VECTRA
SECURITY THAT THINKS

POST-INCIDENT REPORT

Stopping a RansomOp Before Ransomware

TABLE OF CONTENTS

Executive summary 2
External Reconnaissance 3
Initial Access 4
Reconnaissance 5
Lateral Movement to the Domain Controller 8
Investigation and Remediation 9

Vectra® protects business by detecting and stopping cyberattacks.

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers — before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is *Security that thinks®*. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

Vectra customer: Manufacturing

Executive summary

On Sunday June 13, 2021, the Vectra Sidekick team responded to an urgent request for assistance from a customer in the manufacturing sector. Sidekick analysts worked closely with the customer's team to stop and remediate an active attack using detections and data from Vectra Cognito.

- **Cognito Detect for Network** provided AI-driven detections, prioritization, and automated response that surfaced and stopped immediate attack progression
- **Cognito Recall** provided complete network metadata, supporting investigation, response, and full eviction of the adversary.

Post-incident analysis points to UNC2447 as the adversary, a group associated with Five Hands Ransomware. The attack was stopped prior to exfiltration of data or deployment of any ransomware payload.

After an extended external recon phase, the adversary gained access to the network via the Sonicwall VPN after business hours. Within 2 minutes of access, Vectra identified the attack activity and prioritized the attack host to Critical in the Vectra console. Further progression during the evening enabled the attacker to gain domain admin on the domain controller. Automated response from Vectra kicked in at this point to stop further progression through an EDR integration. Immediate and decisive follow-up action by the security team ensured the combined incident response team had time to investigate and fully evict the adversary without risk of ransomware deployment.

Speed of detection and decisive response—tools, people, and processes—was critical to enabling the successful outcome. The active attack phases began at 18:01 local (right after the close of business) and it is near-certain that ransomware would have been deployed overnight if the response had been delayed even hours. Further, the adversary specifically searched for and located Veeam backup configuration files, suggesting an intent to destroy backups as well, disrupting the company's ability to recover without paying.

External Reconnaissance (June 8-June 12)

The first evidence of reconnaissance was on June 8, 2021, when attackers began to probe multiple services, including VPN, FTP, and webmail. The probing originated from Russian IP subnets.

VPN interaction over time

The following day, on June 9, Vectra observed HTTP GET and POST requests inbound to multiple targets, attempting to discover any vulnerabilities in the Apache servers located behind the targets.

The user agent for these requests was unique within the environment. Vectra noted an additional external IP address making a request with the same user agent on June 3, 2021 at 08:01. The same IP address was also briefly active on June 9, 2021. The volume of traffic and bytes transferred was so minimal it was likely a routing mistake by the attacker.

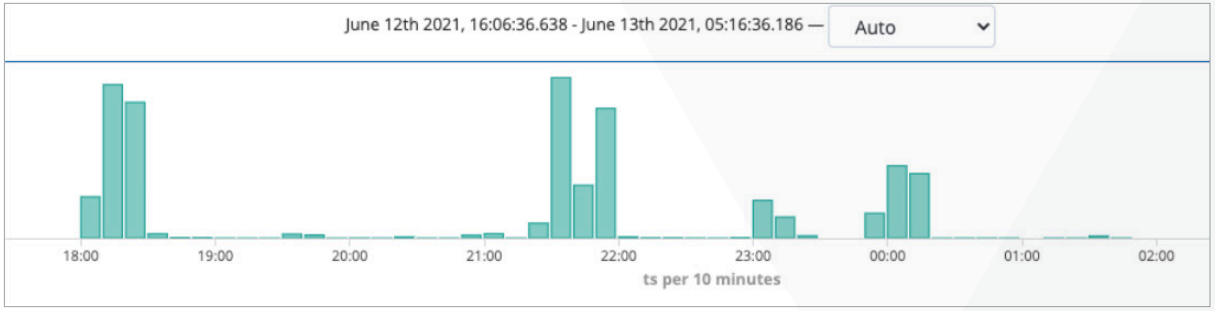
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36

Unique user-agent observed

Initial Access (June 12, 18:01 local)

The attacker first leveraged the attack host to access the network when a valid user account logged in to the VPN at 18:01.

Access was via a Sonicwall VPN. MFA was not yet enabled on the VPN, partially due to licensing requirements which had delayed the project. An unpatched Sonicwall vulnerability that leaked credentials seems the most likely means of gaining credentials, but this is unconfirmed. The attack host also used a valid VPN profile, suggesting either that the connection was proxied through a compromised user laptop or that the VPN profile was stolen and used from the attacker infrastructure.



Attack host sessions over time

Reconnaissance

All activity during this phase originated from the same attack host (located outside of the network) that logged into the VPN.

Upon gaining access, the attacker performed aggressive reconnaissance, leveraging reverse DNS lookups, remote procedure calls and other means to footprint the network. Immediately, numerous Vectra detections identified the attacker's presence as detailed below.

Shortly after the initial login, a large volume of DNS reverse lookups was performed for IPs in the systems subnet, consistent with recon behavior.

DNS requests were also observed to a free online EternalBlue vulnerability scanner and to the domain codeby[.]net, an online programming, ethical hacking and penetration testing forum. The Vectra team's assessment is that the attacker was performing vulnerability discovery and attempting to identify working exploits to run within the environment.

Vectra also observed DNS lookups to Russian domains including yandex[.]ru, ok[.]ru and google[.]ru. This suggests that the attacker was likely of Russian origin. In combination with the DNS activity signals above, this strongly suggests the attacker did not realize that their DNS traffic was being routed through the corporate network.

2.0.5.10.in-addr.arpa	PTR
13.0.5.10.in-addr.arpa	PTR
47.0.5.10.in-addr.arpa	PTR
9.0.5.10.in-addr.arpa	PTR
3.0.5.10.in-addr.arpa	PTR
5.0.5.10.in-addr.arpa	PTR
12.0.5.10.in-addr.arpa	PTR
14.0.5.10.in-addr.arpa	PTR
4.0.5.10.in-addr.arpa	PTR
8.0.5.10.in-addr.arpa	PTR
43.0.5.10.in-addr.arpa	PTR
33.0.5.10.in-addr.arpa	PTR
15.0.5.10.in-addr.arpa	PTR

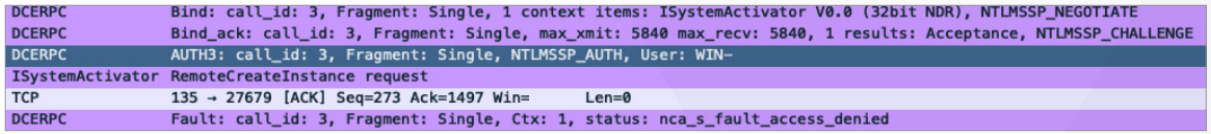
Reverse DNS lookups

By 18:03, **a mere 2 minutes after the initial VPN login**, Vectra had already triggered five detections and prioritized the attack host to Critical. The five detections were:

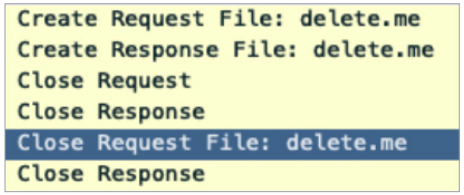
- Automated Replication
- Port Sweep
- RPC Reconnaissance
- RPC Targeted Reconnaissance
- File Share Enumeration

Within the Automated Replication detection, a hostname of format **WIN-XXXXXXXXXXX** was identified attempting to use the **NTLMSSP__AUTH** with account Administrator against the host 10.5.1.20. This generic Windows host name format was not used anywhere else in the environment. The same hostname appears in future RDP data, and we believe that is it the true source host used in the attack.

Over the SMB connection both read and write requests were observed for the filename **delete.me**. This activity is consistent with the recon tool **Netscan** attempting to test write permissions on file shares.



PCAP: Automated Replication Detection



Netscan behavior

At 18:16, Vectra detected Novel Access to SMB Admin Share when the attacker connected. Shortly after this, a connection was made to another system over SMB to the path \\10.5.0.65\backup_exchange$. During this connection the file was transferred to the source host — in total 10.9MB was transferred. Due to the host being connected over VPN at the time, the compressed Veeam file was likely exfiltrated out of the organization.

At 21:09 Vectra detected Suspicious Remote Desktop when the attacker established an RDP session to the host at 10.5.3.28. RDP information indicates the source hostname as **WIN- XXXXXXXXXXX**, believed to be the true source host.

At 21:15, Vectra detected the transfer of the malicious credential dumping tool **mimikatz.exe** to two different systems (10.5.2.12 and 10.5.3.28; hostnames left out for anonymity). Vectra also recorded subsequent file access to retrieve the results.

June 12th 2021, 18:18:13.126	WIN-[illegible]	\\10.5.0.65\backup_exchange$	[illegible]	SMB::FILE_OPEN	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[illegible]	\\10.5.0.65\backup_exchange$	[illegible]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[illegible]	\\10.5.0.65\backup_exchange$	[illegible]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[illegible]	\\10.5.0.65\backup_exchange$	[illegible]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[illegible]	\\10.5.0.65\backup_exchange$	[illegible]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[illegible]	\\10.5.0.65\backup_ex ge$	[illegible]	SMB::FILE_READ	10.5.0.70	10.5.0.65

Vectra Evidence of SMB connections

Lateral Movement to the Domain Controller

All reconnaissance activity was sourced from the same host. After a roughly 2-hour break, during which the attacker was likely reviewing their newly acquired reconnaissance data, the attack moved to the next phase: getting to the Domain Controller.

At 00:25, Vectra detected two suspicious LDAP queries from the attack host looking for subnet and computer object categories.

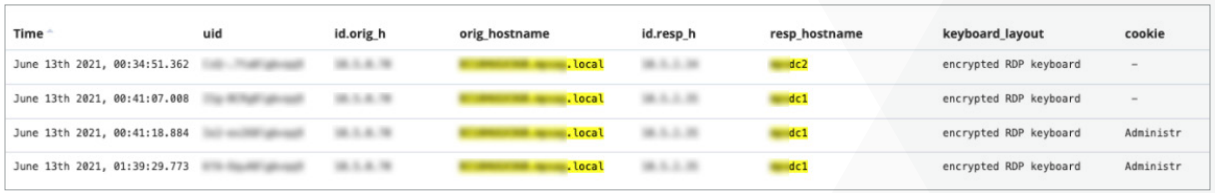
In total 1,006 objects were returned indicating the requests were successful. This type of behavior is not typical and is consistent with reconnaissance of the network.

At 00:34 an RDP connection was observed to a domain controller (DC1). At 00:41, another RDP connection was observed to a second domain controller (DC2). Both sessions had significant data transferred, indicating that they were successful.

LDAP Server: [redacted] (Last seen 1 day, 13 hours ago)

BASE DISTINGUISHED NAME	LDAP REQUEST	RESPONSE	OBJECTS RECEIVED	RESPONSE TIMESTAMP
CN=Subnets,CN=Sites,CN=Configuration,DC=[redacted]DC=local	(objectCategory=subnet)	success	6	June 13, 2021, 12:25 a.m.
[redacted]	(objectcategory=computer)	success	1000	June 13, 2021, 12:25 a.m.

Suspicious LDAP requests



Time	uid	id.orig_h	orig_hostname	id.resp_h	resp_hostname	keyboard_layout	cookie
June 13th 2021, 00:34:51.362	[redacted]	[redacted]	[redacted].local	[redacted]	[redacted]dc2	encrypted RDP keyboard	-
June 13th 2021, 00:41:07.008	[redacted]	[redacted]	[redacted].local	[redacted]	[redacted]dc1	encrypted RDP keyboard	-
June 13th 2021, 00:41:18.884	[redacted]	[redacted]	[redacted].local	[redacted]	[redacted]dc1	encrypted RDP keyboard	Administr
June 13th 2021, 01:39:29.773	[redacted]	[redacted]	[redacted].local	[redacted]	[redacted]dc1	encrypted RDP keyboard	Administr

RDP connections to domain controllers

Beginning at 00:39, DC1 began to scan the network, triggering the following detections:

- Automated Replication
- File Share Enumeration
- Suspicious Remote Execution
- Port Sweep
- Novel Access to SMB Admin Share
- RPC Targeted Recon
- RPC Recon

At 00:41, Vectra triggered automated containment to isolate the system via EDR, stopping the activity.

DC2 followed a similar pattern of scanning and automated response/isolation.

When the automated isolation activity occurred, the security team was also paged. On seeing the situation, the team immediately recognized that this was a serious, ongoing attack and took decisive action to temporarily disconnect internet to allow time for investigation and remediation.

Investigation and Remediation

The Vectra Sidekick team was engaged at this point to assist in scoping the full extent of the activity and ensuring that the adversary had been evicted.

- The suspected-compromised attack host was collected, investigated, and subsequently wiped. No indications of compromise were visible, suggesting that it was more likely the attackers had stolen the VPN profile previously and were connecting from their own infrastructure rather than proxying through a compromised host.
- As the attacker had domain controller access the customer decided the best course of action was to assume the 'worst case scenario' that the attacker had obtained Golden Ticket. As such a full domain rebuild along with double KRBTGT reset was conducted. This was done to avoid the additional delay which would have been required to perform a full endpoint forensic investigation and brought the business back online faster.
- The VPN was patched and 2FA implemented for all accounts.
- Additional custom models were deployed and prioritized when the network was brought back online to ensure any further activity from the attacker would be immediately detected.

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai