows should be investigated.

- Top -

# O365 Suspicious Power Automate Flow Creation

## Command & Control




MITRE | ATT&CK®

T1041 Exfiltration Over C2 Channel

T1008 Fallback Channels

T1105 Ingress Tool Transfer

T1059 Command and Scripting Interpreter

T1020 Automated Exfiltration

### Triggers

- Power Automate Flow creation has been observed by a user not typically associated with this activity.

### Possible Root Causes

- An adversary has leveraged Power Automate as a persistence mechanism inside the environment.
- One of a small set of users who are authorized to perform Power Automate Flow creation has been observed doing so.

### Business Impact

- Adversaries using this technique may gain malicious access to a wide range of internal resources including forms, pages, files, and emails.
- Use of this technique may enable persistence or lateral movement, or may be used to establish a means for subsequent data exfiltration.

### Steps to Verify

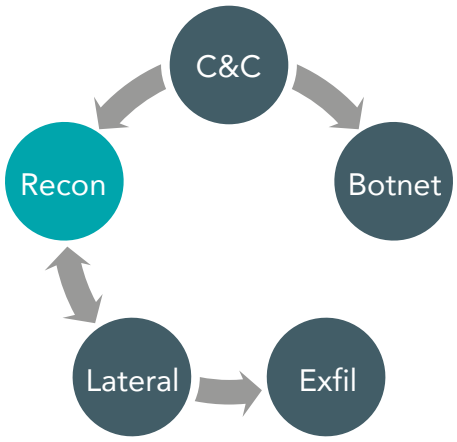
- Power Automate activities from unauthorized users should be immediately investigated
- Users authorized for Power Automate activities should be explicitly triaged in this system to avoid future detections.

- Top -

## Category

# Reconnaissance

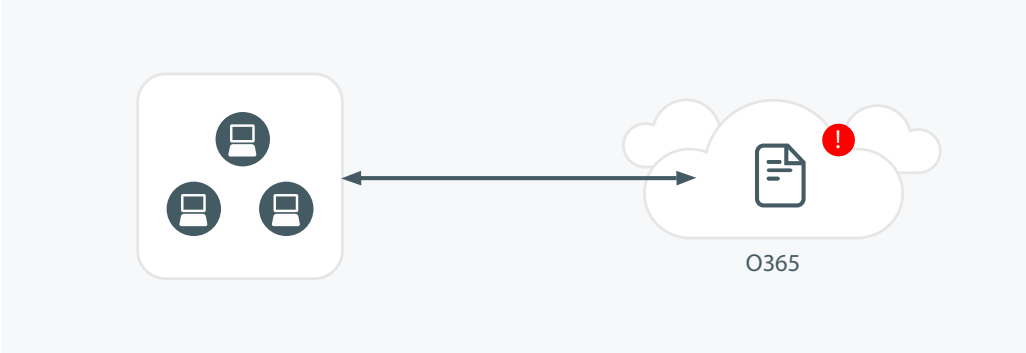
- A host or account is mapping out the inside of your network or cloud environment
- The activity may indicate that this is a targeted attack
- Detection types cover fast scans and slow scans – your vulnerability scanner will show up here as it performs much the same activity as an attacker




- Top -

# O365 Suspicious Compliance Search

## Reconnaissance


MITRE | ATT&CK®

T1119 Automated Collection

T1213 Data from Information Repositories

T1083 File and Directory Discovery

### Triggers

- The Exchange compliance search functionality was observed being used by an account that does not normally use this functionality.
- The threat score is statically assigned.
- The certainty score is statically assigned.

### Possible Root Causes

- Attackers may use compliance searches to search across Exchange mailboxes for sensitive data to collect and exfiltrate.
- Some internal users may use compliance searches to support legitimate business operations like legal and HR for litigation, audit, and compliance purposes.

### Business Impact

- Compliance search capabilities provide an enticing target for adversaries to abuse and may result in the loss of sensitive information up to and including passwords, encryption keys, and even financial data or intellectual property.

### Steps to Verify

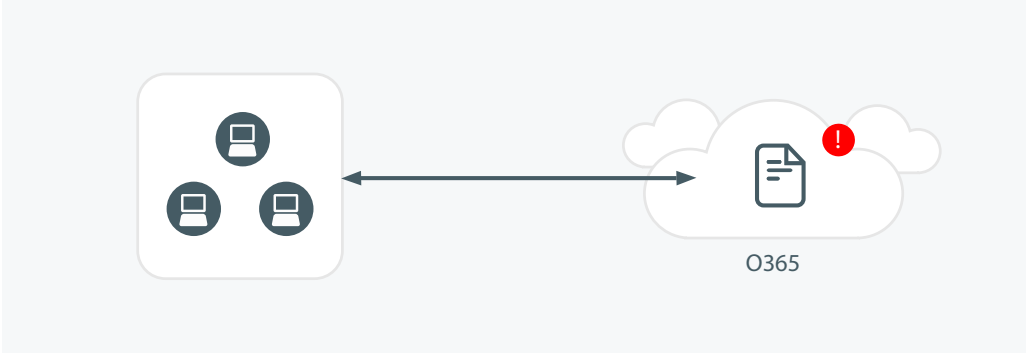
- Review the account in question to ensure they should be issuing compliance searches within the environment.
- Review the search being done to determine if the data being sought may be particularly interesting to attackers.
- Contact the user to ensure the searches are being done in compliance with company policy.

- Top -

# O365 Unusual eDiscovery Search

## Reconnaissance


MITRE | ATT&CK®

T1119 Automated Collection

T1213 Data from Information Repositories

T1083 File and Directory Discovery

### Triggers

- A user is creating or updating an eDiscovery search.

### Possible Root Causes

- An adversary has gained access to eDiscovery capabilities and is using that access to perform reconnaissance across the environment.
- One of a small set of users authorized to perform eDiscovery has been observed doing so.

### Business Impact

- eDiscovery capabilities provide an enticing target for adversaries to abuse and may result in the loss of sensitive information up to and including passwords, encryption keys, and even financial data or intellectual property.
- eDiscovery capabilities may include data traditionally inaccessible through other means but preserved as part of a litigation hold.

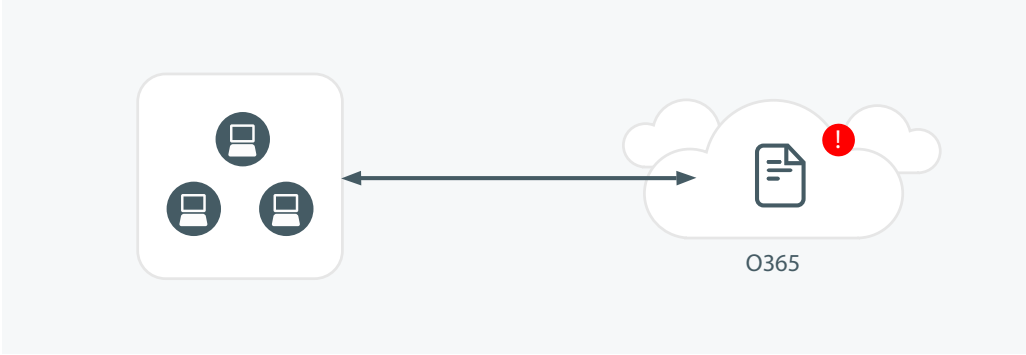
### Steps to Verify

- eDiscovery search from unauthorized users should be immediately investigated.
- Users authorized for eDiscovery should be explicitly triaged in this system to avoid future detections.

- Top -

# O365 Suspect eDiscovery Usage

## Reconnaissance


MITRE | ATT&CK®

T1119 Automated Collection

T1213 Data from Information Repositories

T1083 File and Directory Discovery

T1562 Impair Defenses

## Triggers

- Behaviors commonly associated with covering up a potentially malicious eDiscovery search have been observed.
- The threat score is statically assigned.
- The certainty score is statically assigned.

## Possible Root Causes

- An attacker has compromised the eDiscovery system, is using it to actively collect and exfiltrate data, and is hiding their tracks.
- A legitimate user has abused the eDiscovery system to gain information and has deleted the search quickly to go unnoticed.
- An improperly created eDiscovery Search has been flagged for removal based on deviation from enterprise policies on accepted eDiscovery usage.
- An authorized test of the eDiscovery system has been observed and clean up actions from that test have been flagged as suspicious.

## Business Impact

- eDiscovery search capabilities provide an enticing target for adversaries to abuse and may result in the loss of sensitive information up to and including passwords, encryption keys, and even financial data or intellectual property.
- Abuse of eDiscovery search could result in sensitive data exfiltration as well as advancing an attack deeper into the organization.

## Steps to Verify

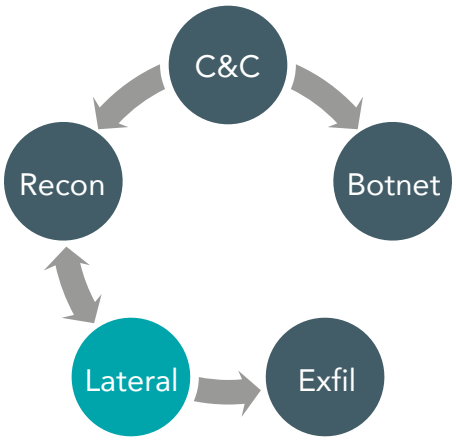
- Review the account in question to ensure they should be issuing compliance searches within the environment.
- Review any remaining and undeleted artifacts associated the search being done to determine if the data being sought may be particularly interesting to attackers.
- Contact the user to ensure the searches are being done in compliance with company policy.

- Top -

## Category

# Lateral Movement

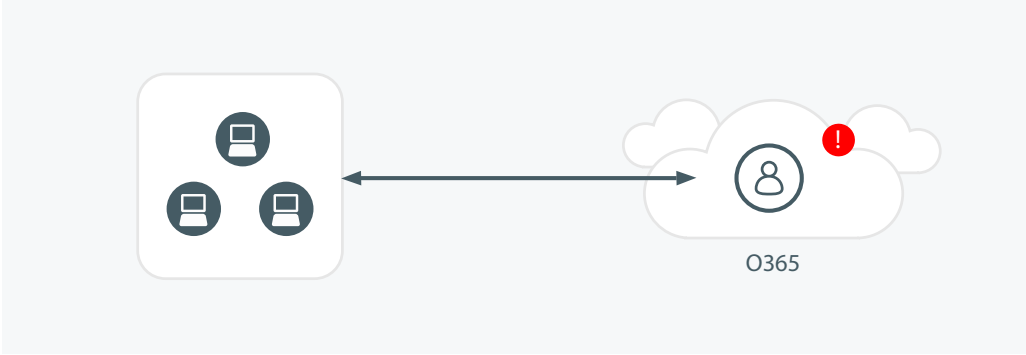
- Covers scenarios of lateral action meant to further a targeted attack
- This can involve attempts to steal account credentials or to steal data from another machine
- It can also involve compromising another host or account to make the attacker's foothold more durable or to get closer to target data




- Top -

# Azure AD Successful Brute-Force

## Lateral Movement


MITRE | ATT&CK®

T1110 Brute Force

### Triggers

- A successful login with suspicious IP Address or User-Agent after frequent failed login attempts.

### Possible Root Causes

- Adoption of weak or reused credentials is common among users and attackers exploit this behavior by repeatedly attempting to login to discovered accounts using leaked or common passwords.
- Legitimate users who repeatedly mistype their password may trigger this detection
- Automated systems or services may attempt to continuously login with incorrect credentials.

### Business Impact

- Accounts compromised through brute-force attacks provide attackers a foothold in the enterprise.
- Attackers who have taken over administrative, executive, or high-value accounts put the enterprise at considerable risk.

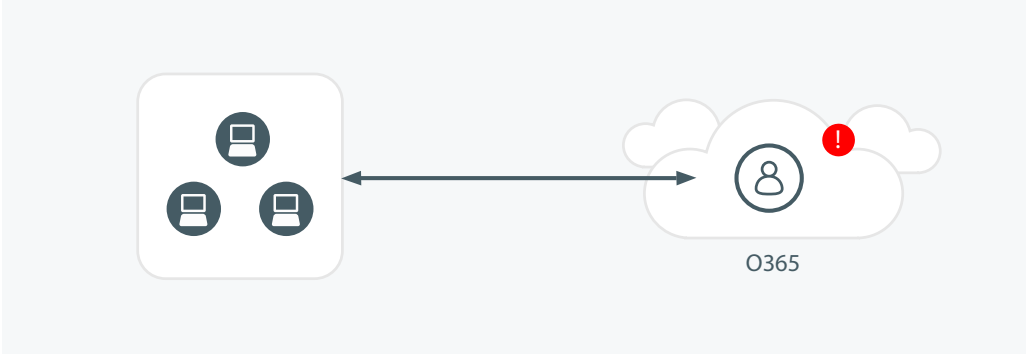
### Steps to Verify

- Brute-force attacks that end with a successful login should immediately be investigated for abnormal or threatening behavior.

- Top -

# O365 Suspicious Mailbox Manipulation

## Lateral Movement


MITRE | ATT&CK®

T1098 Account Manipulation

### Triggers

- Access has been granted to more resources than a user has had historically and has occurred outside of learned administrator behaviors.

### Possible Root Causes

- An attacker has escalated the account's Exchange access rights to enable business email compromise or the collection of additional information to aid in the next step of the attack.
- Employee life-cycle activities such as permanent separation or temporary leaves of absence may legitimately require mailbox modifications which could trigger this detection.
- Some service-specific mailboxes are intentionally granted these permissions.

### Business Impact

- Sensitive data and content may be contained within Exchange which may be useful or desirable to an adversary.
- Data may leak from a user's mailbox by being transmitted to unauthorized entities.

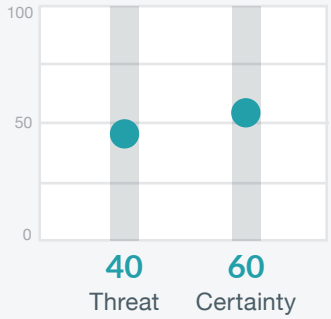
### Steps to Verify

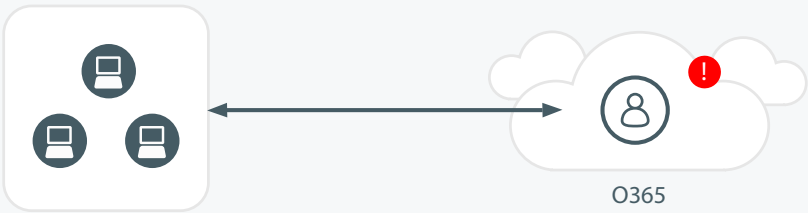
- Validate that the permissions granted are appropriate to the entity in question.

- Top -

# O365 Suspicious Mailbox Rule Creation

## Lateral Movement




MITRE | ATT&CK®

T1564 Hide Artifacts

### Triggers

- An account was observed creating suspicious mailbox rules in Exchange that allow an attacker to manipulate, hide, or delete incoming emails.

### Possible Root Causes

- An attacker with control of an account created mailbox rules that hide or manipulate emails to either evade notice by the mailbox owner or impact business processes.
- A user created a benign but broad or abnormal inbox rule as part of normal business email management.

### Business Impact

- Instances of malicious mailbox rules may indicate an adversary has control of an internal mailbox and can access the users email data and send emails internally and externally on behalf of the user.
- A successful attack can result in immediate data theft or reputation loss from the compromised account.
- A successful attack can result in additional business impact through targeted phishing from the internal account, as they are often trusted and subsequent to less strict security controls relative to external accounts.

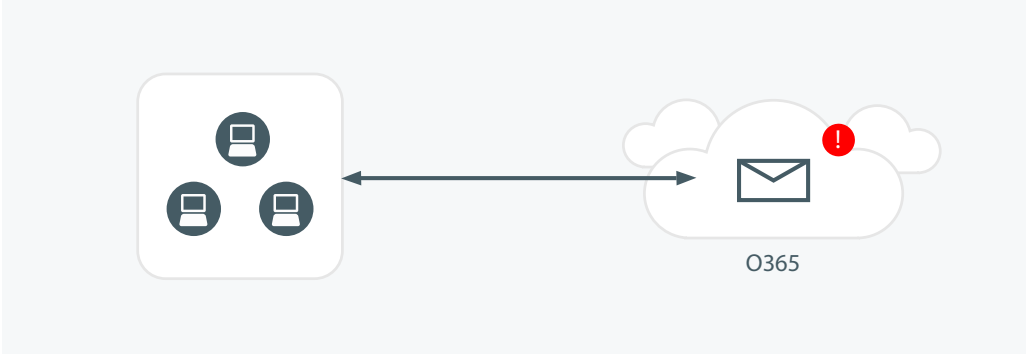
### Steps to Verify

- Investigate the account that performed the action for other indications of malicious activity
- If review indicates possible malicious actions, revert configuration and disable credentials associated with this alert, then perform a comprehensive investigation.

- Top -

# O365 Attacker Tool: Ruler

## Lateral Movement


MITRE | ATT&CK®

T1114 Email Collection

T1137 Office Application Startup

### Triggers

- The Ruler attack tool has been observed.

### Possible Root Causes

- An adversary has used compromised account credentials in conjunction with the Ruler attack tool to enable malicious code or command execution.
- As this is a known attacker tool, there are no non-malicious use cases.

### Business Impact

- Use of this tool may allow an adversary to install malware or execute commands on the endpoint running the exchange client associated with this compromised account. Malware or arbitrary command execution may be used for a variety of malicious activities, such as additional credential compromise, data collection and exfiltration, or to further attack progression.

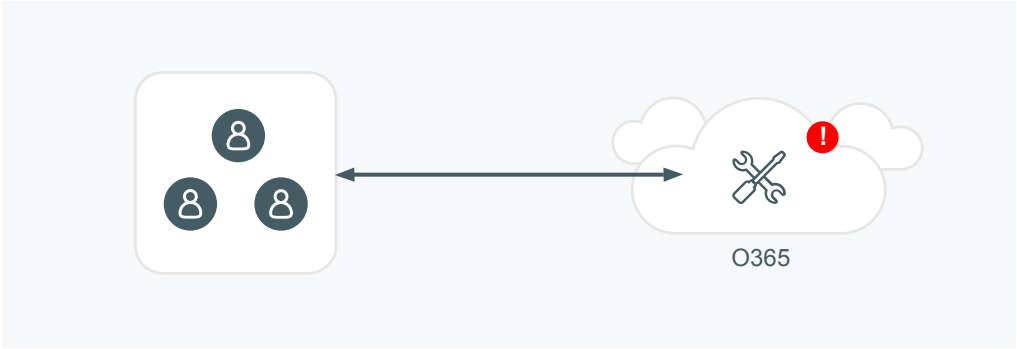
### Steps to Verify

- Investigate the compromised account for additional malicious actions and respond according to findings.

- Top -

# Azure AD Change to Trusted IP Configuration

## Lateral Movement


MITRE | ATT&CK®

T1562 Impair Defenses

### Triggers

- A change to a trusted IP configuration in Azure was observed in either the AzureAD Known Networks configuration or the configuration for trusted networks for multi-factor authentication.

### Possible Root Causes

- Attackers may add networks to the trusted networks ranges to allow them to bypass security controls under conditional access policies or to bypass MFA requirements.
- System administrators may add trusted networks to allow trusted environments to have different security policies applied to them.

### Business Impact

- Modifications to the trusted network configuration may introduce risks by allowing particular IP addresses/ranges to bypass critical security controls.
- Trade-offs in favor of usability over security can be achieved through the configuration of trusted IPs, but when abused or misconfigured can increase risk to an organization by disabling expected security controls.

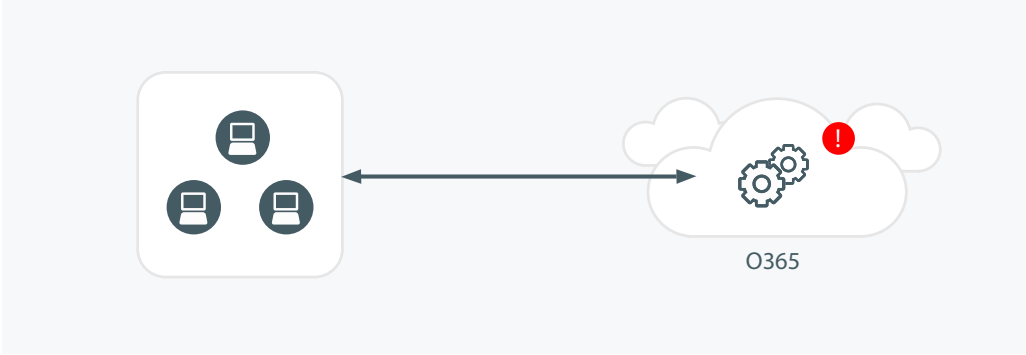
### Steps to Verify

- Investigate the IP addresses to determine if they should be trusted by the organization.
- Contact the owner of the account that made the change to verify it was done legitimately.

- Top -

# O365 Disabling of Security Tools

## Lateral Movement


MITRE | ATT&CK®

T1562 Impair Defenses

### Triggers

- Activities which weaken or disable Office 365 protective security features and tools.

### Possible Root Causes

- Attackers will attempt to disable or downgrade Office 365 security mechanisms to blind defenders or to enable further malicious activities without the risk of detection.
- In some cases, administrators may disable security mechanisms while troubleshooting problems.

### Business Impact

- Attackers who have successfully degraded, disabled, or bypassed security controls can more easily progress towards their objectives.
- Degraded or disabled security controls increase the potential impact of both present and future attacks against the organization.

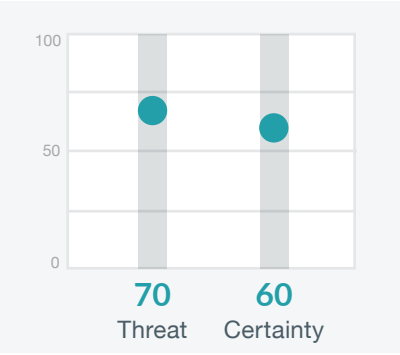
### Steps to Verify

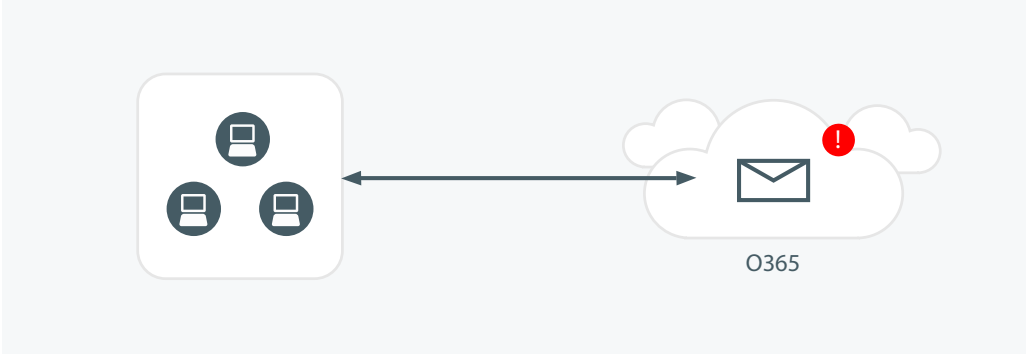
- Review if this configuration is expected and appropriate in light of any available compensating controls.
- If this is a temporary configuration for troubleshooting purposes, confirm it has been reenabled once that troubleshooting is complete.

- Top -

# O365 DLL Hijacking Activity

## Lateral Movement




MITRE | ATT&CK®

T1574 Hijack Execution Flow

## Triggers

- An account that may not download DLLs typically has been observed downloading a DLL file under conditions that highlight the risk of DLL hijacking, such as both a non-DLL and DLL file being downloaded from the same directory in a short time frame.
- Threat scores are statically assigned.
- Certainty scores are statically assigned.

## Possible Root Causes

- An attacker has abused the way applications search for DLLs by placing a malicious DLL file into a shared directory with the intention of compromising any endpoint that loads the malicious DLL file rather than the intended application DLL file.
- In some cases, developers collaborating from a cloud hosted repository could intentionally download and access DLLs this way.

## Business Impact

- DLL Hijacking may result in the complete compromise of a targeted system, and associated accounts and data.
- Endpoints compromised through DLL Hijacking give an attacker an additional foothold in the environment and an opportunity for additional lateral movement, increasing the risk of impact to enterprise systems, users, and data.

## Steps to Verify

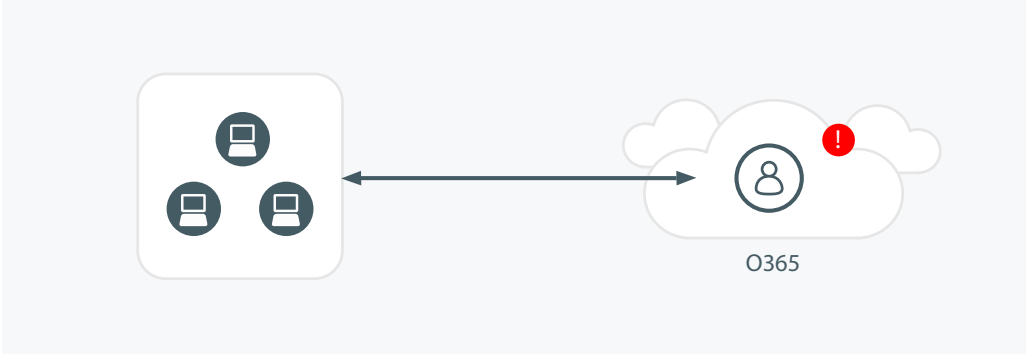
- Investigate the user associated with this action, and verify if this user would be downloading DLL files as part of their expected workflows.
- Investigate presence of additional files accessed as part of this detection, and assess if this is indicative of an authorize remote application, used for legitimate business purposes.

- Top -

# O365 External Teams Access

## Lateral Movement


MITRE | ATT&CK®

T1213 Data from Information Repositories

### Triggers

- A new team member has been added to a team in O365 Teams consisting of an external account from a domain rarely associated with O365 Teams access.
- The threat score is driven by the value of the team being modified.
- The certainty score is driven by how certain we feel about the maliciousness of the action.

### Possible Root Causes

- An adversary has added an external account under their control as a new member of a team by abusing an existing O365 Teams account.
- Sometimes legitimate external users (such as partners, contractors, lawyers, auditors, etc.) are added to an O365 Team as part of an authorized activity.

### Business Impact

- This type of access enables an attacker to perform additional discovery or collection activities by exposing sensitive business information which may include shared files, meeting content, or chat transcripts.
- The impact of such access may include information necessary to enable further attack progression or facilitate the loss of proprietary information or intellectual property, and regulated data.
- In some cases, access to the team's communication fabric and conversation history can enable successful blackmail or extortion against enterprise personnel.

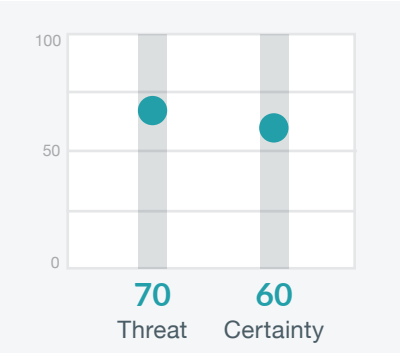
### Steps to Verify

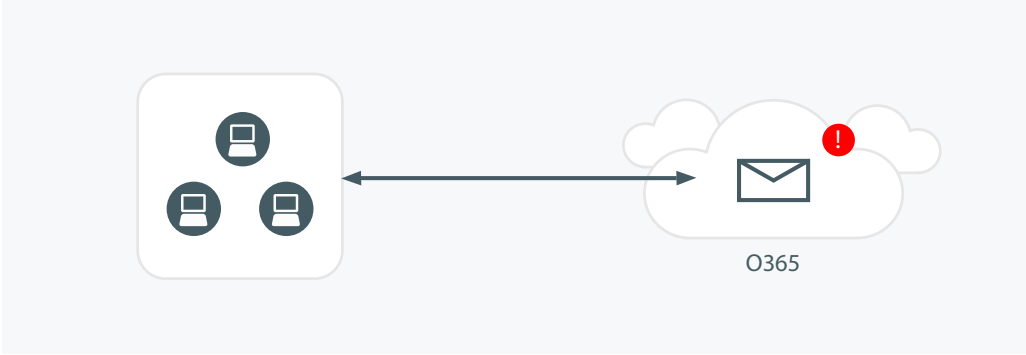
- Validate that the account added is an authorized member of the O365 Team.

- Top -

# O365 Internal Spearphishing

## Lateral Movement




MITRE | ATT&CK®

T1534 Internal Spearphishing

### Triggers

- A user was observed sending multiple emails to internal recipients which were flagged by O365 reputation scanning as likely phishing emails.
- The threat score is statically assigned.
- The certainty score is statically assigned.

### Possible Root Causes

- An attacker has compromised a single account and is abusing its access and implicit trust within an organization to attack additional accounts via spearphishing emails.
- Benign emails have been flagged as suspicious based on their content or attachments, which are most frequently associated with invoices sent to distribution lists.

### Business Impact

- Spearphishing is one of the predominant ways attackers gain and expand access to credentials within an environment and is particularly effective when utilizing the implicit trust of an internal sender.
- Successful internal spearphishing campaigns result in broad access to a large range of resources within the environment, resulting in a significant increase in overall impact of a compromised account incident within an organization.

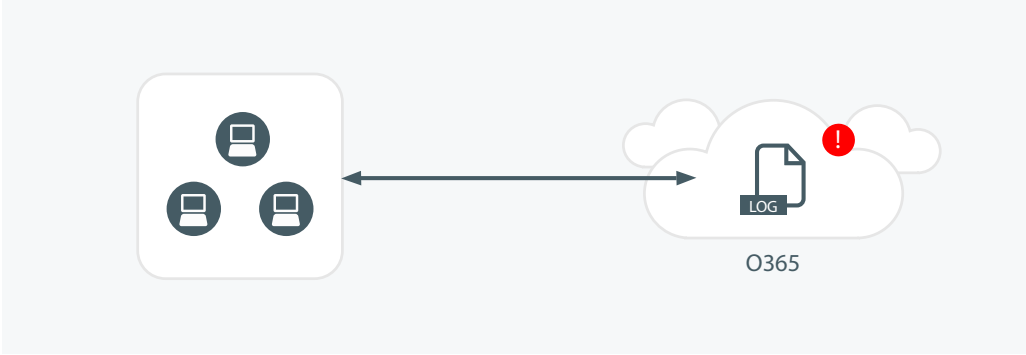
### Steps to Verify

- Review the details and contents of the email to validate it is malicious.
- Review additional detections and events by the source user which may indicate their account has been compromised.
- Validate the source user is aware of and sent the email that was flagged.

- Top -

# O365 Log Disabling Attempt

## Lateral Movement


MITRE | ATT&CK®

T1562 Impair Defenses

### Triggers

- An attempt has been made to disable important Office 365 logs that enhance security.

### Possible Root Causes

- Attackers will seek to disable logging to blind detection mechanisms and cover their tracks.
- Logging may be temporarily turned off by an admin while changing configuration or troubleshooting a problem.

### Business Impact

- An attacker who has disabled logging may progress parts of an attack without being detected, and without producing an auditable record to aid in forensics.
- Disabling logging degrades a critical component of an organization's security architecture.
- Many audit and compliance requirements can only be met through the collection of activity logs.

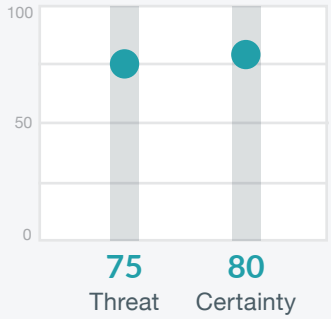
### Steps to Verify

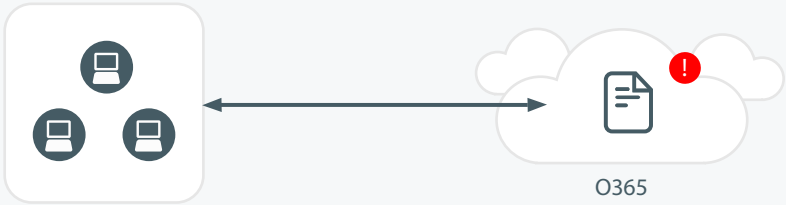
- Review whether this logging configuration is expected and appropriate.
- If this is a temporary configuration for troubleshooting purposes, confirm it has been reenabled once that troubleshooting is complete.

- Top -

# O365 Malware Stage: Upload

## Lateral Movement




MITRE | ATT&CK®

T1203 Exploitation for Client Execution

### Triggers

- Files which were subsequently flagged as malware were uploaded into the environment by this account.

### Possible Root Causes

- Attackers will stage malicious files in preparation for an attempt to infect other users from a trusted file repository.
- On rare occasions, benign files may be classified as malicious.

### Business Impact

- An attacker who has disabled logging may progress parts of an attack without being detected, and without producing an auditable record to aid in forensics.
- Disabling logging degrades a critical component of an organization's security architecture.
- Many audit and compliance requirements can only be met through the collection of activity logs.

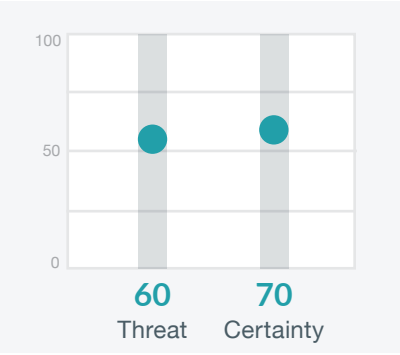
### Steps to Verify

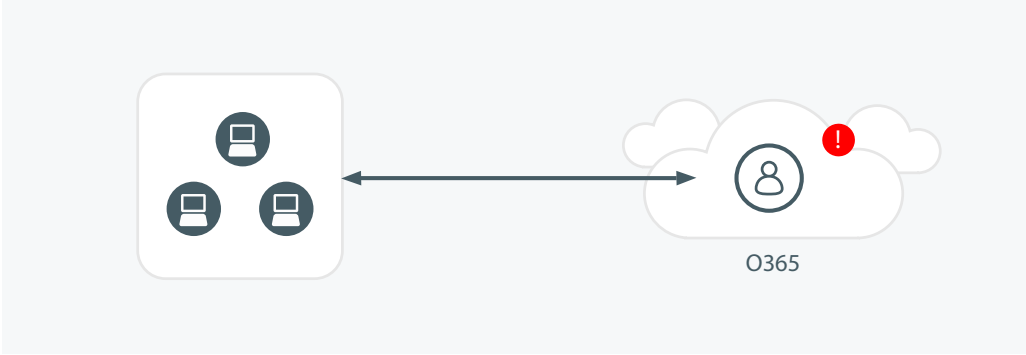
- Review whether this logging configuration is expected and appropriate.
- If this is a temporary configuration for troubleshooting purposes, confirm it has been reenabled once that troubleshooting is complete.

- Top -

# Azure AD MFA Disabled

## Lateral Movement




MITRE | ATT&CK®

T1562 Impair Defenses

### Triggers

- An account was observed disabling Multi-Factor Authentication (MFA) for another account.
- The threat score is statically assigned.
- The certainty score is statically assigned.

### Possible Root Causes

- An attacker is disabling MFA on an account to bypass this security control as a means of maintaining or acquiring additional access to the environment.
- Administrators may disable MFA for accounts used by automated processes or to temporarily enable users to access an environment after losing their second factor device.

### Business Impact

- MFA is a critical security control that if bypassed may be indicative of an active threat in the environment or increase risk of the account becoming compromised in the future.
- Compromised accounts provide attackers with access to critical systems and data which may be stolen, modified, or deleted.

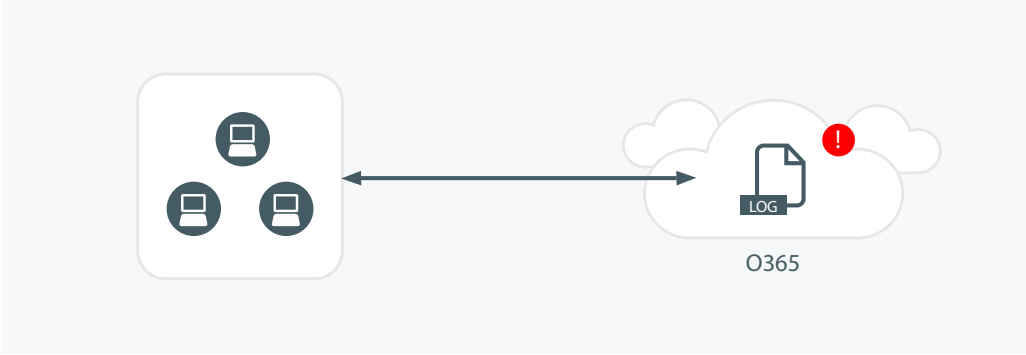
### Steps to Verify

- Review the account and internal policy to determine if MFA should be enabled for this account.
- Verify the action of disabling MFA on this account was intentional and followed internal security policies and change control processes.

- Top -

# Azure AD Newly Created Admin Account

## Lateral Movement


MITRE | ATT&CK®

T1136 Create Account

## Triggers

- An account has been created with administrative privileges (TenantAdmins, PrivilegedRoleAdmins, ApplicationAdministrators) that provide broad access to the environment.
- The threat score is statically assigned.
- The certainty score is statically assigned.

## Possible Root Causes

- An attacker that has gained administrative rights has added additional administrative accounts to the environment as a back-up access method if their existing access is disabled or otherwise removed at a future date.
- Existing legitimate administrators may add additional administrative users unintentionally or via social engineering.
- A new, legitimate, administrative account was added.

## Business Impact

- Unauthorized administrative users have complete control within the environment, creating significant on-going risk to a broad range of resources.
- Attackers with access to the identified administrative rights will be able to operate unfettered within the environment.
- Attackers using multiple administrative accounts improve their resilience to an incident response and are able to silo operations to prevent the detection of a single compromised admin account from affecting access and actions undertaken from other compromised admin accounts.

## Steps to Verify

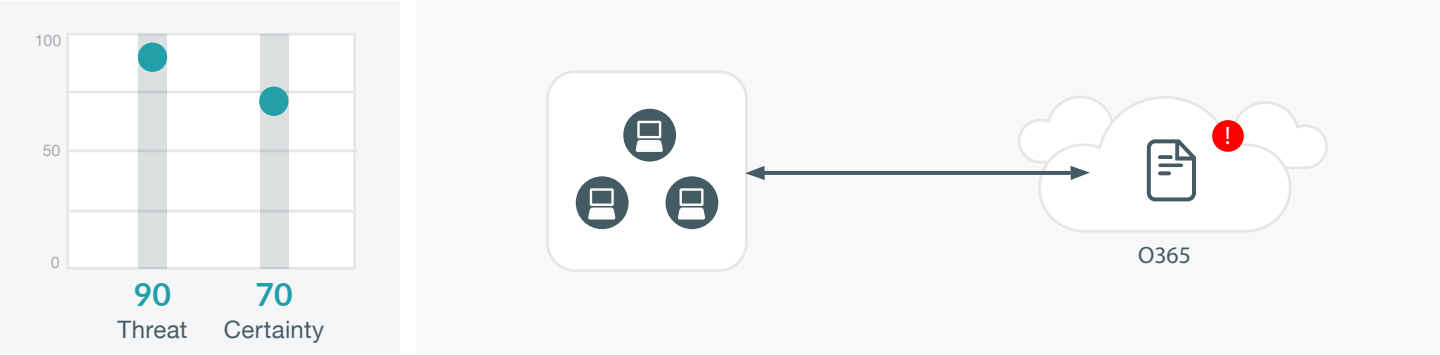
- Validate the administrative account was created according to organizational change control policies and that the access granted is appropriate and necessary.

- Top -

# O365 Ransomware

## Lateral Movement




MITRE | ATT&CK®

T1486 Data Encrypted for Impact

### Triggers

- A series of file modifications typically associated with ransomware.

### Possible Root Causes

- An account is being used to access an organization's cloud storage and encrypt and rewrite files.
- In some cases, automated jobs or services that perform widespread file renaming may trigger this detection.

### Business Impact

- Ransomware attacks directly impact access to the organization's data and are popular among attackers due to the possibility of a quick transition from attack to monetization.
- After files have been encrypted, the attacker will ask the organization to pay a ransom in return for a promise to provide the encryption key which would allow the files to be decrypted.
- Even if an organization is willing to pay the ransom, there is no guarantee that the encryption key will be provided by the attacker or that the decryption process will work.
- Absent the encryption key, an organization must rely on restoration of files from backups.

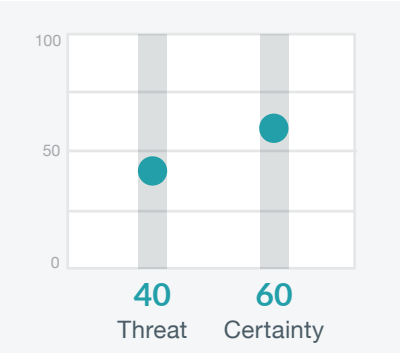
### Steps to Verify

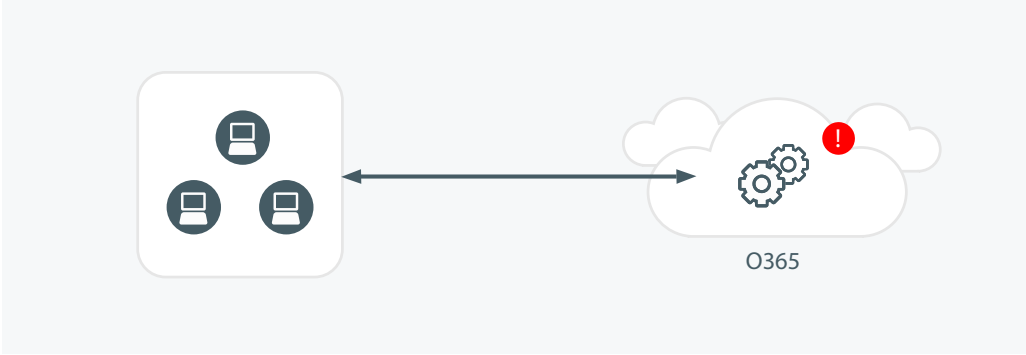
- Review the integrity of the affected files and determine whether they appear encrypted.

- Top -

# O365 Risky Exchange Operation

## Lateral Movement




MITRE | ATT&CK®

T1484 Group Policy Modification

T1098 Account Manipulation

## Triggers

- High risk Exchange operations which range from allowing the exfiltration of data, the creation of backdoor rules, execution of VBS scripts, or forwarding and collecting sensitive information.

## Possible Root Causes

- An attacker is manipulating Exchange to gain access to a specific set of data or to enable continued attack progression.
- In some cases, these operations may be authorized activities for a small set of highly privileged users who perform them so infrequently that they are outside what the detection model considers normal.
- Authorized configurations in cases of a permanent employee separation or temporary leave of absence may involve activities that would otherwise compromise mailbox integrity.

## Business Impact

- Sensitive data and content may be contained within Exchange which may be useful or desirable to an adversary.
- Compromising Exchange may allow an attacker to continue their attack progression.

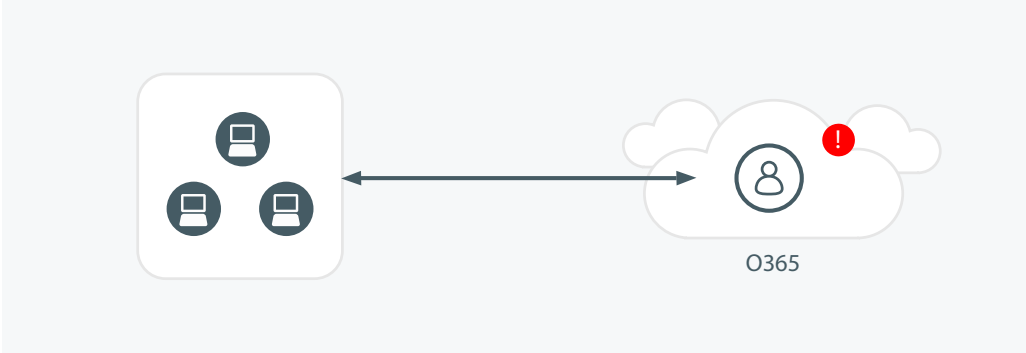
## Steps to Verify

- Verify whether these changes to the configurations are intentional and have been made with appropriate compensating safeguards.

- Top -

# Azure AD Privilege Operation Anomaly

## Lateral Movement


MITRE | ATT&CK®

T1078 Valid Accounts

### Triggers

- Abnormal Azure AD operations that may be associated with privilege escalation or account takeover.

### Possible Root Causes

- Attackers may be escalating privileges and performing admin-level operations after regular account takeover.
- A user whose learned activity baseline has been lost as a result of a prolonged leave of absence or a change in job function has returned to their regular job.
- A user's role may have evolved as part of a special project or assignment and the user is performing Azure AD activities previously outside of their learned baseline.

### Business Impact

- Users substantially deviating from their learned baseline in ways that correspond to threats associated with privilege escalation or account takeover often indicate an adversary foothold.
- Account takeover and privilege escalation can lead to sensitive information leakage, ransomware attacks, and other abuses.

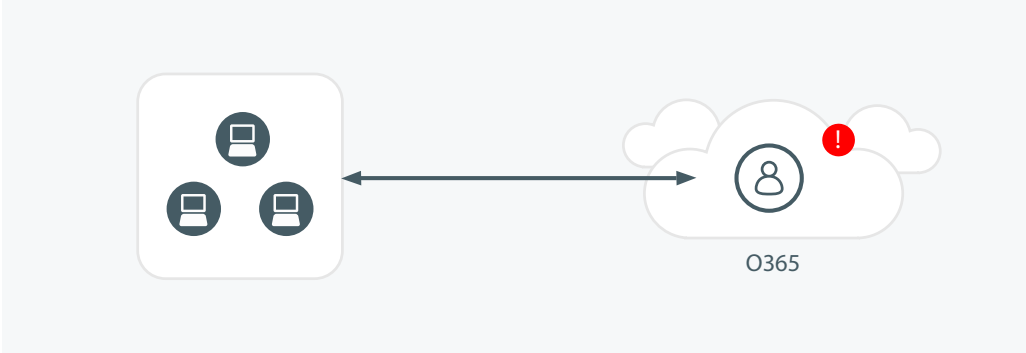
### Steps to Verify

- Investigate both the target and result of these operations to understand the potential impact.

- Top -

# O365 Suspicious SharePoint Operation

## Lateral Movement


MITRE | ATT&CK®

T1078 Valid Accounts

T1213 Data from Information Repositories

### Triggers

- Abnormal administrative SharePoint operations that may be associated with malicious activities.

### Possible Root Causes

- An attacker has located a SharePoint administrative account and is using it in pursuit of attack progression.
- A user whose learned activity baseline has been lost as a result of a prolonged leave of absence or a change in job function has returned to their regular job
- An admin's role may have evolved as part of a special project or assignment, requiring SharePoint operations previously outside their normal observed behavior.

### Business Impact

- SharePoint is often leveraged across organizations for data which may be sensitive in nature, and desirable to an attacker.
- There exists the potential for the full Office 365 subscription to be compromised if an admin account is taken over.

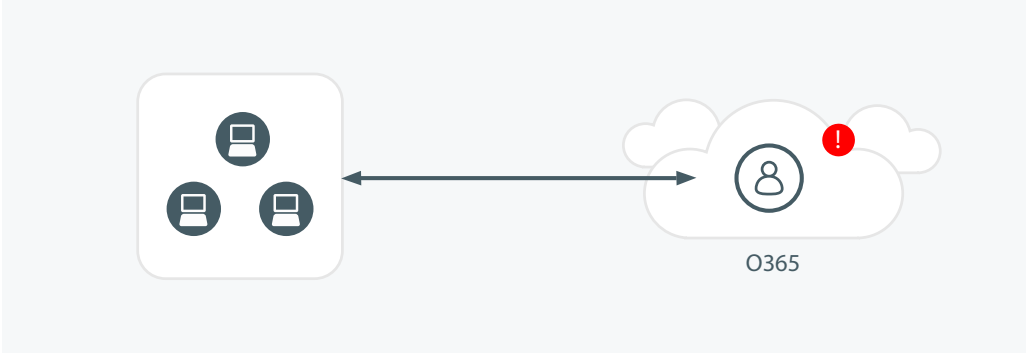
### Steps to Verify

- Investigate both the target and the effect of these operations to understand the full impact.

- Top -

# O365 Suspicious Teams Application

## Lateral Movement


MITRE | ATT&CK®

T1550 Use Alternate Authentication Material

T1528 Steal Application Access Token

## Triggers

- A rarely used, third-party Microsoft Teams integrated application has been granted excessive or risky permissions that may enable malicious activities to be taken on behalf of the authorizing user
- The threat score is statically assigned.
- The certainty score is statically assigned.

## Possible Root Causes

- An attacker is trying to trick the user into authorizing a third-party app that will allow the the attacker to execute malicious actions.
- In some cases rare, legitimate applications do require a set of permissions that are authorized despite the risk they present.

## Business Impact

- Malicious third-party apps can be used to undermine existing security controls, such as multi-factor authentication (MFA), and enable malicious action on behalf of the authorizing user, increasing risk to enterprise system and data and increasing the likelihood of further attack progression.
- A suspicious teams application could result in outcomes ranging from the compromise of an individual account or host, to broader compromise of a full teams channel.
- Malicious apps may enable a foothold into the environment as a means of maintaining persistent access.
- Malicious apps could may allow the collection of sensitive information or act as a mechanism to support data exfiltration.

## Steps to Verify

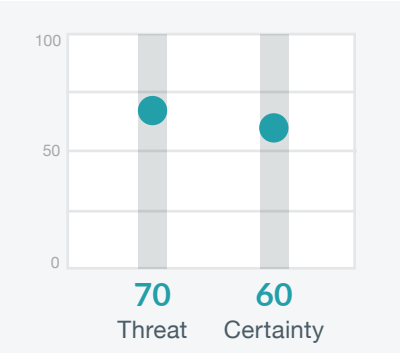
- Verify that the application in question is authorized for the associated user.
- Validate that the required permission set is appropriate for the authorized business process associated with this application.
- Investigate for additional malicious indicators associated with this application or user.

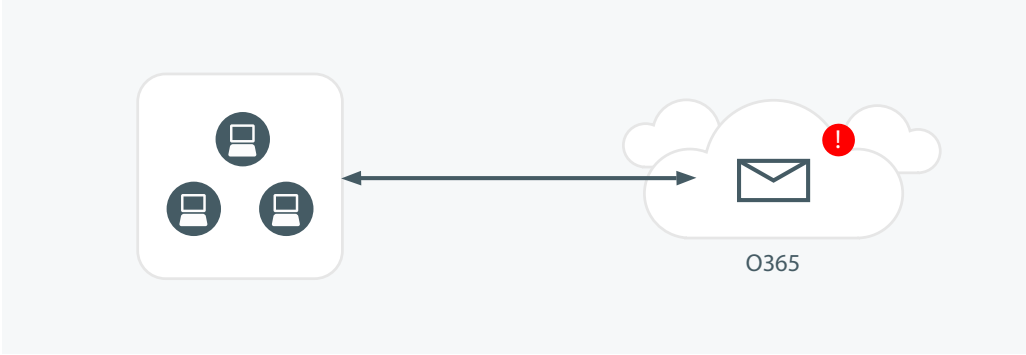
- Top -

# Azure AD Unusual Scripting Engine Usage

## Lateral Movement




MITRE | ATT&CK®

T1059 Command and Scripting Interpreter

## Triggers

- An account has executed O365 operations with either tools, scripting engines or command line interfaces which could be\u00a0maliciously used by attackers.
- The threat score is driven by the quantity of operations executed by the account.
- The certainty score is driven by the uniqueness of the User Agent reported for the account.

## Possible Root Causes

- An attacker is \"living off the land\" through the misuse of authorized tools (curl, AutoHotKey32, etc.) to extend their attack.
- An attacker has used a scripting engine (Powershell, Python, and others) to build and execute attack tools.
- When attacker is not careful, the default User Agent strings are submitted by these tools, indicating that the operation is not done interactively by a legitimate human user.
- Automation tools and scripts are sometimes used by power users and IT personnel to access O365.

## Business Impact

- Automated tools increase attack speed and volume while reducing human error, and attackers that successfully leverage them have an opportunity to move faster and in some cases with a lower chance of detection.
- Use of automation tools is a \"force multiplier\" that increases chances of successful breaches and data exfiltration, significantly increasing risks to the enterprise.

## Steps to Verify

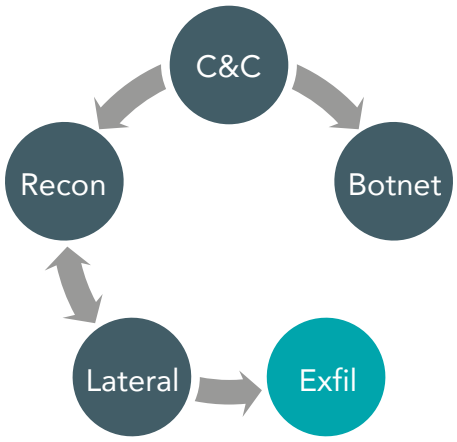
- Investigate O365 operation in context of the user, verify if this user would reasonably conduct these types of operations.
- Investigate tooling or scripting engine to validate if this is an appropriate and approved tool for a user of this type.

- Top -

## Category

# Exfiltration

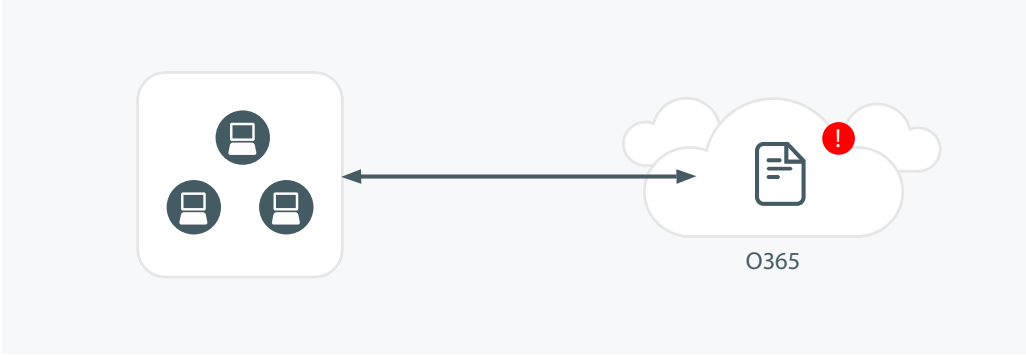
- Covers scenarios where data is being sent outside or collected in a way meant to hide the data transfer
- While data is constantly being sent out of the network or cloud environment, it usually does not involve the use of techniques meant to hide the transfer
- The host or account transmitting the data, where it is transmitting the data, the amount of data and the technique used to send it all provide indicators of exfiltration




- Top -

# O365 eDiscovery Exfil

## Exfiltration


MITRE | ATT&CK®

T1048 Exfiltration Over Alternative Protocol

### Triggers

- A user is previewing or downloading the results of an eDiscovery activity.

### Possible Root Causes

- An adversary has gained access to eDiscovery capabilities and is using that access to collect or exfiltrate data.
- One of a small set of users authorized to perform eDiscovery has been observed doing so.

### Business Impact

- eDiscovery capabilities provide an enticing target for adversaries to abuse and may result in the loss of sensitive information up to and including passwords, encryption keys, and even financial data or intellectual property.
- eDiscovery capabilities may include data traditionally inaccessible through other means but preserved as part of a litigation hold.

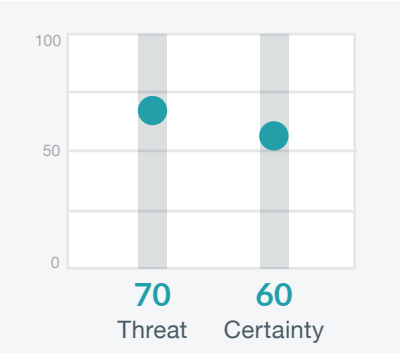
### Steps to Verify

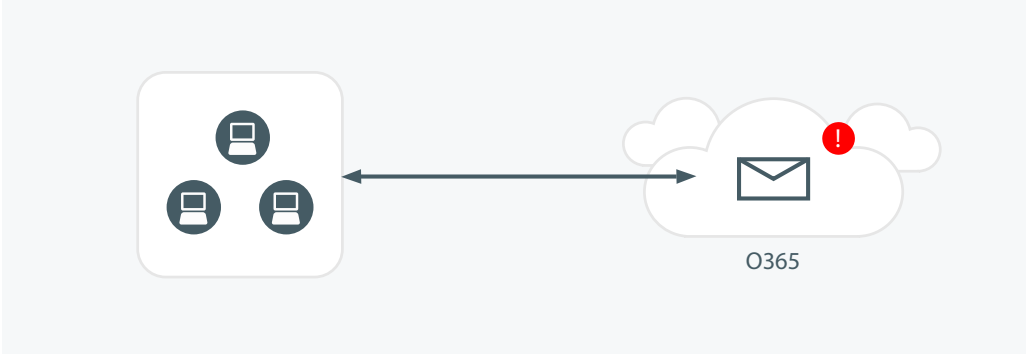
- eDiscovery activities from unauthorized users should be immediately investigated.
- Users authorized for eDiscovery should be explicitly triaged in this system to avoid future detections.

- Top -

# O365 Exfiltration Before Termination

## Exfiltration




MITRE | ATT&CK®

T1213 Data from Information Repositories

### Triggers

- The risk of insider threat has been observed by an account downloading or exfiltrating files prior to that account being deleted or disabled.
- Threat scores are assigned a static value.
- Certainty scores are assigned a static value.

### Possible Root Causes

- A user with foreknowledge of separation or reassignment has intentionally acquired or stolen organizational data prior to departure with the intent to retain access to information or data for which they will no longer be authorized access.
- In some cases, suspicious data acquisition by a user prior to a separation or reassignment event may be part of an authorized activity.

### Business Impact

- Insider threat places an organization at risk of loss of sensitive information such as intellectual property, financial data, or other data associated with legal and compliance protections.
- The successful exfiltration of data by an insider may lead to regulatory fines or penalties, loss of competitive advantages, or other outcomes detrimental to business and organizational success.

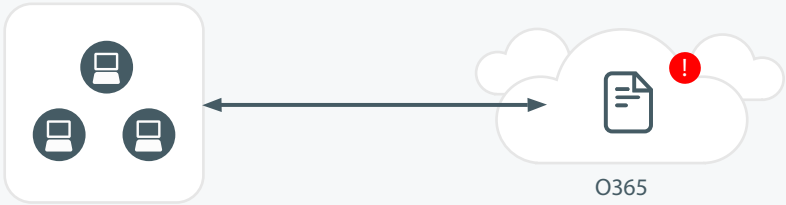
### Steps to Verify

- Investigate the reason this account was disabled or deleted, and if maintaining access to these files continues to be authorized.
- Investigate if the files associated with this detection include sensitive information.

- Top -

# O365 Suspicious Download Activity

## Lateral Movement


MITRE | ATT&CK®

T1567 Exfiltration Over Web Service

### Triggers

- An account was seen downloading an unusual number of objects compared to the user's past behavior or the behavior of other O365 users.
- The Threat score is driven by a combination of factors which include the quantity of objects downloaded, the relative rarity associated with downloading those objects, and rarity of downloading from the source sites for those objects.
- The Certainty score is driven by a combination of factors which include a historic baseline of that user's download volumes, a comparison of that user relative to other users, and dimensions related to the locations where these objects have been downloaded from.

### Possible Root Causes

- An attacker may be using SharePoint / OneDrive download functions to exfiltrate data.
- Users downloading an unusually large number of files as they start new projects, back up data or access multiple files to support their job function.

### Business Impact

- Ability to exfiltrate a significant number of sensitive files from the enterprise is often the last stage of the security compromise.
- Exfiltration of sensitive business data may lead to loss of control of company secrets and intellectual property.

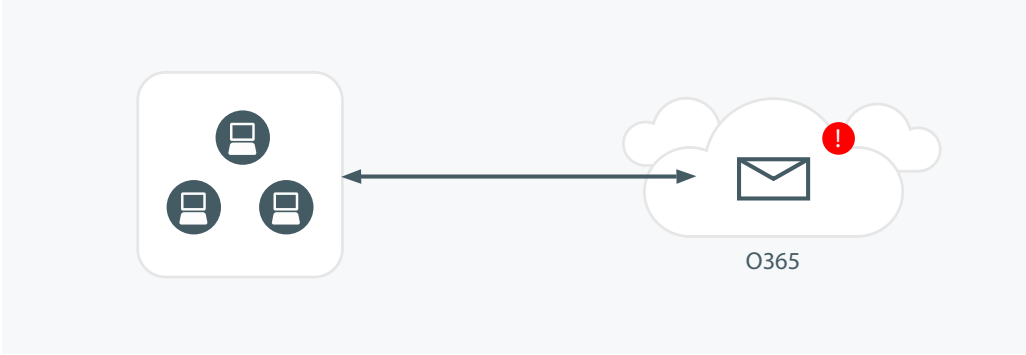
### Steps to Verify

- Review the details and contents of the files to assess risk, and validate these are authorized downloads.
- Review additional detections and events by the source user which may indicate their account has been compromised.

- Top -

# O365 Suspicious Exchange Transport Rule

## Exfiltration


MITRE | ATT&CK®

T1114 Email Collection

## Triggers

- A new Exchange transport rule has been created with a potentially risky action that may provide email collection, exfiltration, or deletion capabilities (BlindCopyTo, CopyTo, Delete).
- The threat score is statically assigned.
- The certainty score is statically assigned.

## Possible Root Causes

- An attacker has gained Exchange administrator access with the capabilities of forwarding sensitive emails prior to their arrival in a user's inbox to an attacker controlled email address (internal or external).
- An attacker may be preparing to delete important emails prior to their arrival in a user's inbox to prevent important alerts or notifications from occurring.
- A legitimate transport rule was added to support business requirements or prevent dangerous emails from reaching user inboxes.

## Business Impact

- Because email services are critical to so many enterprise activities, attackers prioritize access both as a means of progressing an attack as well as a mechanism for data exfiltration.
- Forwarded emails may expose sensitive data.
- Deleted emails may mask security alerts or important emails alerting an organization to a breach.
- The combination of forwarded and deleted emails may allow an external party to impersonate internal users to further their goals.

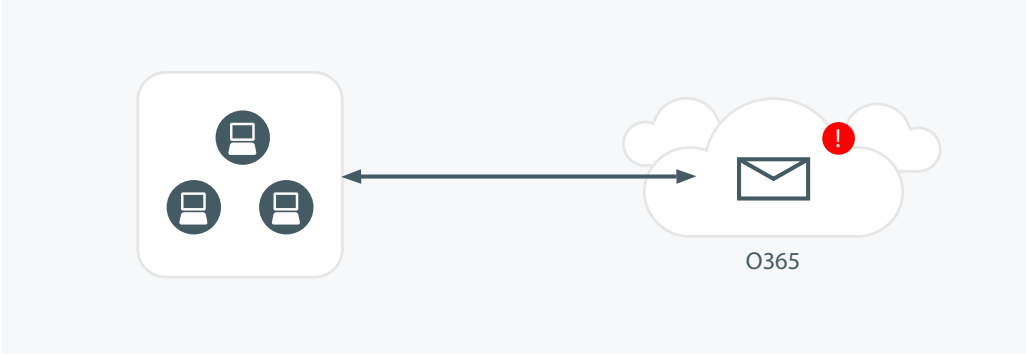
## Steps to Verify

- Validate the new transport rule serves a business purpose, does not create a risk of data exposure, and has been implemented according to proper change control processes.

- Top -

# O365 Suspicious Mail Forwarding

## Exfiltration


MITRE | ATT&CK®

T1114 Email Collection

### Triggers

- Mail forwarding which may be used as a collection or exfilltration channel for an adversary has been observed.

### Possible Root Causes

- An external attacker has established persistent access to contents of a specfic mailbox without the need to otherwise maintain any kind of persistence through installing software.
- Employee life-cycle activities such as a permanent separation or a temporary leave of absence may legitimately require mailbox modifications which could triggering this detection.
- Emails belonging to executives may be forwarded to their associated administrative assistants.
- Emails for service accounts may be forwarded to the staff members who manage those services.

### Business Impact

- Attackers who have gained persistence through the email systems may passively collect and exlfiltrate data.
- Sensitive business information often resides in email systems and may be leaked through e-mail theft.

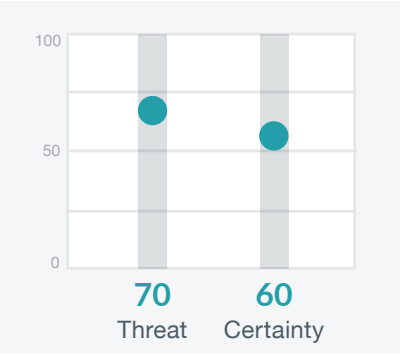
### Steps to Verify

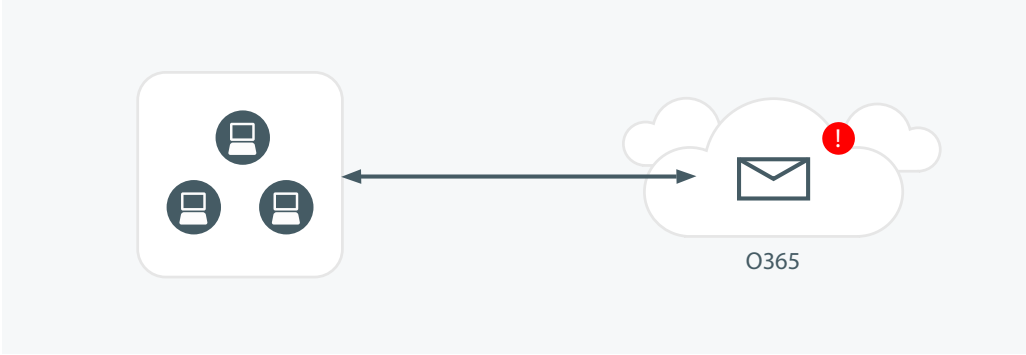
- Verify if sensitive data has been unintentionally forwarded using this feature.

- Top -

# O365 Suspect Power Automate Activity

## Exfiltration




MITRE | ATT&CK®

T1041 Exfiltration Over C2 Channel

T1008 Fallback Channels

T1059 Command and Scripting Interpreter

T1020 Automated Exfiltration

## Triggers

- Abnormal Power Automate activity was observed from a user in the environment.
- A user leveraged a Power Automate flow connector that was unusual for either the user or the environment.
- A user modified another user existing flow in a suspect manner.

## Possible Root Causes

- An attacker may be creating automated tasks within the environment to secretly exfil, manipulate data for impact, or create network control channels.
- A normal user is attempting to subvert normal IT policies by leveraging native Microsoft infrastructure without authorization.
- One of a small set of users who are authorized to leverage Power Automate flow was observed doing so.

## Business Impact

- Power Automate, Microsoft's native and on-by-default O365 automation tool, can be leveraged by attackers to interact directly with internal data and infrastructure to facilitate data exfil or attack automation.

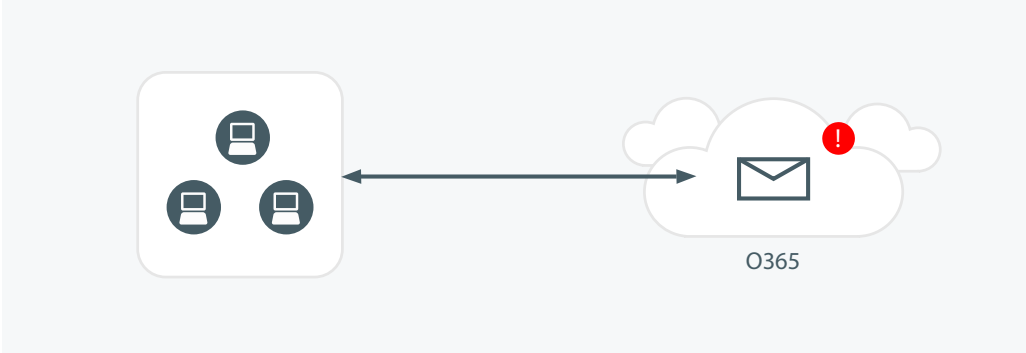
## Steps to Verify

- Power Automate activities involving unauthorized connectors should be investigated immediately.
- Users modifying other user's Power Automate flows should have explicit permission to do so.
- Users authorized for Power Automate activities should be explicitly triaged to avoid future detections.

- Top -

# O365 Suspicious Sharing Activity

## Exfiltration


MITRE | ATT&CK®

T1213 Data from Information Repositories

### Triggers

- An account was seen sharing files and/or folders at a volume that is higher than is normal for both the environment and for the account.
- Threat is driven by the number of objects shared.
- When mosts users do not share normally the, certainty is drive by how uncommon sharing is for all users. When sharing is normally observed, certainty is driven by a combination of the amount of deviation from the user's normal shared object volume and the proportion of objects shared from directories other than the user's personal directory.

### Possible Root Causes

- Attackers may use SharePoint/OneDrive sharing functions to exfiltrate data and enable on-going access to data over extended periods of time.
- Use of sharing enables attackers to maintain access to data after an a compromised account is remediated
- Users who rarely share files may periodically share more files than most other users in the environment as part of their job function.

### Business Impact

- While some level of sharing may be normal for an environment or user, those users who emerge as sharing unusual amounts of data should be reviewed to validate the sharing is legitimate and does not pose a risk.
- Sharing of a large volume or breadth of files or folders exposes the organization to an increased risk of data theft or loss.

### Steps to Verify

- Review the data being shared to determine if the information should be exposed to external parties.
- Review the sharing permissions to ensure the least possible data is exposed.
- Validate with the user that the sharing was intended and follows organizational policies on data sharing with external parties.

- Top -

## Category
# Info

- Reports on new and novel events without directly impacting scoring
- New and novel events occur normally in most network and cloud environments and in most cases are not directly linked to threats
- Awareness of new and novel events support better situational awareness and provide additional context when observed with kill chain alerts





- Top -

## Azure AD Login Attempt to Disabled Account

- A login attempt for an account that has been explicitly disabled was observed within the environment, potentially indicating environment probing or attempted access by former employees.

## O365 Brute Force Attempt

- Reports when one or more external IPs are seen attempting to brute-force into an account without any successful attempts.



# Detect for AWS



# Kingpin Technology



Vectra attributes all of our detections to actionable User identities such as IAM Users, SAML Users, an External Account, or AWS Services.

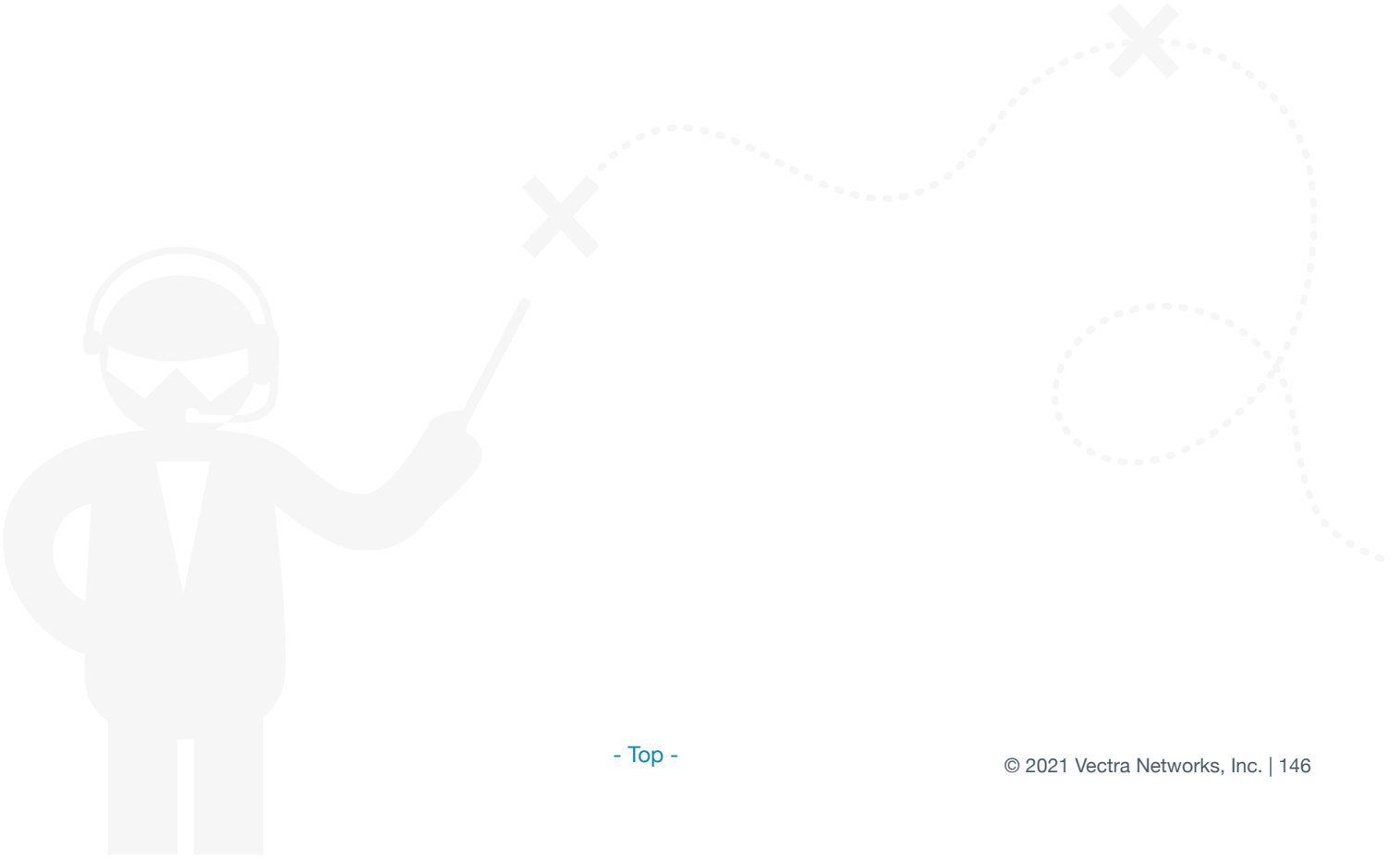
This is a complex problem because users in AWS are encouraged to assume other roles to perform actions, and actively discouraged to perform actions as the account they logged in with. In some cases, users will even assume roles after assuming a role in order to be able to perform certain actions. Our dedicated team of Data Scientists use advanced machine learning techniques to attribute any activity up to the original actor based on logged activity across your AWS account. When you see any AWS detections in our product, you will be able to see a chain of roles assumed by the actor before performing their action, which will explain how this user assumed this role.

- Top -

## Category

# Command & Control

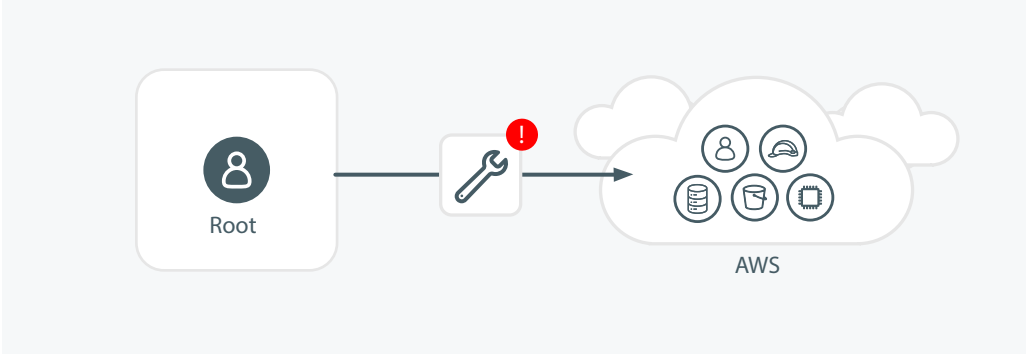
- An attacker is controlling an AWS account to orchestrate their attack against AWS infrastructure and services
- Attackers will access credential through various methods
- Attackers will control accounts in order to then perform reconnaissance and lateral movement in the name of achieving an object like data exfiltration or resource impact
- Actions are associated with Command and Control, Initial Access, Reconnaissance MITRE Tactics



- Top -

# AWS Root Credential Usage

## Command & Control


MITRE | ATT&CK®

T1078 Valid Accounts

## Triggers

- An action was taken by the root account.

## Possible Root Causes

- An attacker has compromised the root account and is using the unfettered access it grants to further their attack.
- Administrators are using the root account for normal activities, which is against best practices and should not be done.

## Business Impact

- Malicious use of the root account indicates significant opportunity for negative impact to organizational assets, services, and data to include disruptive impact and sensitive data loss.
- Misuse of the root account by admins for routine activities greatly elevates the risk of accidental damage or disruption.

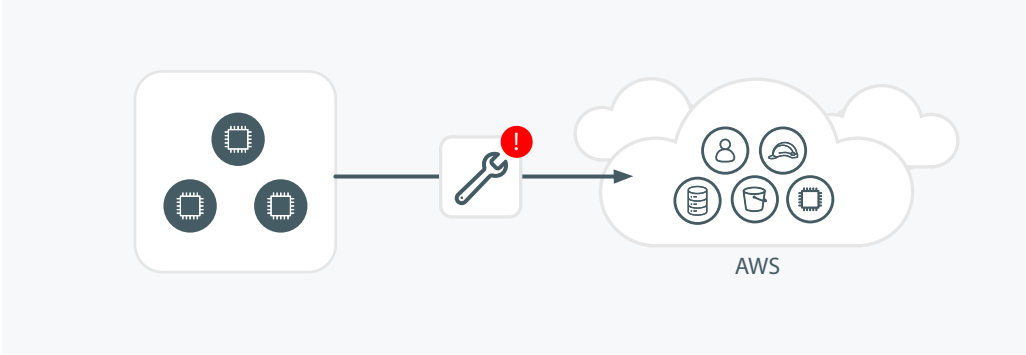
## Steps to Verify

- Review the activity completed by the root account for indications of malicious activity.
- Validate with the team responsible for administering AWS that they used the root account for an authorized activity.

- Top -

# AWS Suspicious Credential Usage

## Command & Control


MITRE | ATT&CK®

T1078 Valid Accounts

### Triggers

- EC2 generated temporary credential used outside of EC2.

### Possible Root Causes

- An attacker has extracted a temporary credential from an EC2 instance and is using it to further their attack.
- An application is using temporary credential generation via EC2s in an unusual way.

### Business Impact

- Attackers may use temporary credentials as a means of maintaining persistent command and control in an environment, which increases the risk of data loss or impacted assets and services.

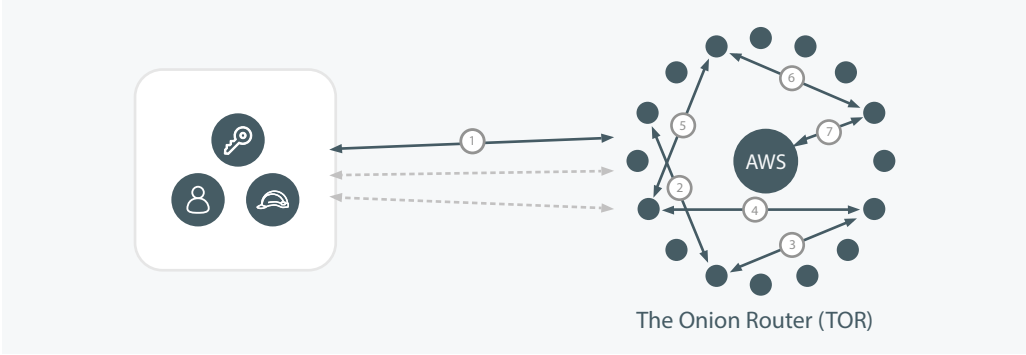
### Steps to Verify

- Review the actions being undertaken by the credential after the identified activity and potential risk posed by that access.
- Discuss with the EC2 instance owners to determine if the use of instance generated temporary keys outside of EC2 is known and legitimate.
- If the review determines there is a high risk to data or the environment, disable the credentials and perform a comprehensive investigation.

- Top -

# AWS TOR Activity

## Command & Control


MITRE | ATT&CK®

T1090 Proxy

## Triggers

- A credential was observed accessing the environment from a known anonymized (TOR) exit node.

## Possible Root Causes

- An attacker is using an anonymizing proxy like TOR to obfuscate details of their source connection or make an investigation more difficult by using multiple source IP addresses.
- A user may be intentionally using TOR to circumvent restrictions preventing access to the resources in question, such as those applied by the country they are accessing from.

## Business Impact

- Attackers identified under this detection are actively operating within the environment while maintaining some level of operational security by obfuscating their source details.
- Attackers operating using TOR will reduce the ability of teams to connect identified attacker behavior with other behaviors not yet identified since it enables the attacker to regularly change the source detail of their connections while undertaking operations within the environment.
- Authorized users that have adopted TOR may be in violation of IT Policies and be placing organizational assets at risk.

## Steps to Verify

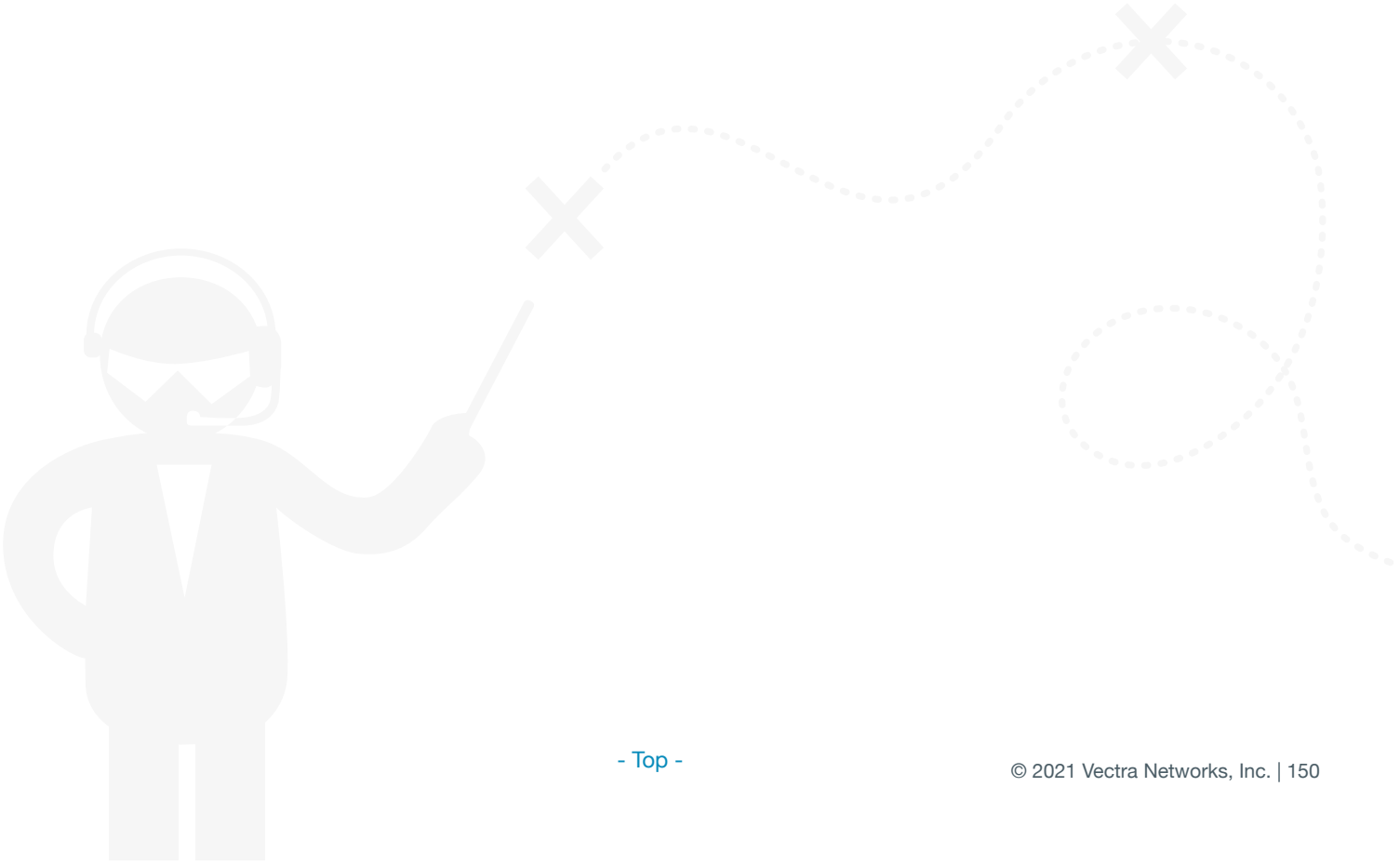
- Review the actions being undertaken by the user after the identified activity and potential risk posed by that access
- Review security policy to determine if the use of TOR is allowed.
- Discuss with the user to determine if the use of TOR is known and legitimate.
- If the review determines there is a high risk to data or the environment, disable the credentials and perform a comprehensive investigation.

- Top -

## Category

# Reconnaissance

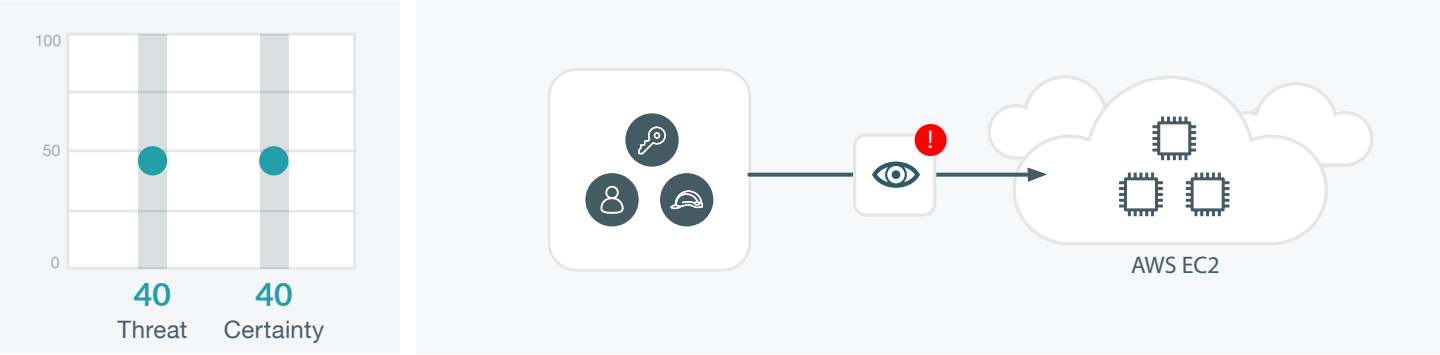
- An attacker is surveying and learning about AWS infrastructure
- Attackers with control of an account will look to identify paths to their final objectives
- Attackers will probe AWS services in-order to find credentials to gain additional access
- Attackers will identify services in order to collect, exfiltrate, or impact data
- Actions are associated with the Discovery MITRE Tactic



- Top -

# AWS EC2 Enumeration

## Reconnaissance




MITRE | ATT&CK®

T1526 Cloud Service Discovery

### Triggers

- Credential was observed performing a set of anomalous API requests that can be associated with the discovery or subsequent phases of an attack.

### Possible Root Causes

- An attacker may be actively looking for privilege escalation opportunities.
- A security or IT service may intentionally be enumerating these APIs for monitoring reasons.

### Business Impact

- Privilege escalation may indicate the presence of an adversary that is modifying permissions to progress towards an objective.

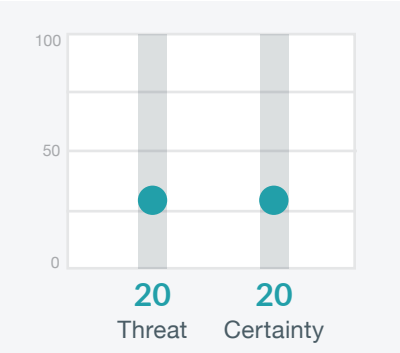
### Steps to Verify

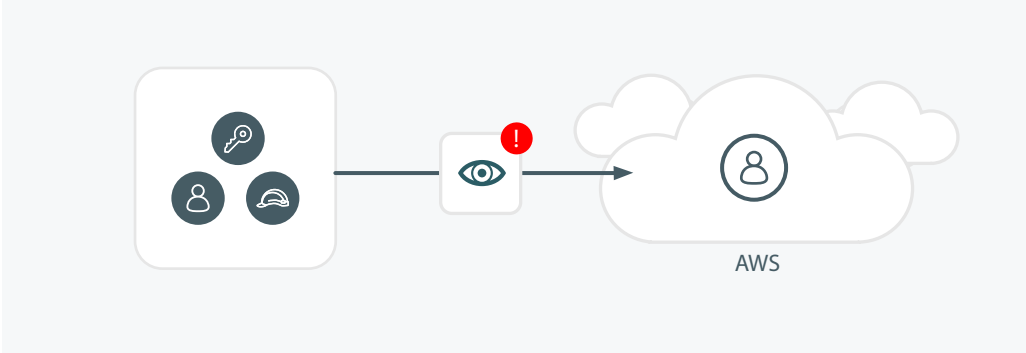
- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Organization Discovery

## Reconnaissance




MITRE | ATT&CK®

T1580 Cloud Infrastructure Discovery

T1614 System Location Discovery

### Triggers

- A user lists AWS account aliases via ListAliases or retrieves details for the AWS organization via DescribeOrganization

### Possible Root Causes

- An attacker is enumerating details on the AWS organization to further their attack planning and next steps.
- An administrator or user is retrieving organization details as part of their normal duties.
- Automation in the environment is collecting these details to support additional activities.

### Business Impact

- Recon may indicate the presence of an adversary gaining details necessary to support additional malicious activities within the environment.

### Steps to Verify

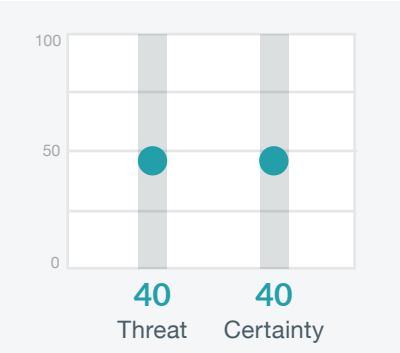
- Investigate the account context that performed the action for other signs of malicious activity.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

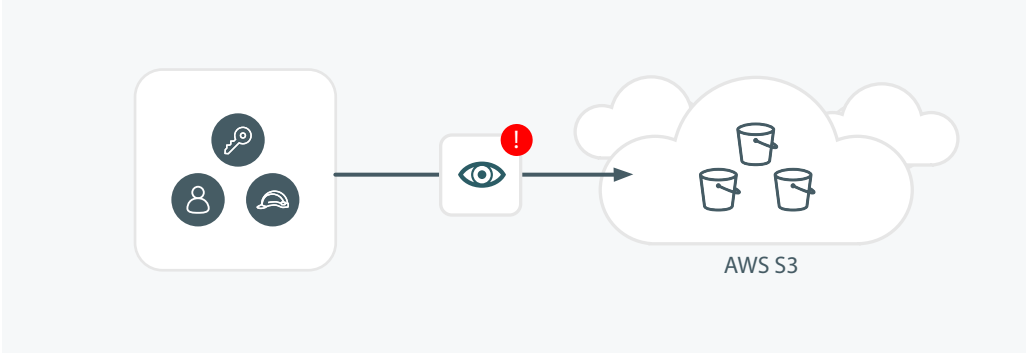
- Top -

# AWS S3 Enumeration

## Reconnaissance




MITRE | ATT&CK®

T1526 Cloud Service Discovery

### Triggers

- Credential was observed performing a set of anomalous API requests that can be associated with the discovery or subsequent phases of an attack.

### Possible Root Causes

- An attacker may be actively looking for privilege escalation opportunities.
- A security or IT service may intentionally be enumerating these APIs for monitoring reasons.

### Business Impact

- Privilege escalation may indicate the presence of an adversary that is modifying permissions to progress towards an objective.

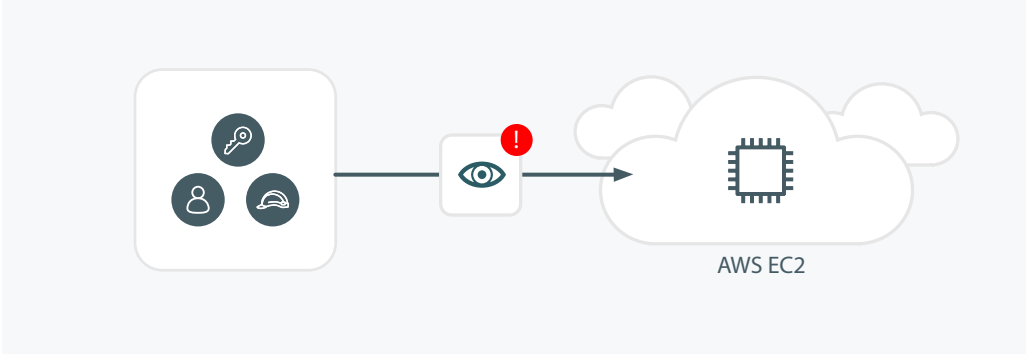
### Steps to Verify

- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Credential Access from EC2

## Reconnaissance


MITRE | ATT&CK®

T1552 Unsecured Credentials

## Triggers

- A set of AWS control plane APIs commonly used to search EC2 user data on EC2 resources for credentials was invoked in an unusual way that may be associated with a potential attack.

## Possible Root Causes

- An attacker is searching for credentials inside of the EC2 user data to pivot in the environment.
- An authorized administrator is performing an unusual activity commonly associated with attack progression.

## Business Impact

- Lateral movement may indicate that an adversary has established a foothold in the environment and is progressing towards their objective, increasing the risk of material impact.

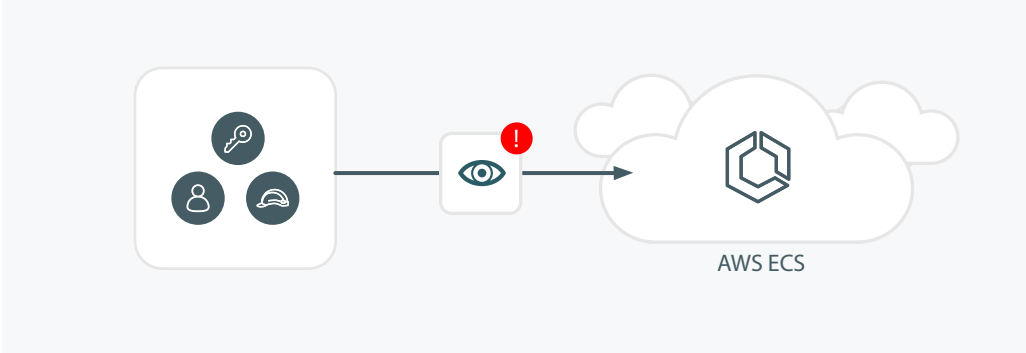
## Steps to Verify

- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Credential Access from ECS

## Reconnaissance


MITRE | ATT&CK®

T1552 Unsecured Credentials

## Triggers

- Credential was observed performing a set of API requests to retrieve a broad range of container configuration details which may further their attack through the leak of credentials or other data about the environment.

## Possible Root Causes

- An attacker may be actively looking for privilege escalation opportunities.
- A security or IT service may intentionally be enumerating these APIs for monitoring or configuration management reasons.

## Business Impact

- Stolen credentials allow an adversary to leverage authorized services and APIs to extend their attack which can be difficult for traditional security solutions to detect.
- Abused credentials are typically associated with impactful attacks, and if unmitigated may increase the likelihood that an adversary may inflict a loss of data or service availability.

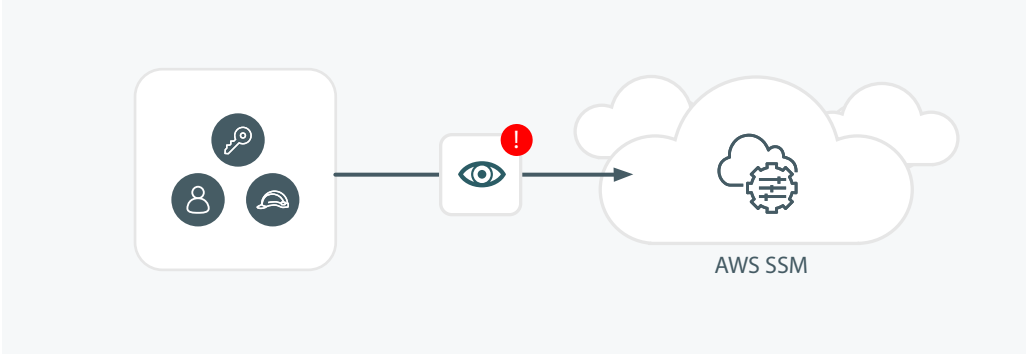
## Steps to Verify

- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Credential Access from SSM

## Reconnaissance


MITRE | ATT&CK®

T1552 Unsecured Credentials

### Triggers

- Credential was observed performing a set of API requests to list and then retrieve parameters within the AWS parameter store.

### Possible Root Causes

- An attacker may be actively looking for privilege escalation opportunities.
- A security or IT service may intentionally be enumerating these APIs for monitoring or configuration management reasons.

### Business Impact

- Stolen credentials allow an adversary to leverage authorized services and APIs to extend their attack which can be difficult for traditional security solutions to detect.
- Abused credentials are typically associated with impactful attacks, and if unmitigated may increase the likelihood that an adversary may inflict a loss of data or service availability.

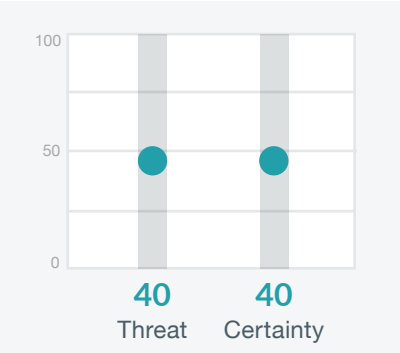
### Steps to Verify

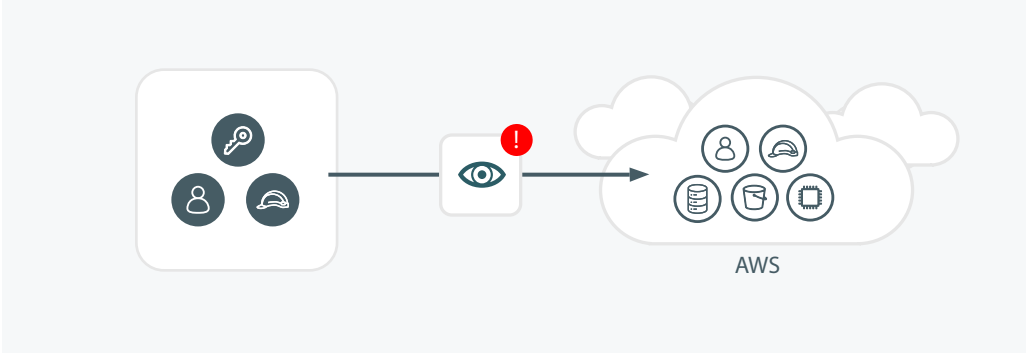
- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that parameters requested do not contain sensitive details, such as credentials. If they do, investigate those credentials for potential malicious use.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Escalation Reconnaissance

## Reconnaissance




MITRE | ATT&CK®

T1069 Permission Groups Discovery

### Triggers

- Credential was observed performing a set of unusual API requests that can be associated with the discovery or subsequent phase of an attack.

### Possible Root Causes

- An attacker may be actively looking for privilege escalation opportunities,
- A security or IT service may intentionally be enumerating these APIs for monitoring reasons.

### Business Impact

- Privilege escalation may indicate the presence of an adversary that is modifying permissions to progress towards an objective.

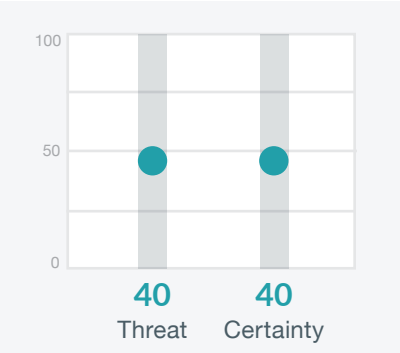
### Steps to Verify

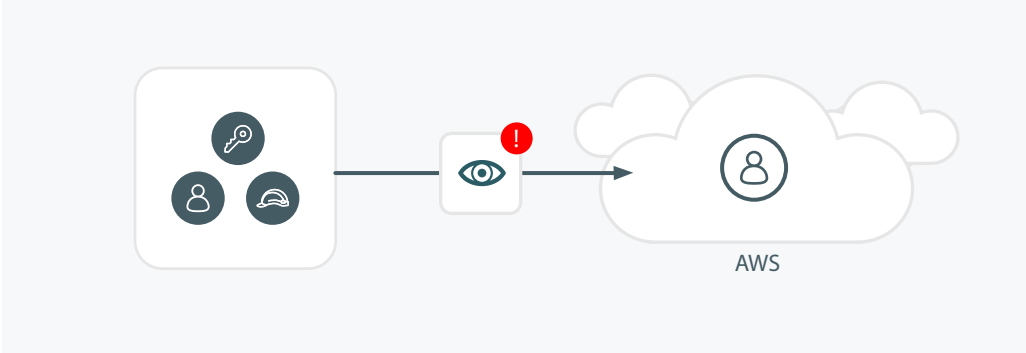
- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS User Permissions Enumeration

## Reconnaissance




MITRE | ATT&CK®

T1069 Permission Groups Discovery

### Triggers

- Credential was observed performing a set of unusual API requests that can be associated with the discovery or subsequent phase of an attack.

### Possible Root Causes

- An attacker may be actively looking for privilege escalation opportunities,
- A security or IT service may intentionally be enumerating these APIs for monitoring reasons.

### Business Impact

- Privilege escalation may indicate the presence of an adversary that is modifying permissions to progress towards an objective.

### Steps to Verify

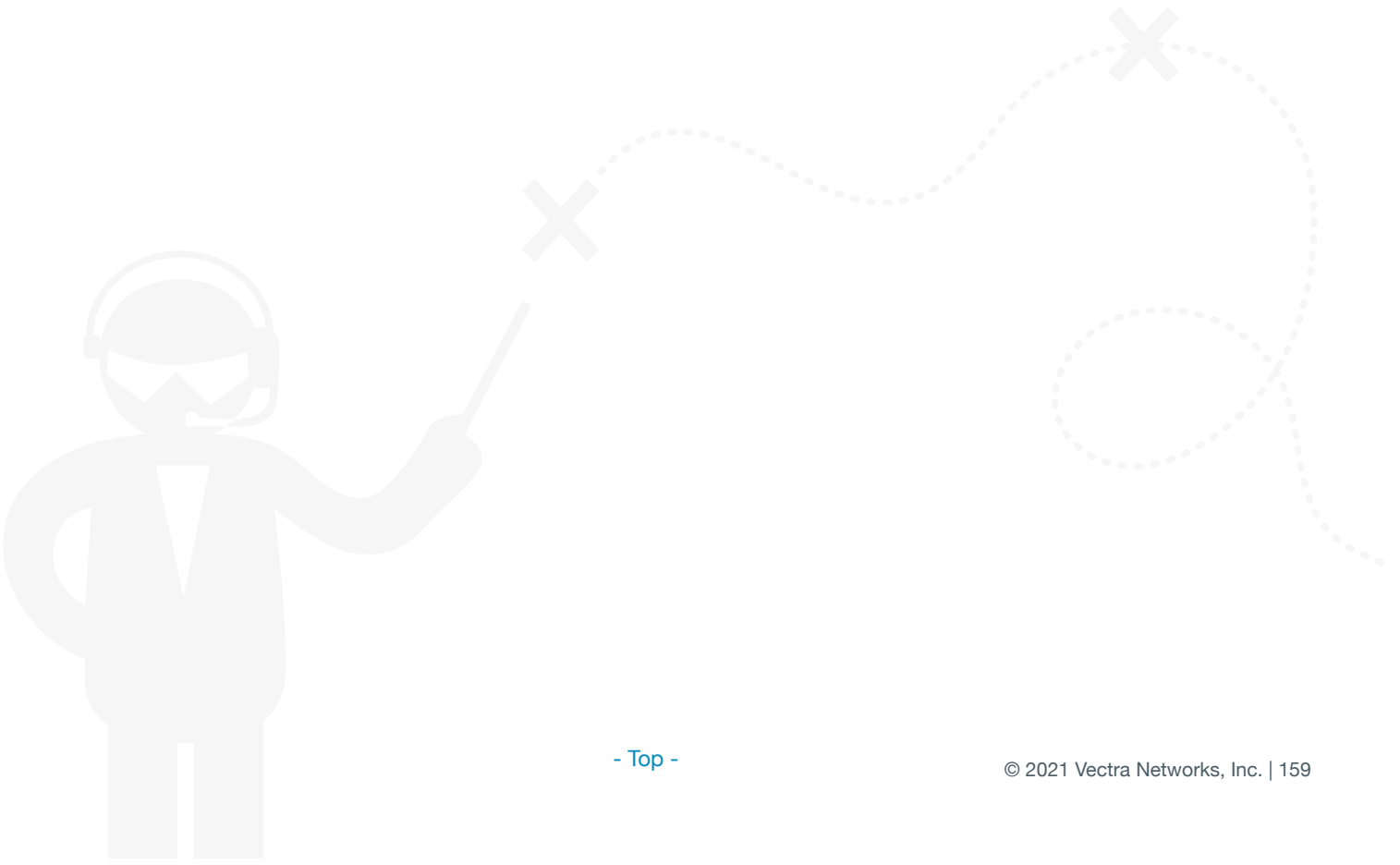
- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

## Category

# Lateral Movement

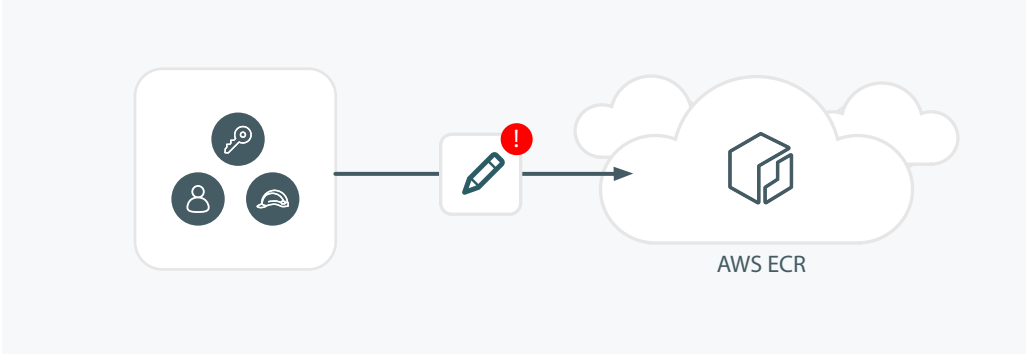
- An attacker in the AWS environment is spreading and taking actions that ensure continuous undetected access
- Attackers after gaining access to the credentials and discovering the environment will propagate and solidify their access
- Attackers will take actions to modify services and identifies to ensure continued access
- Attackers will leverage credentials within their defined permissions but for non-intended purposes to further the attacker's objective
- Actions are associated with Execution, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement, Credential Access MITRE Tactics



- Top -

# AWS ECR Hijacking

## Lateral Movement


MITRE | ATT&CK®

T1525 Implant Internal Image

### Triggers

- After enumerating ECR repositories and enumerating the images within those repositories, the attacker requests an authorization token for an image.

### Possible Root Causes

- An attacker is inserting a backdoor into an existing image.
- An ECR administrator is making an authorized change to the image.

### Business Impact

- Lateral movement may indicate that an adversary has established a foothold in the environment and is progressing towards their objective, increasing the risk of material impact.
- An inserted backdoor may provide hidden access persistence within the environment, allowing attackers to return to the environment after eviction.

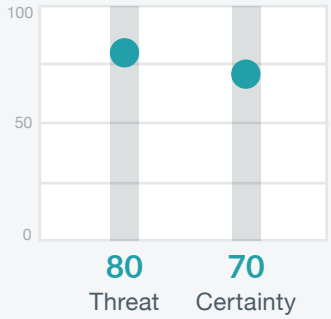
### Steps to Verify

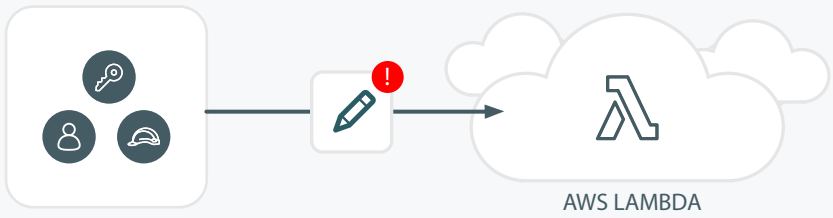
- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Lambda Hijacking

## Lateral Movement




MITRE | ATT&CK®

T1525 Implant Internal Image

### Triggers

- After enumerating Lambda functions and IAM roles, create a Lambda function, and add a new rule to that Lambda function.

### Possible Root Causes

- An attacker is creating a Lambda function that serves as a backdoor into the environment.
- An administrator is creating a Lambda function with a trigger for legitimate reasons.

### Business Impact

- Lateral movement may indicate that an adversary has established a foothold in the environment and is progressing towards their objective, increasing the risk of material impact.
- An inserted backdoor may provide hidden access persistence within the environment, allowing attackers to return to the environment after eviction.

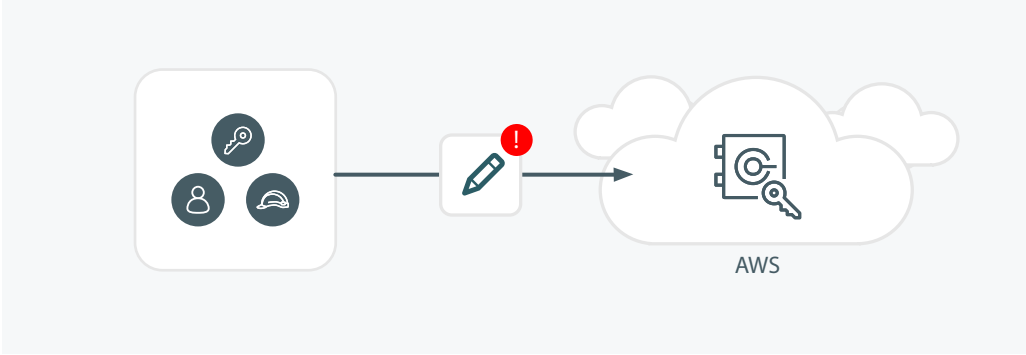
### Steps to Verify

- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Logging Disabled

## Lateral Movement


MITRE | ATT&CK®

T1562 Impair Defenses

### Triggers

- Disable or delete CloudTrail logging within a region where the logging is already enabled.

### Possible Root Causes

- An attacker has deleted CloudTrail logs to hide their tracks and/or has deleted the logs to prevent investigation of their historical activities.
- An administrator has disabled CloudTrail logging as part of normal changes to the environment.

### Business Impact

- Inability to detect future attacks, investigate future or historical attacks, or audit activity within the environment.
- Increased risk of activity that may negatively impact the business going unnoticed.

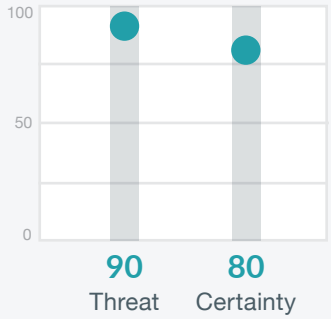
### Steps to Verify

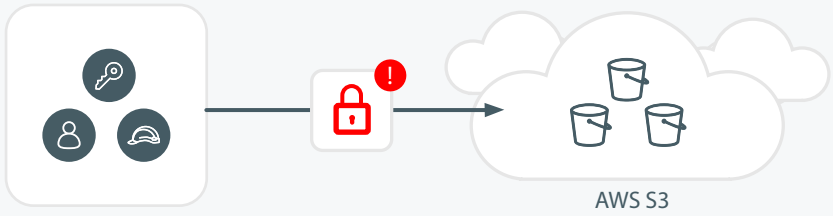
- Review the actions being undertaken by the user after the identified activity and potential risk posed by that access in regions where logging remains (if any).
- Review security policy to determine if the removal of logging capabilities is allowed.
- Discuss with the user to determine if the activity is known and legitimate.
- If the review determines there is a high risk to data or the environment, disable the credentials and perform a comprehensive investigation.

- Top -

# AWS Ransomware S3 Activity

## Lateral Movement




MITRE | ATT&CK®

T1486 Data Encrypted for Impact

### Triggers

- A large number of S3 objects were copied in a way that may indicate the encryption phase of ransomware activity in the environment.

### Possible Root Causes

- An attacker leveraging AWS APIs to encrypt S3 objects with the goal of demanding a ransom for the key to decrypt.
- Security or IT operations are manipulating and encrypting S3 objects in bulk as part of normal operations.

### Business Impact

- Ransomware attacks directly impact access to the organization's data and are popular among attackers due to the possibility of a quick transition from attack to monetization.
- After files have been encrypted, the attacker will ask the organization to pay a ransom in return for a promise to provide the encryption key which would allow the files to be decrypted.
- Even if an organization is willing to pay the ransom, there is no guarantee that the encryption key will be provided by the attacker or that the decryption process will work.

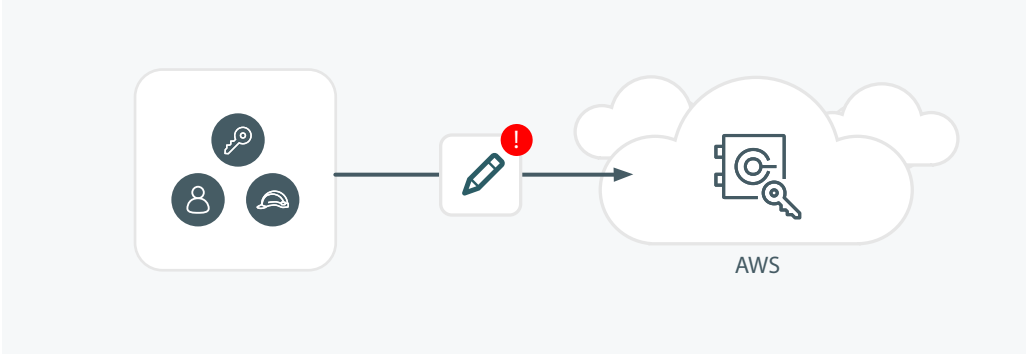
### Steps to Verify

- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this
- resource.
- If review indicates possible malicious actions or high-risk configuration, disable credential associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Security Tools Disabled

## Lateral Movement


MITRE | ATT&CK®

T1562 Impair Defenses

### Triggers

- Credential was observed performing a set of API requests capable of disabling native AWS security measures.

### Possible Root Causes

- Attackers are attempting to disable or downgrade AWS security mechanisms to blind defenders or to enable further malicious activities without the risk of detection.
- A security or IT service may intentionally be disabling security tools while troubleshooting problems.

### Business Impact

- Attackers who have successfully degraded, disabled, or bypassed security controls can more easily progress towards their objectives.
- Unintentional disabling of security controls increases the potential impact of both present and future attacks against the organization.

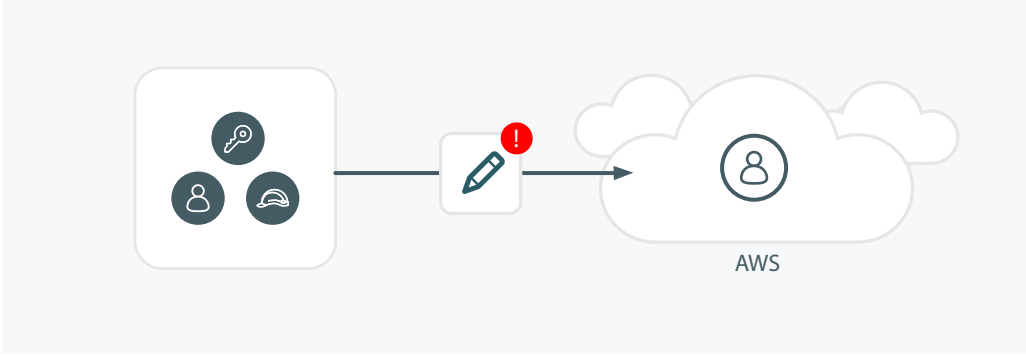
### Steps to Verify

- Review if this configuration is expected and appropriate in light of any available compensating controls.
- If this is a temporary configuration for troubleshooting purposes, confirm it has been reenabled once that troubleshooting is complete.

- Top -

# AWS Suspect Admin Privilege Granting

## Lateral Movement


MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

### Triggers

- Apply a highly permissive inline policy (i.e. ":" or "*:*") to a user, role, or group.

### Possible Root Causes

- An attacker is changing the permissions of a user, role, or group to enable them to leverage those permissions to gain additional or persistent access to the environment.
- An administrator has been granted highly permissive policies to enable them complete access to the environment.

### Business Impact

- Lateral movement may indicate that an adversary has established a foothold in the environment and is progressing towards their objective, increasing the risk of material impact.

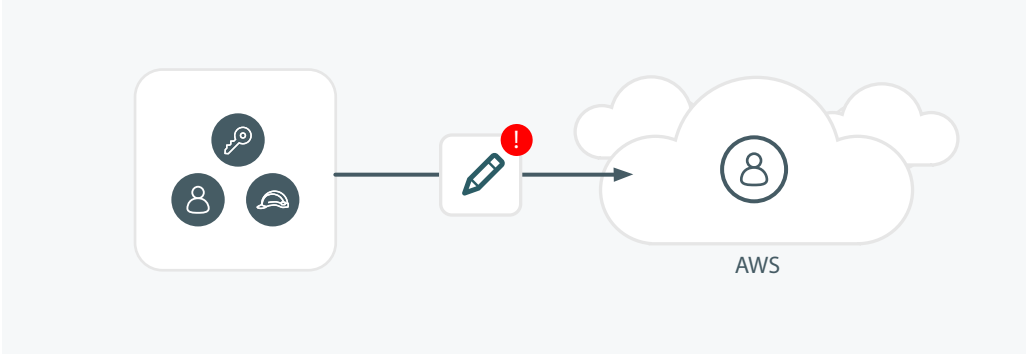
### Steps to Verify

- Investigate the account context that performed the action for other signs of malicious activity.
- Review whether this account should have access to the console for their normal duties.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Console Pivot

## Lateral Movement


MITRE | ATT&CK®

T1538 Cloud Service Dashboard

T1098 Account Manipulation

### Triggers

- An account enumerates users or obtains details on their own account, after which they request a token for console login and use that token to login to the console.

### Possible Root Causes

- An attacker is pivoting from the AWS API to the AWS management console to continue their attack progression.
- An administrator has started to use the AWS management console in an unusual way.

### Business Impact

- Lateral movement may indicate that an adversary has established a foothold in the environment and is progressing towards their objective, increasing the risk of material impact.

### Steps to Verify

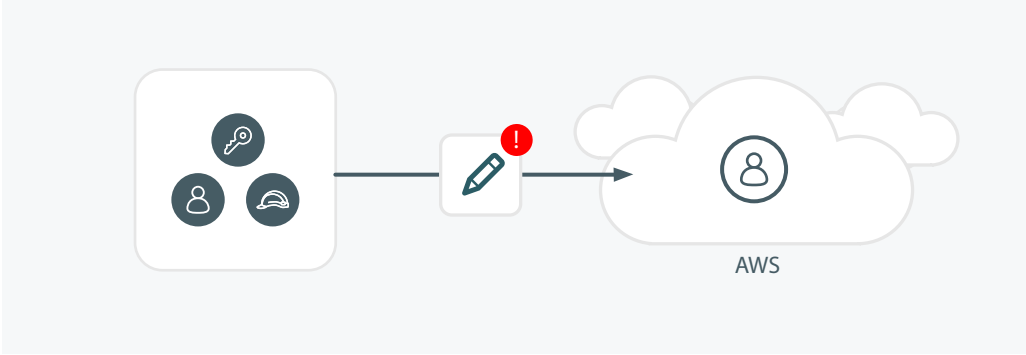
- Investigate the account context that performed the action for other signs of malicious activity.
- Review whether this account should have access to the console for their normal duties.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Login Profile Manipulation

## Lateral Movement


MITRE | ATT&CK®

T1098 Account Manipulation

### Triggers

- A source AWS account modifies the login profile of a target account, following which the target account accesses the AWS console.

### Possible Root Causes

- An attacker is enabling access to the console for credentials they have access to, to further their attack.
- An administrator has enabled console access for another user within the environment.

### Business Impact

- Lateral movement may indicate that an adversary has established a foothold in the environment and is progressing towards their objective, increasing the risk of material impact.

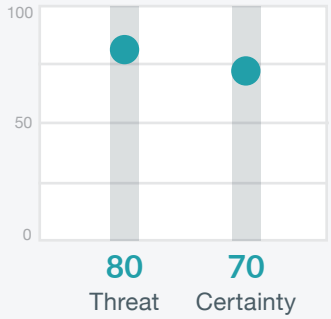
### Steps to Verify

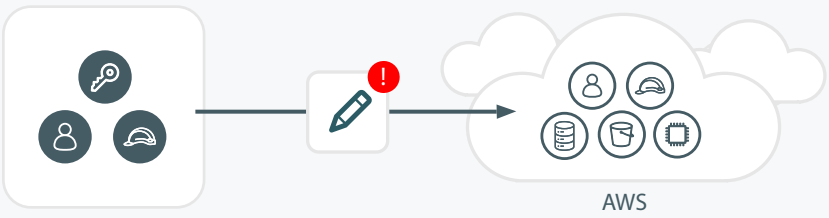
- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this
- resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Privilege Escalation

## Lateral Movement




MITRE | ATT&CK®

T1098 Account Manipulation

### Triggers

- Credential was observed performing a set of unusual API requests that enumerate privileges, following which a modification of privileges was observed which may be indicative of a privilege escalation occurring within the environment.

### Possible Root Causes

- An attacker has attempted to escalate privileges within the environment.
- An account misconfiguration has weakened IAM protections associated with resource authorizations.
- A security service, administrator, or other automation completed these actions as part of normal environment operation.

### Business Impact

- Privilege escalation may indicate the presence of an adversary that is modifying permissions to progress towards an objective.
- IT misconfigurations may act to increase the risk of impact to assets, data, or services.

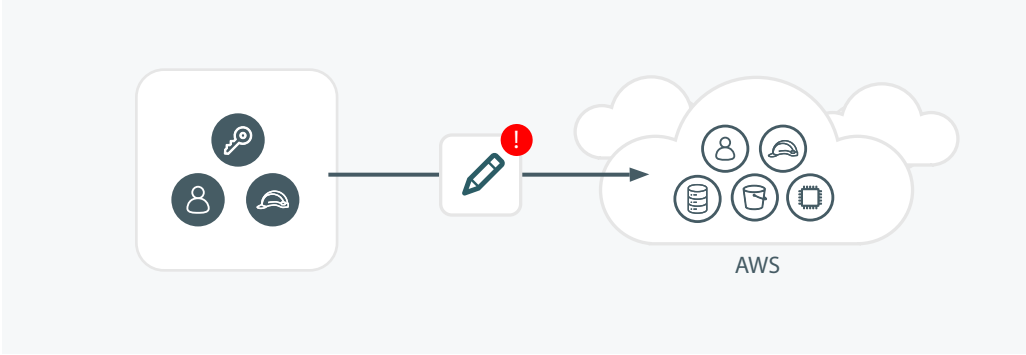
### Steps to Verify

- Investigate the account context that made the change for other signs of malicious activity.
- Validate that the modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS User Hijacking

## Lateral Movement


MITRE | ATT&CK®

T1098 Account Manipulation

### Triggers

- After enumerating users in the environment, add an access key to another user in the environment.

### Possible Root Causes

- An attacker is expanding access to additional users within the environment.
- Authorized IT Automation is using access keys to interact on behalf of other users within the environment.

### Business Impact

- Lateral movement may indicate that an adversary has established a foothold in the environment and is progressing towards their objective, increasing the risk of material impact.

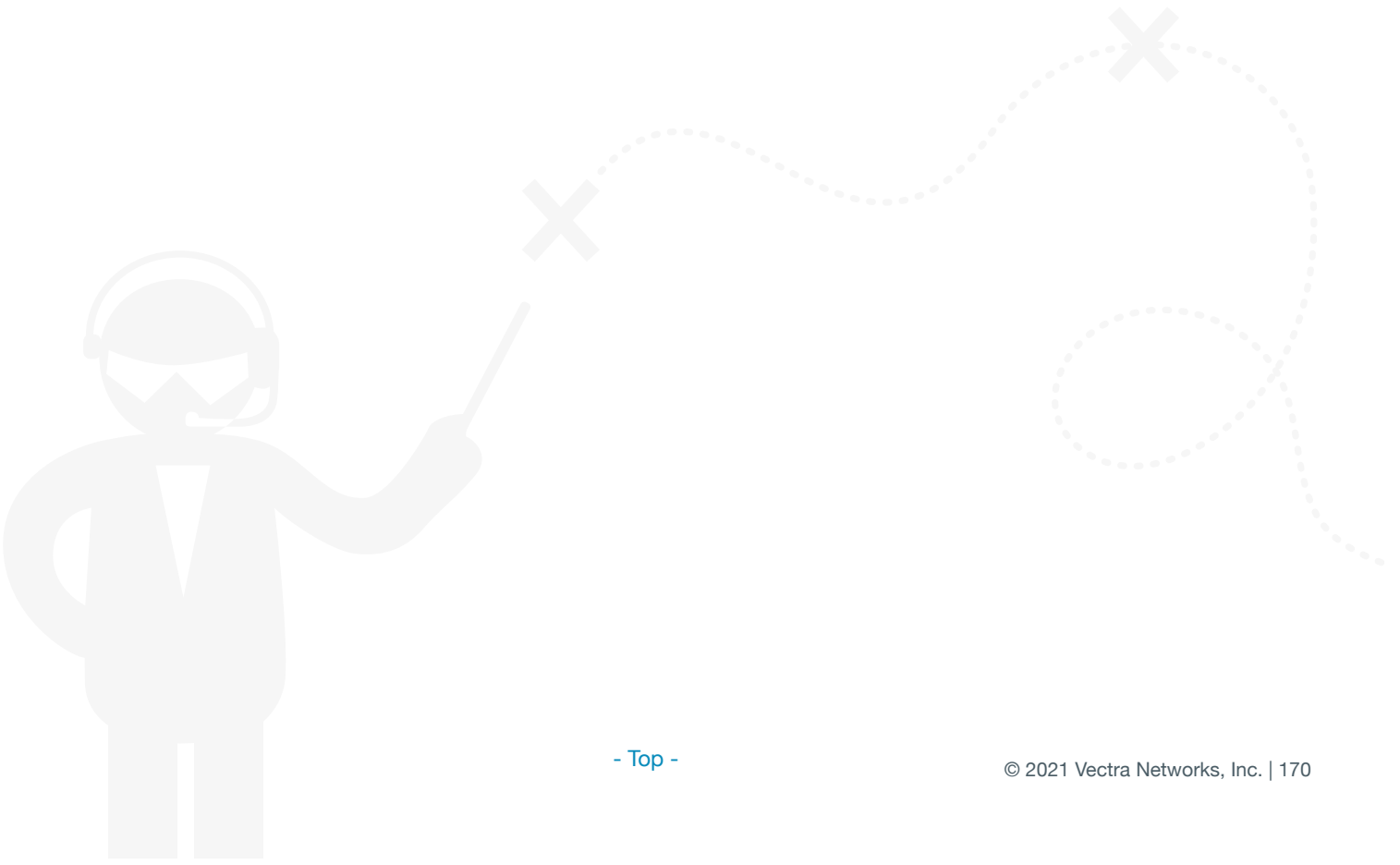
### Steps to Verify

- Investigate the account context that performed the action for other signs of malicious activity.
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

## Category
# Exfiltration

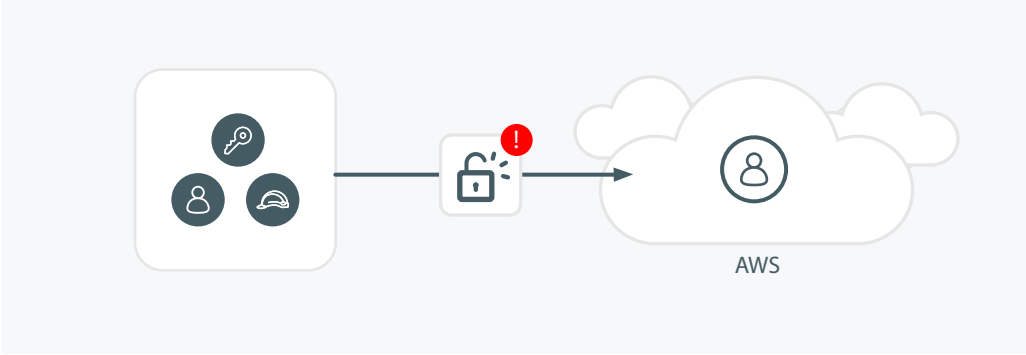
- An attacker with access to the AWS environment is collecting and removing data from the environment
- Attackers after gaining access and gaining sufficient permissions will steal high value data
- Attackers will take actions to modify services and identifies to ensure continued access
- Attackers will leverage credentials within their defined permissions but for non-intended purposes to further the attacker's objective
- Actions are associated with Execution, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement, Credential Access MITRE Tactics



- Top -

# AWS Suspect External Access Granting

## Exfiltration


MITRE | ATT&CK®

T1078 Valid Accounts

T1098 Account Manipulation

### Triggers

- A credential was observed enabling external access to AWS resources through an IAM role.

### Possible Root Causes

- An attacker may be creating a means of accessing data from a separate AWS account.
- A sanctioned third-party security or IT service may be granted access to AWS resources in order to perform normal activities.

### Business Impact

- Once an adversary achieves persistent access, they've established the opportunity to stage subsequent phases of an attack.

### Steps to Verify

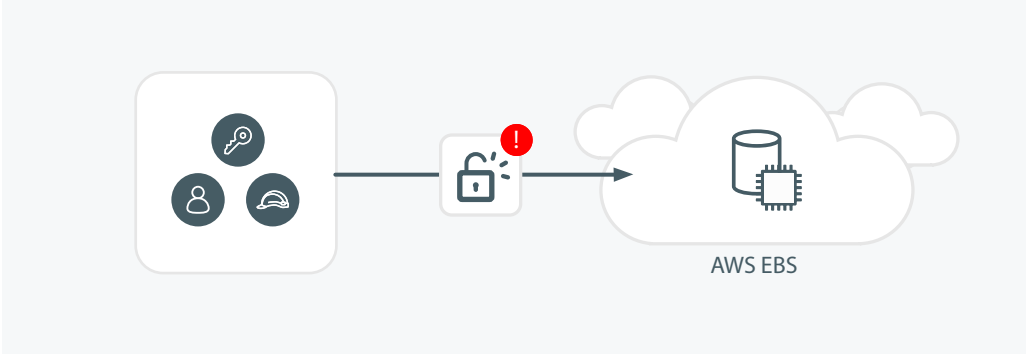
- Validate that the access is authorized, given the purpose and policies governing these resources.
- If review indicates possible malicious actions or high-risk configuration, delete the created IAM role and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Public EBS Change

## Exfiltration


MITRE | ATT&CK®

T1213 Data from Information-Repositories

T1530 Data From Cloud Storage Object

T1537 Transfer Data to Cloud Account

### Triggers

- A credential was observed performing a set of AWS control plane API actions related to exfiltration EC2 snapshots.

### Possible Root Causes

- An attacker may be actively looking for privilege escalation opportunities
- A security or IT service may intentionally be enumerating these APIs for monitoring reasons.

### Business Impact

- Exfiltration by an attacker of EC2 snapshots may expose details that support further attack progression, or lead to data loss.

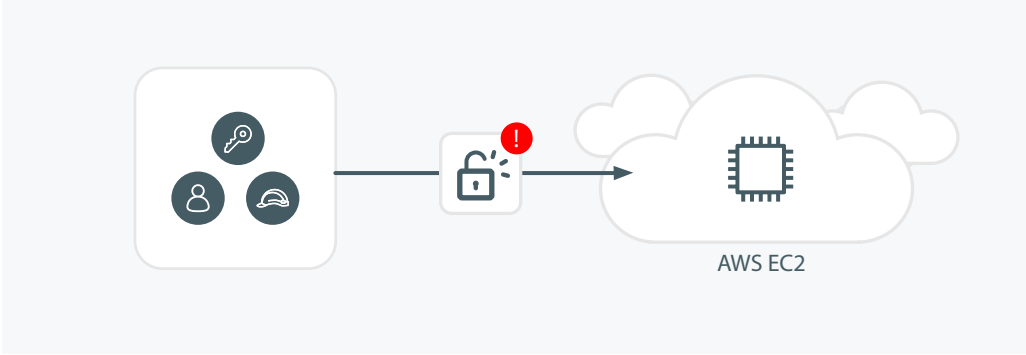
### Steps to Verify

- Investigate the account context that performed this action for other signs of malicious activity.
- Investigate for data loss.
- If review indicates possible malicious actions or high-risk configuration, revert applicable configurations and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Public EC2 Change

## Exfiltration


MITRE | ATT&CK®

T1213 Data from Information-Repositories

T1530 Data From Cloud Storage Object

T1537 Transfer Data to Cloud Account

T1578 Modify Cloud Compute Infrastructure

### Triggers

- After enumerating the existing security group policies, the ingress policy for an EC2 instance is modified.

### Possible Root Causes

- An attacker is enabling external access to an EC2 instance to maintain persistence.
- An EC2 instance is exposed to external access as a part of its normal operation.

### Business Impact

- Once an adversary achieves persistent access, they've established the opportunity to stage subsequent phases of an attack.

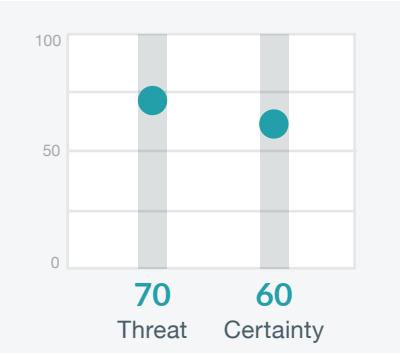
### Steps to Verify

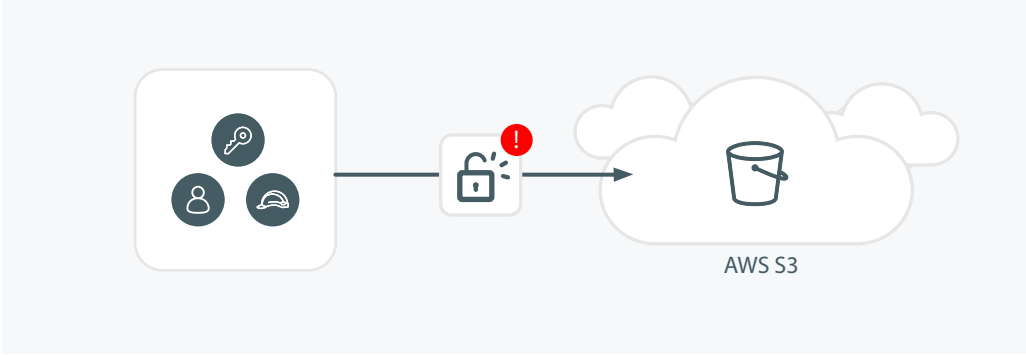
- Validate that any modifications are authorized, given the purpose and policies governing this resource.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

- Top -

# AWS Suspect Public S3 Change

## Exfiltration




MITRE | ATT&CK®

T1213 Data from Information-Repositories

T1530 Data From Cloud Storage Object

T1537 Transfer Data to Cloud Account

## Triggers

- A credential was observed suspiciously invoking a set of S3 APIs that permits public access to a given bucket.

## Possible Root Causes

- An attacker may be scanning and maliciously modifying configurations around an S3 bucket to enable data exfiltration.
- An IT misconfiguration may have been made by an authorized user which could weaken the posture around an S3 bucket and promote the risk of data loss.
- An internal tool is scanning the buckets for security reasons.

## Business Impact

- Malicious or unintentional weakening of security posture controls around S3 buckets are commonly associated with data loss.

## Steps to Verify

- Investigate the account context that made the change for other signs of malicious activity.
- Investigate for data loss.
- Verify if the S3 bucket in question is authorized for public access.
- If review indicates possible malicious actions or high-risk configuration, revert configuration and disable credentials associated with this alert then perform a comprehensive investigation.

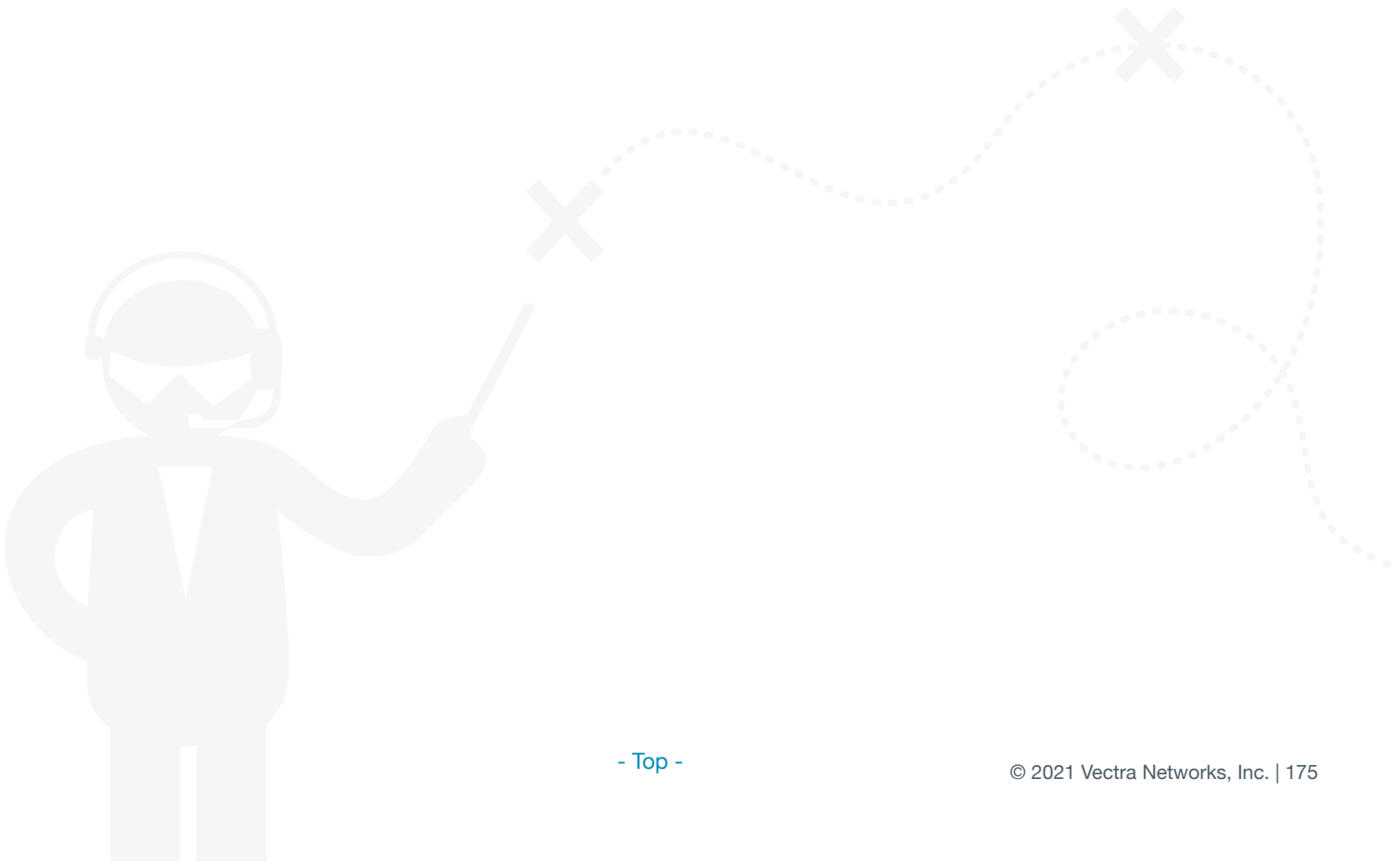
- Top -

## Category

# Botnet

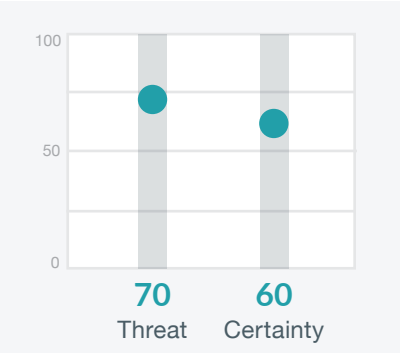
- An attacker with access to the AWS environment is leveraging AWS infrastructure for financial gain
- Actions are associated with the Impact MITRE Tactic

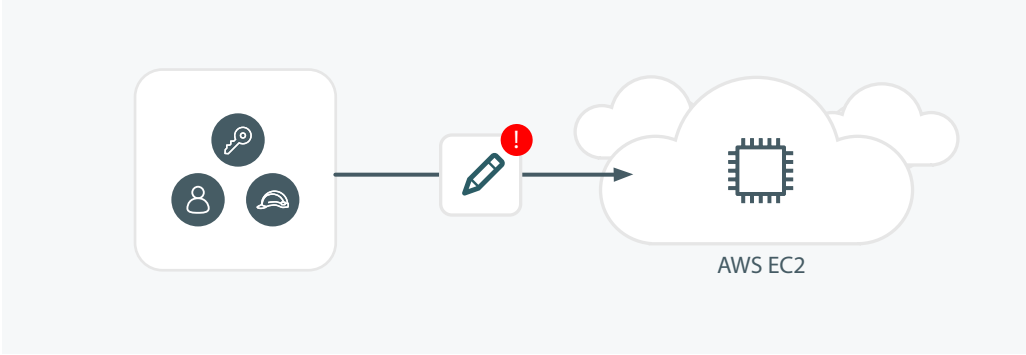


- Top -

# AWS Cryptomining

## Botnet




MITRE | ATT&CK®

T1496 Resource Hijacking

### Triggers

- Using a compromised EC2 instance token, multiple high-powered EC2 instances are started.

### Possible Root Causes

- An attacker is leveraging a compromised EC2 instance and/or token to create powerful EC2 instances for use in cryptomining.
- Internal infrastructure and applications are configured to create highly powered EC2 instances to enable compute intensive operations to occur in support of that application.

### Business Impact

- High powered EC2 instances utilized for cryptomining result in significant costs billed to the organization that owns the AWS account.

### Steps to Verify

- Investigate the source of the EC2 instances being started to determine if this resource should be creating new, high-powered, EC2 instances.
- Investigate the newly created EC2 instances to determine their purpose and ensure they are not malicious.
- If review indicates possible malicious actions, perform a comprehensive investigation to determine initial source of EC2 compromise, remove EC2 access and remediate compromised resources and accounts.

- Top -

# Attack Campaigns



## How is a campaign formed?

Campaigns are formed when there is at least one active *advanced* command & control detection and several other hosts are observed to be communicating with the same domain or IP address. In the future, there will be additional scenarios on which campaigns will be based.

## When is a campaign closed?

A campaign is closed when all advanced command & control detections underlying the campaign become inactive (time out as a result of prolonged inactivity), are triaged out (either whitelisted or modified to “custom” category) or are marked as fixed. Once a campaign is closed, it will not be reopened.

## What is included in the campaign?

The campaign UI will display objects for all the internal hosts involved in the campaign and the external IP or domain to which the advanced command & control is taking place. Lines connecting the host objects in the UI to the external IP or domain either denote a detection or the presence of communication without a detection (they look the same when zoomed out on a dense campaign – labels for the detections emerge upon zoom in). Lines connecting internal host objects to each other denote the presence of lateral detections in which one host is targeting another host in the campaign.

## Can I be notified of the creation of a campaign?

Under *Settings* > *Notifications*, you can request email notifications when a new campaign is closed or an existing campaign is closed. You can also configure syslog notifications to the log server of your choice for these same events.

## How can I see the sequence of events in the campaign?

The *View Events* action on the individual campaign page displays a list of details related to the evolution of the campaign and activity within it. Individual connections to the external domain or IP and updates to detections included in the campaign are detailed in the order in which they were observed. The event log can also be downloaded in CSV format for audit reasons or to enable offline analysis.

