VECTRA®

Hybrid Attack Report:

A Breakdown of Emerging Hybrid Attacker Methods

All modern attacks are hybrid attacks. Learn how today's cyber attackers infiltrate, escalate privileges, move laterally and progress their attacks.

Introduction

As cyber attackers continue to advance their tactics, techniques and procedures (TTPs), defenders must adapt strategies to keep their organizations secure. In today's hybrid world, defending the enterprise means adjusting to a bigger, ever-expanding surface filled with more sophisticated attacker methods while having to contend with more security alerts, noise, complexity and burnout.

To effectively defend against today's attacks — defenders are required to know:

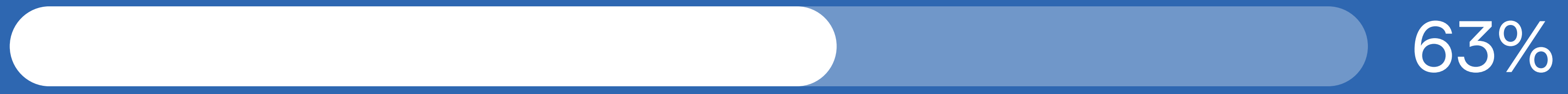
- Where is our hybrid cloud environment exposed to attackers?
- Where have hybrid attackers already infiltrated our environment?
- Where are hybrid attackers moving laterally to progress inside our environment?

Here, we reveal the tactics being used by real threat actors in real attacks on hybrid cloud environments. You'll see how attackers gain access, go undetected and pivot to the cloud — and how security teams detect and stop them before damage occurs. You'll discover:

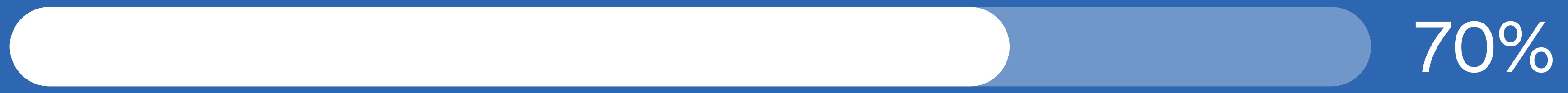
- The latest attacker tradecraft used in today's hybrid cloud attacks
- Where security tools have been bypassed or ineffective
- How defenders can pivot to prioritize active attacks

Attackers Have Room to Run Across Hybrid Cloud

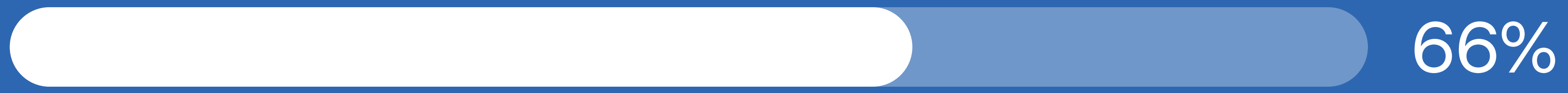
A majority of SOC analysts say the size of their organization's attack surface (63%),



the number of security tools (70%)



and alerts (66%) they manage have significantly increased in the past three years.[1]



Cyber attackers use this to their advantage. To compromise new areas. To bypass security tools that can't detect across every hybrid cloud surface. And to blend in with normal activity as SOC teams struggle to identify urgent threats among hundreds of daily alerts.

To explore the true anatomy of today's hybrid cloud attacks, we've broken down five attacks with granular details covering the initial compromise through the tactics used in each and where defenders have the opportunity to detect and prioritize the activity. The information in each attack discussed represents a combination of details gathered by Vectra AI MDR analysts, Vectra AI threat researchers, the MITIRE ATT&CK knowledge base and other publicly available information disclosed about various cybercrime groups and their tactics.

[1] Global Report: 2023 State of Threat Detection, The Defender's Dilemma

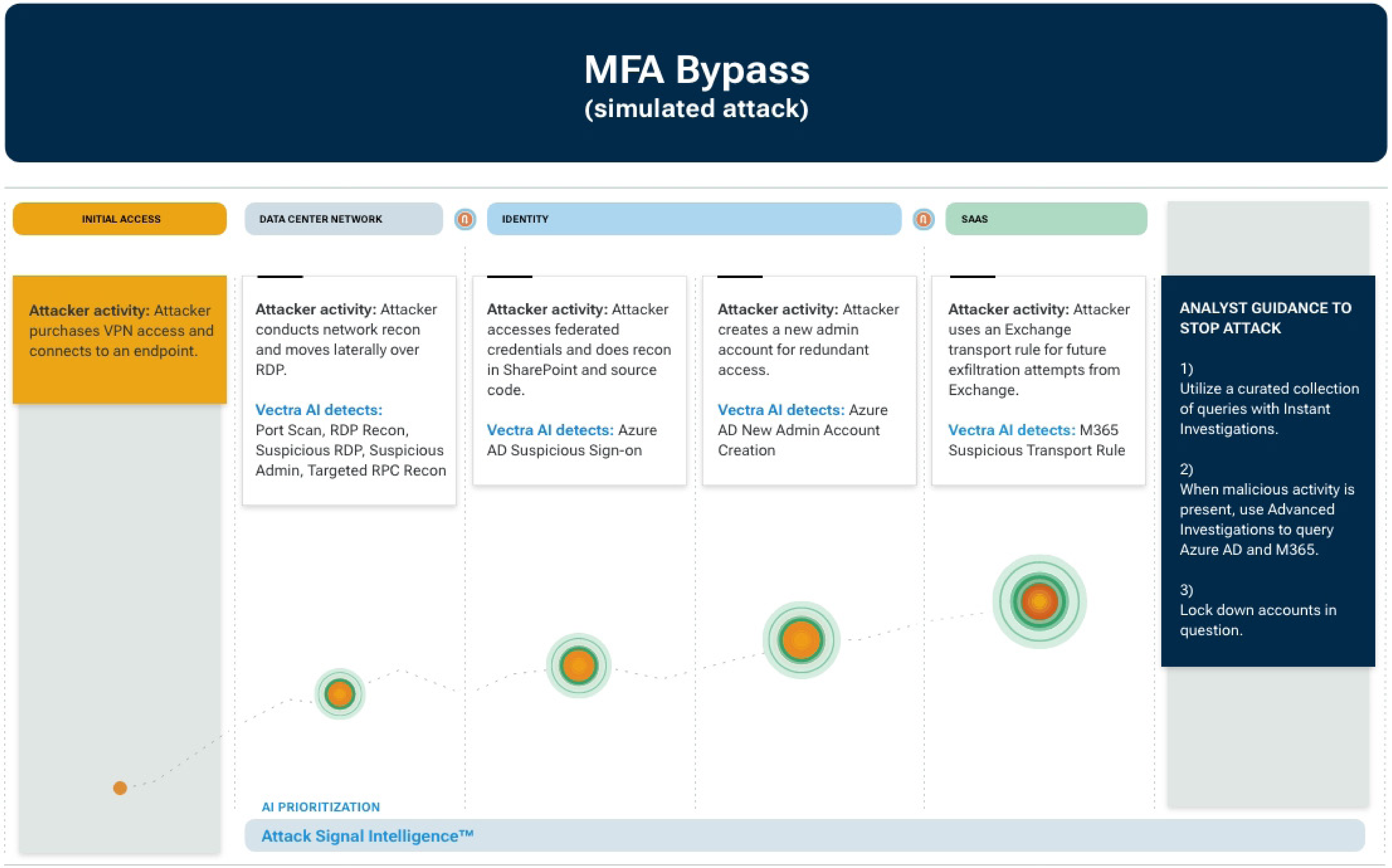
Table of contents

Emerging Attack Methods:

MFA Bypass

Incident background:

Lapsus$ was a well-funded cybercrime group associated with several high-impact hybrid attacks focused on ransomware and data. The group's techniques have been adopted into most ransomware gang playbooks, and according to reports, it's possible that Lapsus$ members and affiliates have decided to limit their public profile, join other cybercrime groups or rebrand.



MFA Bypass
(simulated attack)

Attacker activity: Attacker purchases VPN access and connects to an endpoint.

Attacker activity: Attacker conducts network recon and moves laterally over RDP.

Vectra AI detects: Port Scan, RDP Recon, Suspicious RDP, Suspicious Admin, Targeted RPC Recon

Attacker activity: Attacker accesses federated credentials and does recon in SharePoint and source code.

Vectra AI detects: Azure AD Suspicious Sign-on

Attacker activity: Attacker creates a new admin account for redundant access.

Vectra AI detects: Azure AD New Admin Account Creation

Attacker activity: Attacker uses an Exchange transport rule for future exfiltration attempts from Exchange.

Vectra AI detects: M365 Suspicious Transport Rule

ANALYST GUIDANCE TO STOP ATTACK

1) Utilize a curated collection of queries with Instant Investigations.

2) When malicious activity is present, use Advanced Investigations to query Azure AD and M365.

3) Lock down accounts in question.

Attack Signal Intelligence™

Emerging Attack Methods:

MFA Bypass

Attack traits:

- Targeting source code
- Email theft

Attack implications:

- Mass exfiltration
- Ransomware
- Reputation damage
- Business disruption

Reports show Lapsus$ using compromised credentials to gain access and progress attacks, even with multifactor authentication (MFA) in place. Detection beyond EDR would be required to prioritize and stop a similar attack once actors gain a foothold inside a hybrid environment.

Prioritizing tactics:

Once attackers gain access, it's critical that any tactics they use to advance are prioritized. Here, the attackers moved laterally by using a remote desktop and were able access federated credentials to aid in recon activities and ultimately advance towards their target.

MITRE ATT&CK Techniques:

- Remote Services / ID: T1021
- Reconnaissance / ID: TA0043
- Valid Accounts / ID: T1078
- Lateral movement / ID: TA0008
- Email Forwarding Rule / ID: T1114.003

Attack Signal Intelligence™ detects and prioritizes:

- Port Scan
- RDP Recon
- Suspicious RDP
- Suspicious Admin
- Targeted RPC Recon
- Azure AD Suspicious Sign-on
- Azure AD New Admin Account Creation
- M365 Suspicious Transport Rule

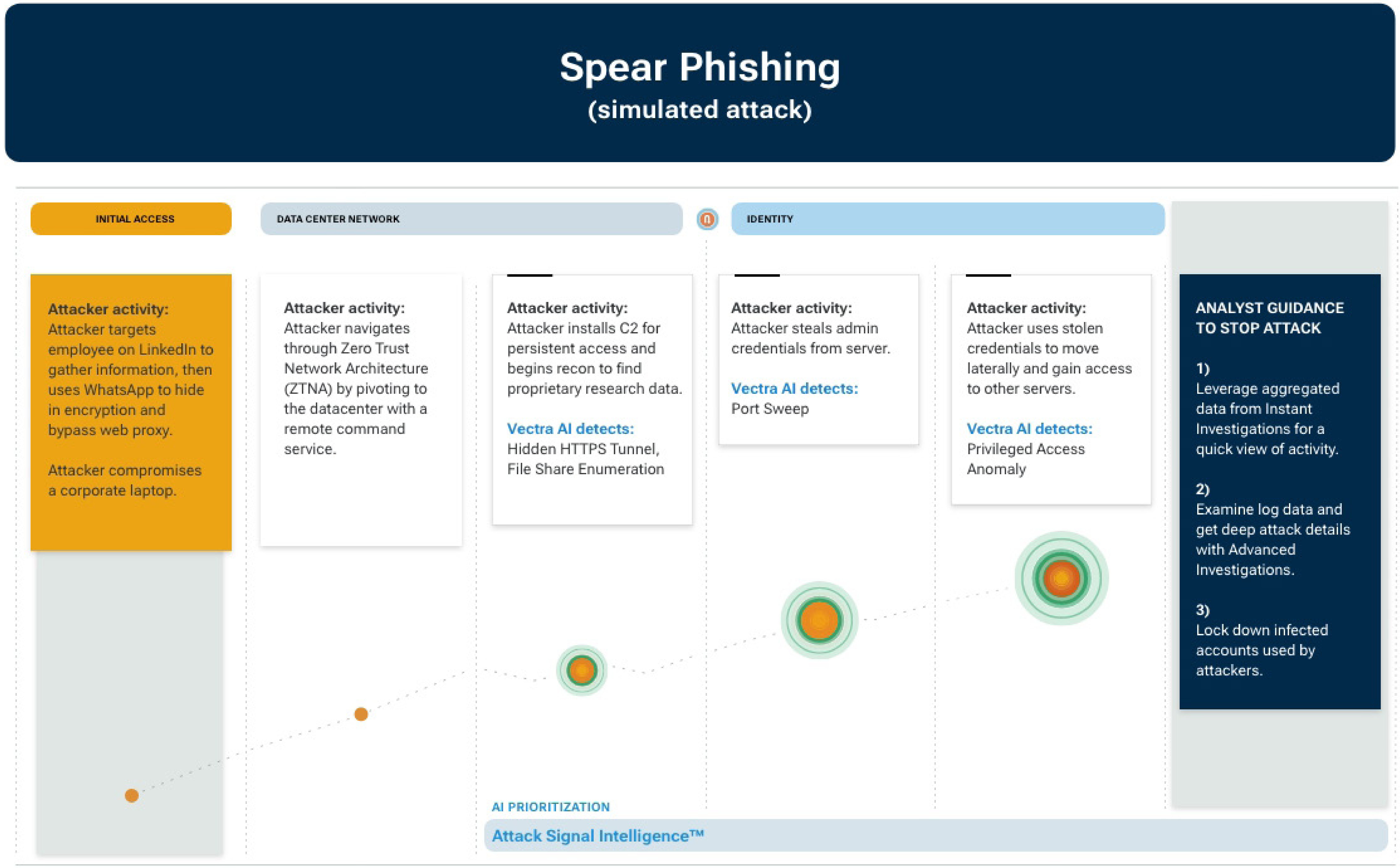
VECTRA

Emerging Attack Methods:

Spear Phishing

Incident background:

Lazarus is a North Korean state-sponsored cybercrime group that in addition to targeting pharmaceutical companies, has been reportedly associated with high-profile attacks such as the one on Sony Pictures in 2014. Recent reports also cite Lazarus for attempting to exploit the Log4J remote code execution vulnerability.



Spear Phishing

(simulated attack)

INITIAL ACCESS

DATA CENTER NETWORK

IDENTITY

Attacker activity:
Attacker targets employee on LinkedIn to gather information, then uses WhatsApp to hide in encryption and bypass web proxy.

Attacker compromises a corporate laptop.

Attacker activity:
Attacker navigates through Zero Trust Network Architecture (ZTNA) by pivoting to the datacenter with a remote command service.

Attacker activity:
Attacker installs C2 for persistent access and begins recon to find proprietary research data.

Vectra AI detects:
Hidden HTTPS Tunnel, File Share Enumeration

Attacker activity:
Attacker steals admin credentials from server.

Vectra AI detects:
Port Sweep

Attacker activity:
Attacker uses stolen credentials to move laterally and gain access to other servers.

Vectra AI detects:
Privileged Access Anomaly

ANALYST GUIDANCE TO STOP ATTACK

1)
Leverage aggregated data from Instant Investigations for a quick view of activity.

2)
Examine log data and get deep attack details with Advanced Investigations.

3)
Lock down infected accounts used by attackers.

AI PRIORITIZATION

Attack Signal Intelligence™

Emerging Attack Methods:

Spear Phishing

Attack traits:

- Spear-phishing tactics target employees on LinkedIn
- Attempts to steal proprietary patent information
- Look to exploit vulnerabilities

Attack implications:

- Loss of patent
- Delayed time to market
- Revenue loss
- Reputation damage
- Customer trust concerns

In this example, Lazarus highlights the ability of sophisticated attackers to successfully bypass security controls. Secure web gateway, email security, anti-virus, firewalls, IPS and other tools won't stop the actors from gaining access. Once attackers gain a foothold, detection and prioritization of the attacker activity inside the environment is key for security teams to stop the attack from progressing.

Prioritizing tactics:

It's possible to efficiently prioritize and stop similar attacks by having clarity into attacker movements with detections mapped to specific tactics. Upon gaining access, attackers often set up command and control (C2) for persistent access and start recon activities to locate research data. From there, they can look to swipe admin credentials and move laterally to other servers.

MITRE ATT&CK Techniques:

- External Remote Services / ID: T1133
- Command and Control / ID: TA0011
- Credential Access / ID: TA0006
- Lateral movement / ID: TA0008

Attack Signal Intelligence™ detects and prioritizes:

- Hidden TTPS Tunnel
- File Share Enumeration
- Port Sweep
- Azure AD Privilege Operation Anomaly

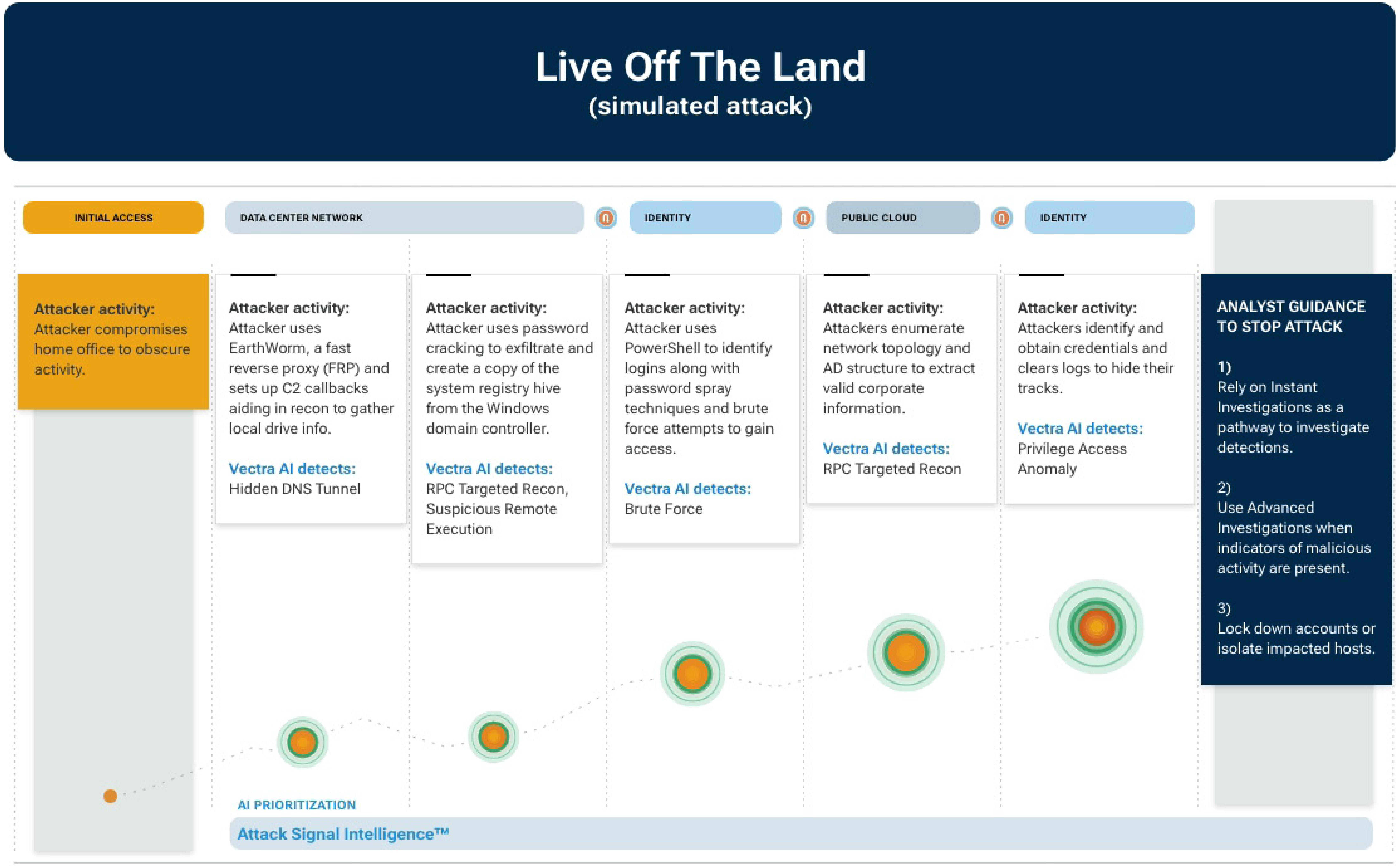
VECTRA

Emerging Attack Methods:

Live off the Land

Incident background:

Active since 2021, the China state-sponsored cyber actor, Volt Typhoon targets include communications, manufacturing, utility, transportation, construction, maritime, government, information technology and education sectors. Behaviors indicate that the group intends to maintain access to its targets without being detected for as long as possible.



Live Off The Land
(simulated attack)

INITIAL ACCESS

Attacker activity: Attacker compromises home office to obscure activity.

DATA CENTER NETWORK

Attacker activity: Attacker uses EarthWorm, a fast reverse proxy (FRP) and sets up C2 callbacks aiding in recon to gather local drive info.

Vectra AI detects: Hidden DNS Tunnel

Attacker activity: Attacker uses password cracking to exfiltrate and create a copy of the system registry hive from the Windows domain controller.

Vectra AI detects: RPC Targeted Recon, Suspicious Remote Execution

IDENTITY

Attacker activity: Attacker uses PowerShell to identify logins along with password spray techniques and brute force attempts to gain access.

Vectra AI detects: Brute Force

PUBLIC CLOUD

Attacker activity: Attackers enumerate network topology and AD structure to extract valid corporate information.

Vectra AI detects: RPC Targeted Recon

IDENTITY

Attacker activity: Attackers identify and obtain credentials and clears logs to hide their tracks.

Vectra AI detects: Privilege Access Anomaly

ANALYST GUIDANCE TO STOP ATTACK

1) Rely on Instant Investigations as a pathway to investigate detections.

2) Use Advanced Investigations when indicators of malicious activity are present.

3) Lock down accounts or isolate impacted hosts.

AI PRIORITIZATION

Attack Signal Intelligence™

Emerging Attack Methods:

Live off the Land

Upon gaining access, Volt Typhoon makes quick use of live off the land techniques without malware in play — making behavioral detection key to stopping the attack. Here, they attempt to use C2 callbacks when starting recon to gather local drive info. In order to steal credential information, they may also create copies of the AD domain database and abuse PowerShell commands to identify logins while working towards their target.

Attack traits:

- Evades endpoint detection and response (EDR)
- Blends in with normal user activity
- Utilizes live off the land (LOTL) techniques

Attack implications:

- Data exfiltration
- Loss of intellectual property
- Business disruption
- Loss of PII
- Reputation damage

Prioritizing tactics:

When actors work to enumerate network topology and AD structure, identify and obtain credentials and clear logs — these subtle movements blend in with normal network activity, but provide security teams with the chance to stop the attack before it's too late. AI-driven detection, triage and prioritization capabilities will further empower security teams with additional context into attack behaviors so they can be stopped prior to damage taking place.

MITRE ATT&CK Techniques:

- Proxy / ID: T1090
- System Information Discovery / ID: T1082
- OS Credential Dumping / ID: T1003
- Command and Scripting Interpreter / ID: T1059
- System Owner / User Discovery / ID: T1033
- Brute Force: Password Spraying / ID: T1110.003
- Brute Force / ID: T1110
- System Network Configuration Discovery / ID: T1016
- Permission Groups Discovery: Domain Groups / ID: T1069.002
- Credentials from Password Stores / ID: T1555
- Indicator Removal: Clear Window Event Logs / ID: T1070.001
- Masquerading / ID: T1036

Attack Signal Intelligence™ detects and prioritizes:

- HTTPS Hidden Tunnel
- RPC Targeted Recon
- Suspicious Remote Execution
- Brute Force
- Privilege Access Anomaly

VECTRA

Emerging Attack Methods:

Credential Stuffing

Incident background:

With attackers in possession of user credentials, it's only a matter of time before they would find a way into the environment. Tools such as MFA can be taken out of play when attackers possess credentials, which was the case during this incident. While the initial attempt failed, the attackers remained persistent and ultimately found a way in.

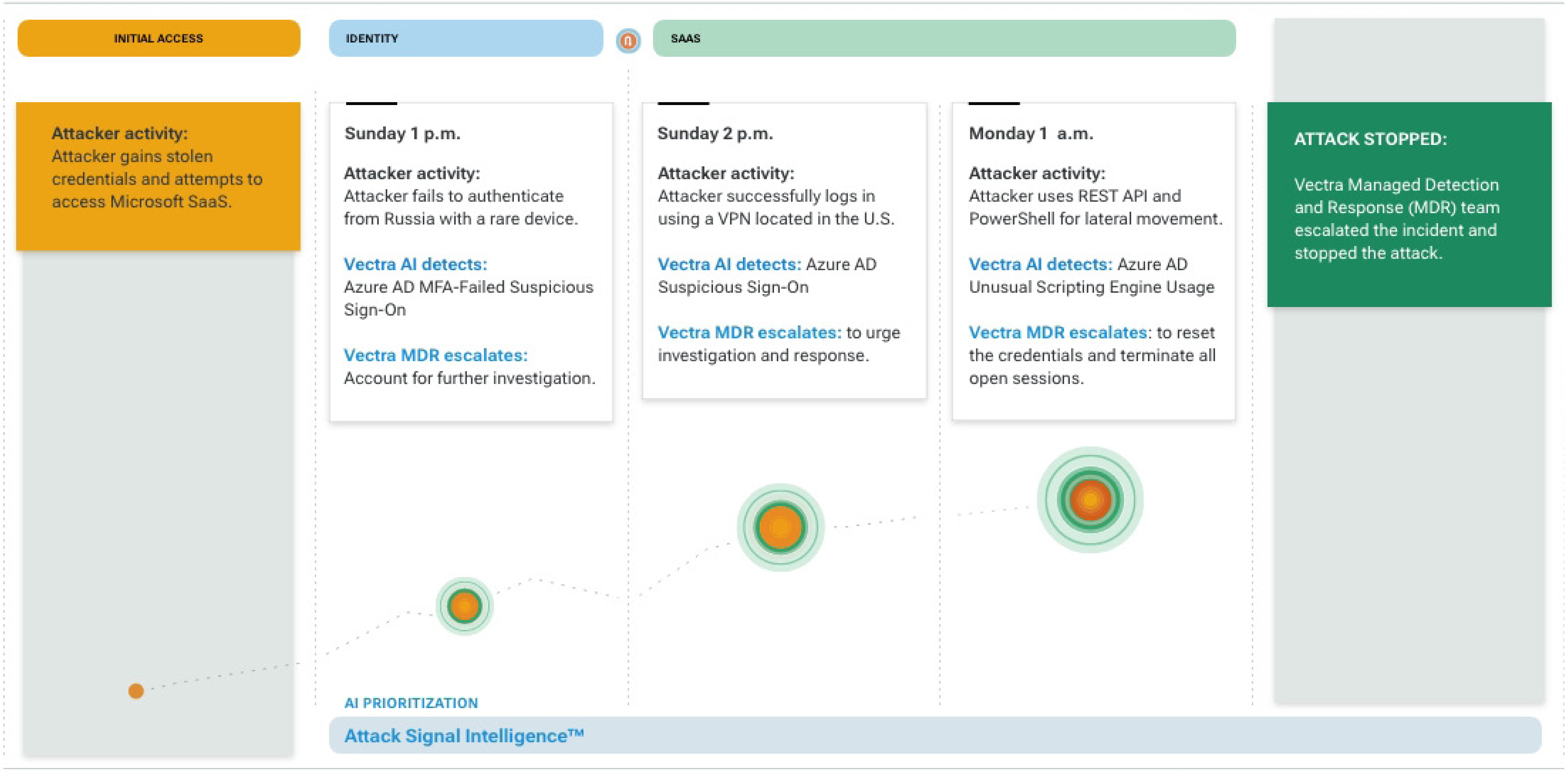
Credential Stuffing

(Real Attack Stopped by Vectra AI)

Investigation And Response Time

First Vectra AI Alert
00:00

Attack Stopped
12:00



INITIAL ACCESS

Attacker activity:
Attacker gains stolen credentials and attempts to access Microsoft SaaS.

IDENTITY

Sunday 1 p.m.

Attacker activity:
Attacker fails to authenticate from Russia with a rare device.

Vectra AI detects:
Azure AD MFA-Failed Suspicious Sign-On

Vectra MDR escalates:
Account for further investigation.

SAAS

Sunday 2 p.m.

Attacker activity:
Attacker successfully logs in using a VPN located in the U.S.

Vectra AI detects: Azure AD Suspicious Sign-On

Vectra MDR escalates: to urge investigation and response.

Monday 1 a.m.

Attacker activity:
Attacker uses REST API and PowerShell for lateral movement.

Vectra AI detects: Azure AD Unusual Scripting Engine Usage

Vectra MDR escalates: to reset the credentials and terminate all open sessions.

ATTACK STOPPED:

Vectra Managed Detection and Response (MDR) team escalated the incident and stopped the attack.

AI PRIORITIZATION

Attack Signal Intelligence™

Emerging Attack Methods:

Credential Stuffing

Attack traits:

- Stolen credentials leveraged by attackers
- Multiple sign-on attempts
- Targeting SaaS systems

Attack implications:

- Intellectual Property (IP) theft
- Sabotage
- Loss of competitive advantage
- Reputation damage
- Loss of customer trust

After the initial compromise, multiple Vectra AI threat detections were triggered as the attacker progressed. In this case, the customer uses Vectra Managed Detection and Response (MDR) for analyst reinforcement where the team escalated and ultimately stopped the incident as the attacker took action. Whether the response comes from an MDR analyst or an internal member of the security team, the key factor to stopping the attack is having an integrated threat signal to detect and prioritize attacker behavior post compromise.

Prioritizing tactics:

Acting quickly after gaining credentials, the threat actor attempted to authenticate from Russia through an unusual device. With the first attempt failing, they found an alternate route and successfully logged in using a VPN located in the U.S. Once inside, the attackers discovered an opportunity to move laterally through REST API and PowerShell techniques.

MITRE ATT&CK Techniques:

- Credentials from Password Stores / ID: T1555
- Credential Access / ID: TA0006
- External Remote Services (remote command service): ID: T1133
- PowerShell Command – Command and Scripting Interpreter / ID: T1059
- Lateral Movement / ID: TA0008
- Masquerading / ID: T1036

Attack Signal Intelligence™ detects and prioritizes:

- Azure AD MFA-Failed Suspicious Sign-On
- Azure AD Suspicious Sign-On detection
- Azure AD Unusual Scripting Engine Usage

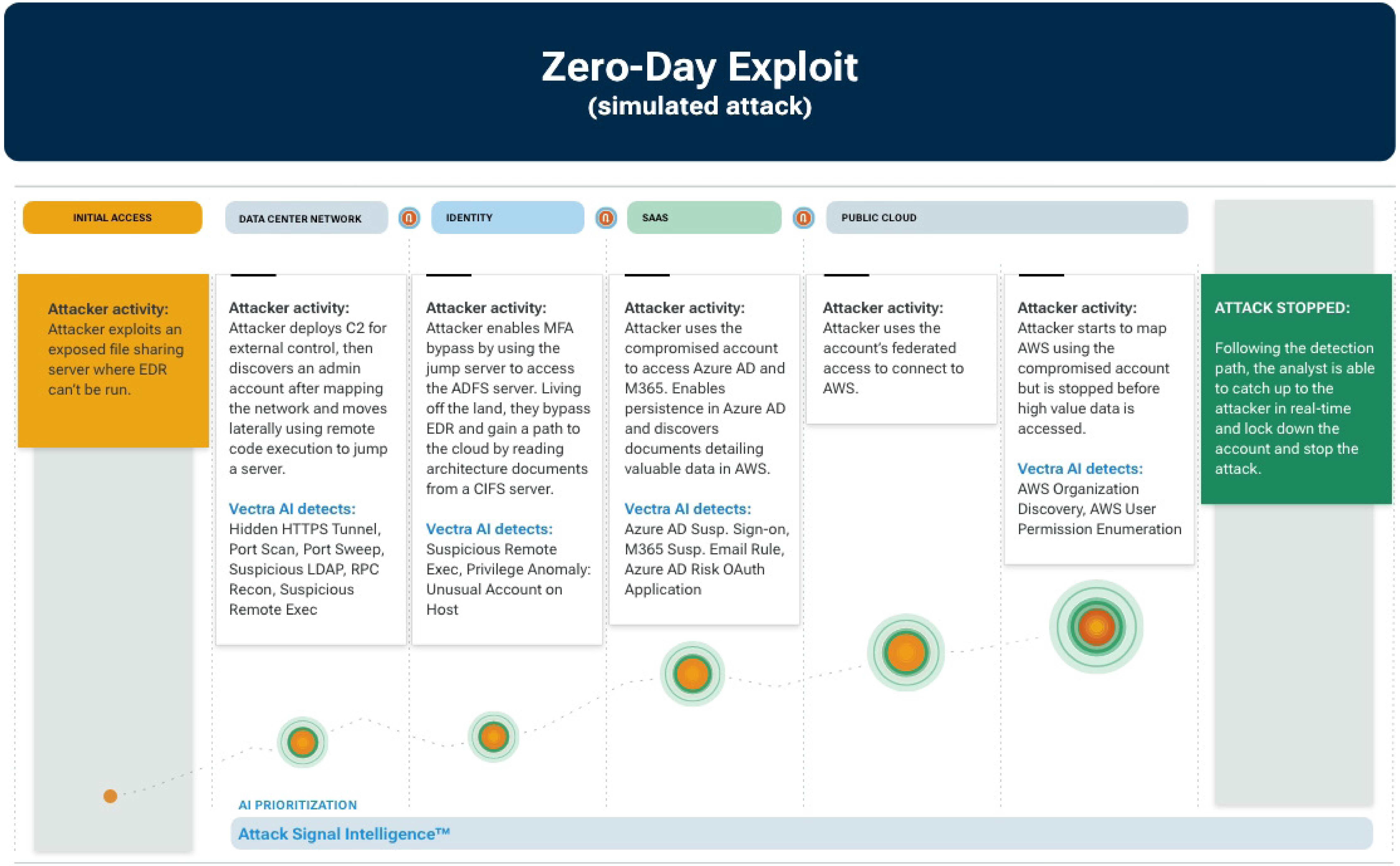
VECTRA

Emerging Attack Methods:

Zero-Day Exploit

Incident background:

Here we have an initial exploit that poses a detection challenge as IT isn't in control of a marketing server. This keeps EDR out of play as proprietary software had drivers installed that would interfere with an agent. Further into the progression, EDR wouldn't alert due to the actions involving native tools, while MFA was also bypassed.



Zero-Day Exploit
(simulated attack)

INITIAL ACCESS | DATA CENTER NETWORK | IDENTITY | SAAS | PUBLIC CLOUD

Attacker activity: Attacker exploits an exposed file sharing server where EDR can't be run.

Attacker activity: Attacker deploys C2 for external control, then discovers an admin account after mapping the network and moves laterally using remote code execution to jump a server.

Vectra AI detects: Hidden HTTPS Tunnel, Port Scan, Port Sweep, Suspicious LDAP, RPC Recon, Suspicious Remote Exec

Attacker activity: Attacker enables MFA bypass by using the jump server to access the ADFS server. Living off the land, they bypass EDR and gain a path to the cloud by reading architecture documents from a CIFS server.

Vectra AI detects: Suspicious Remote Exec, Privilege Anomaly: Unusual Account on Host

Attacker activity: Attacker uses the compromised account to access Azure AD and M365. Enables persistence in Azure AD and discovers documents detailing valuable data in AWS.

Vectra AI detects: Azure AD Susp. Sign-on, M365 Susp. Email Rule, Azure AD Risk OAuth Application

Attacker activity: Attacker uses the account's federated access to connect to AWS.

Attacker activity: Attacker starts to map AWS using the compromised account but is stopped before high value data is accessed.

Vectra AI detects: AWS Organization Discovery, AWS User Permission Enumeration

ATTACK STOPPED:

Following the detection path, the analyst is able to catch up to the attacker in real-time and lock down the account and stop the attack.

AI PRIORITIZATION

Attack Signal Intelligence™

Emerging Attack Methods:

Zero-Day Exploit

Attack traits:

- Zero-day exploit targeted
- Attackers move between cloud and on-premises
- Prevention security kept out of play

Attack implications:

- Data exfiltration
- Loss of intellectual property
- Business disruption
- Reputation damage

With an accurate timestamp of the incident and clear threat detections, analysts have the ability to catch up to attackers in real-time and disable any infected accounts and lock down hosts.

Prioritizing tactics:

When progressing towards the cloud, attackers can navigate environments with an abundance of tactics including command and control (C2). In this example, the attackers were able to locate admin accounts, add malware to evade MFA and ultimately locate a cloud architecture diagram along with gaining access to Azure AD and AWS. During the process, the actors claimed possession of high-privileged credentials, enabling potential access to critical parts of the network.

MITRE ATT&CK Techniques:

- Command and Control / ID: TA0011
- Account Discovery / ID: T1087.001
- Credential Access / ID: TA0006
- Account Manipulation / ID: T1098
- Valid Accounts / ID: T1078
- Email Hiding Rules / ID: T1564.008

Attack Signal Intelligence™ detects and prioritizes:

- HTTPS Hidden Tunnel
- HTTPS Tunnel, Port Scan, Port Sweep, Suspicious LDAP, RPC Recon
- Suspicious Remote Execution
- Privilege Anomaly: Unusual Account on Host
- Azure AD Suspicious Sign-on
- M365 Suspicious Email Rule
- Azure AD Risky OAuth Application
- AWS sign-in
- AWS Organization Discovery
- AWS User Permission Enumeration

Focus on attacker methods

Each attack, each threat actor and every environment present a unique set of challenges for defenders. However, the analysis across each attack highlights a relatively small set of underlying attacker methods as shown in the MITIRE ATT&CK techniques described.

5/5 attacks
exploit security tool weakness.

5/5 attacks
occur across multiple attack surfaces including: cloud, SaaS, identity and network.

5/5 attacks
hide and progress among normal activity by moving laterally, gaining admin access and through live off the land techniques.

5/5 attacks
leverage stolen admin credentials or passwords.

In addition to the MITRE ATT&CK techniques referenced across each attack, defenders can also use the MITRE D3FEND framework to see how each technique can be addressed and under which circumstance a solution would work. Or, with each attack anatomy above, defenders can see where techniques occur across the attack lifecycle and where a durable set of AI-driven countermeasures can be applied to stop them.

VECTRA

Prioritizing attacks that prey on hybrid cloud environments

It's clear that attackers are exposing security gaps and weaknesses in hybrid environments to infiltrate and progress attacks. While they evade detection, move past EDR, steal credentials, bypass MFA and continue to prove prevention security measures ineffective — security teams can still effectively detect and stop their behaviors with focus in three areas:

- Integrated attack coverage across all hybrid cloud attack surfaces.
- Integrated attack signal: an integrated AI-driven attack signal lets SOC teams know what's malicious, so they can focus on the most urgent threats.
- Integrated control: integrated, automated and co-managed investigation and response capabilities with full attack context enables the real-time investigations needed to stop attacks.

Enterprises can utilize the Vectra AI Platform to modernize their SOC with resilience, efficiency and effectiveness against today's hybrid attacks. Teams can monitor for attacker behavior post-compromise across all hybrid cloud attack surfaces with coverage for over 90% of MITRE ATT&CK techniques to eliminate hybrid attack blind spots. Vectra AI is the most referenced vendor by MITRE D3FEND for defensive countermeasures and prevention solutions, while its open XDR architecture has more than 40 integrations for attack context, investigation workflow and response.

Learn more about the Vectra AI Platform, today.

About Vectra

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers.

For more information, visit www.vectra.ai