VECTRA
SECURITY THAT THINKS

POST-INCIDENT REPORT

A customer's perspective: Ransomware Post-Incident Report

TABLE OF CONTENTS

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: Pharmaceutical company

Executive summary

This post-incident report from a Vectra® pharmaceutical customer* shows step by step how the Cognito® network detection and response (NDR) platform identified early indicators of a ransomware attack and prevented the encryption of network file shares.

Vectra has been authorized to publish this post-incident report by ensuring anonymity and protecting the customer's private data. This type of report is ordinarily kept confidential for internal analysis only.

Inside the compromised network on Day 1 – one week prior to the intended ransomware detonation – the Vectra Consulting Analyst Team detected unmistakable reconnaissance and lateral movement attack behaviors.

These phases of the attack lifecycle indicated the attacker was looking for critical systems to compromise before encrypting network file shares for ransom. Vectra showed that scans came from wide range of hosts and other scans were related to ransomware activities as network file shares were enumerated.

Uncovering additional evidence, Vectra observed that one compromised host was communicating with a known malicious IP address in Ukraine that has been associated with Sodinokibi malware. External connections were performed successfully to a Ukraine IP address with a data transfer of about 80 MB.

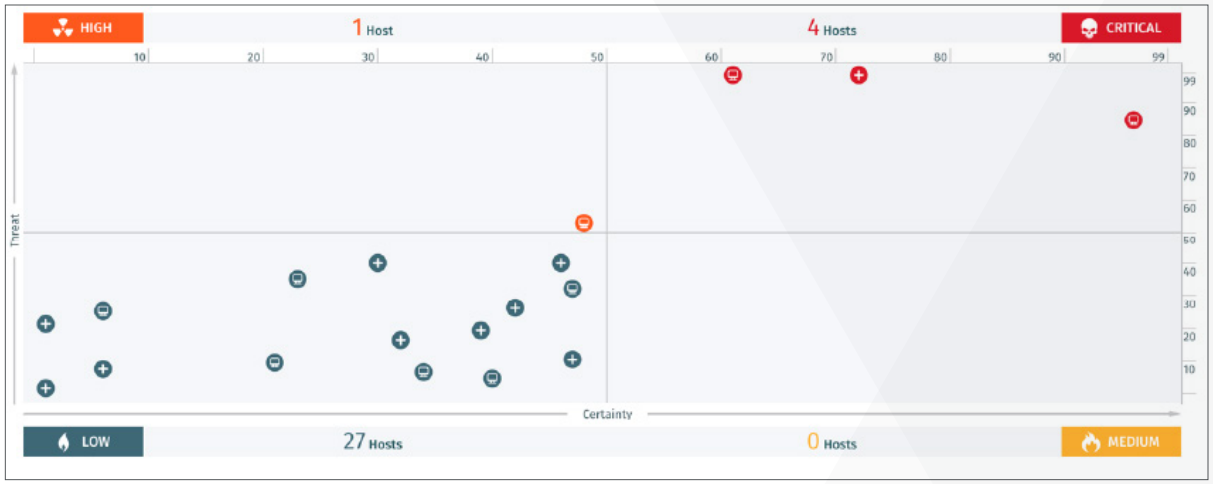
The number of detections identified by Vectra was concerning due to the sheer volume of data that was being sent to the outside. Additional information from the customer linked the attack to Maze ransomware.

This post-incident report shows the importance of early cyberattack detection to avert damage and catastrophic data breaches. With certainty and precision, it is vital to identify precursor behaviors, swiftly investigate incidents, and arm yourself with the appropriate response tools.

*The customer's name has been withheld for privacy reasons. All detection screen images in this report were provided by the customer and have been obscured to protect privacy.

General analysis

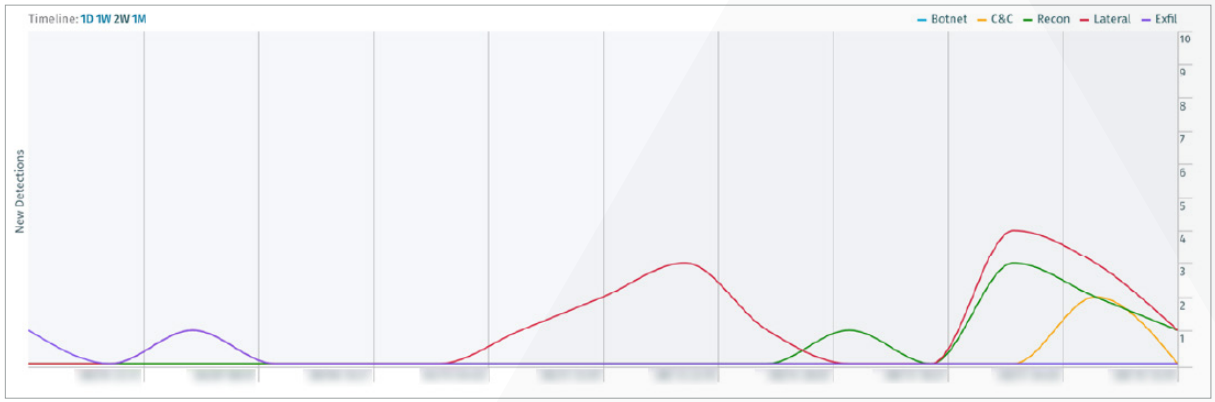
After the attack, the Cognito NDR platform showed four hosts in the *Critical* quadrant, one in in the *High* quadrant, and several hosts in the *Low* quadrant. Three of the four Critical hosts were confirmed infected:



Host Dashboard on YY

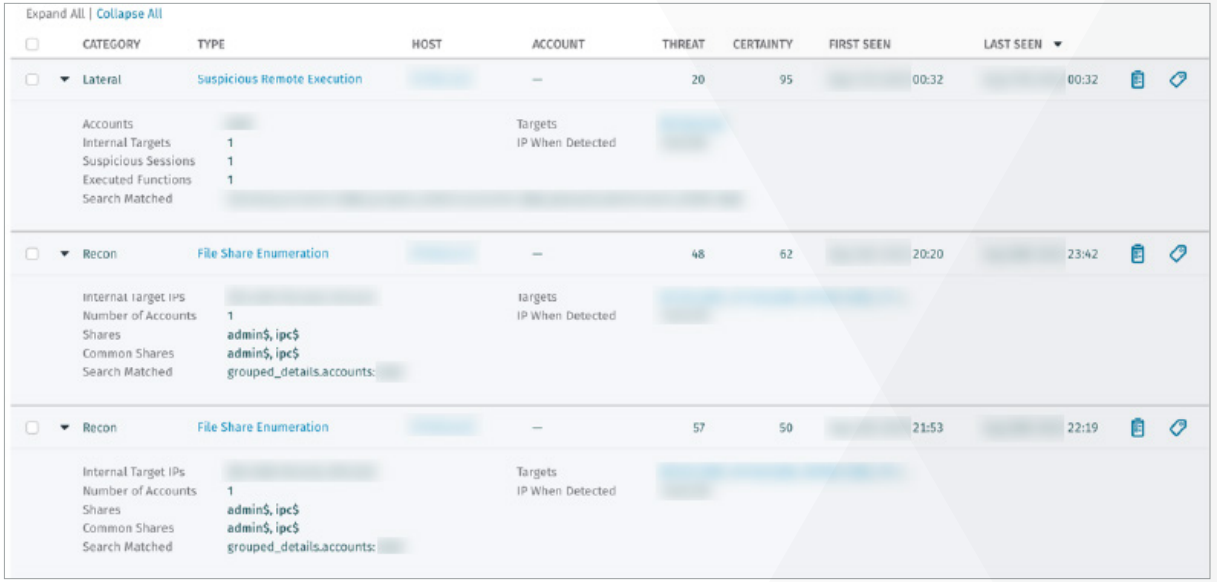
Vectra can clearly see the type of actions executed prior to the ransomware attack on the detection's timeline.

The first spike in the chart occurred six days before the attack. The second spike shows the actual encryption.



Detection chart on YY

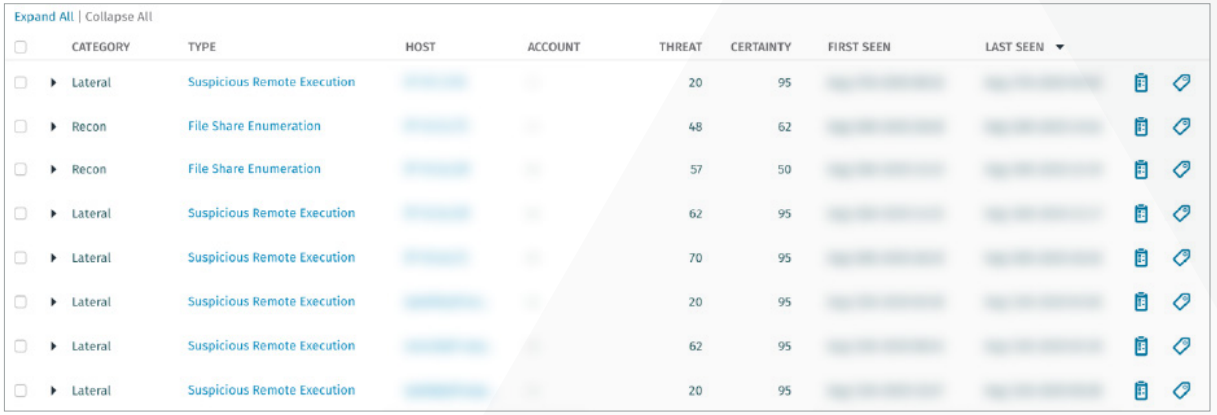
The attacker used a legitimate but compromised user account to move laterally and enumerate file shares on a wide range of hosts.



Suspicious remote execution using a customer account

The first traces of lateral movement using this account were observed one week prior to the ransomware detonation. All lateral movement observed was done via the StartServiceW function, which is usually observed when PsExec is used.

The full timeline of detections over the period is available in the appendix of this document.

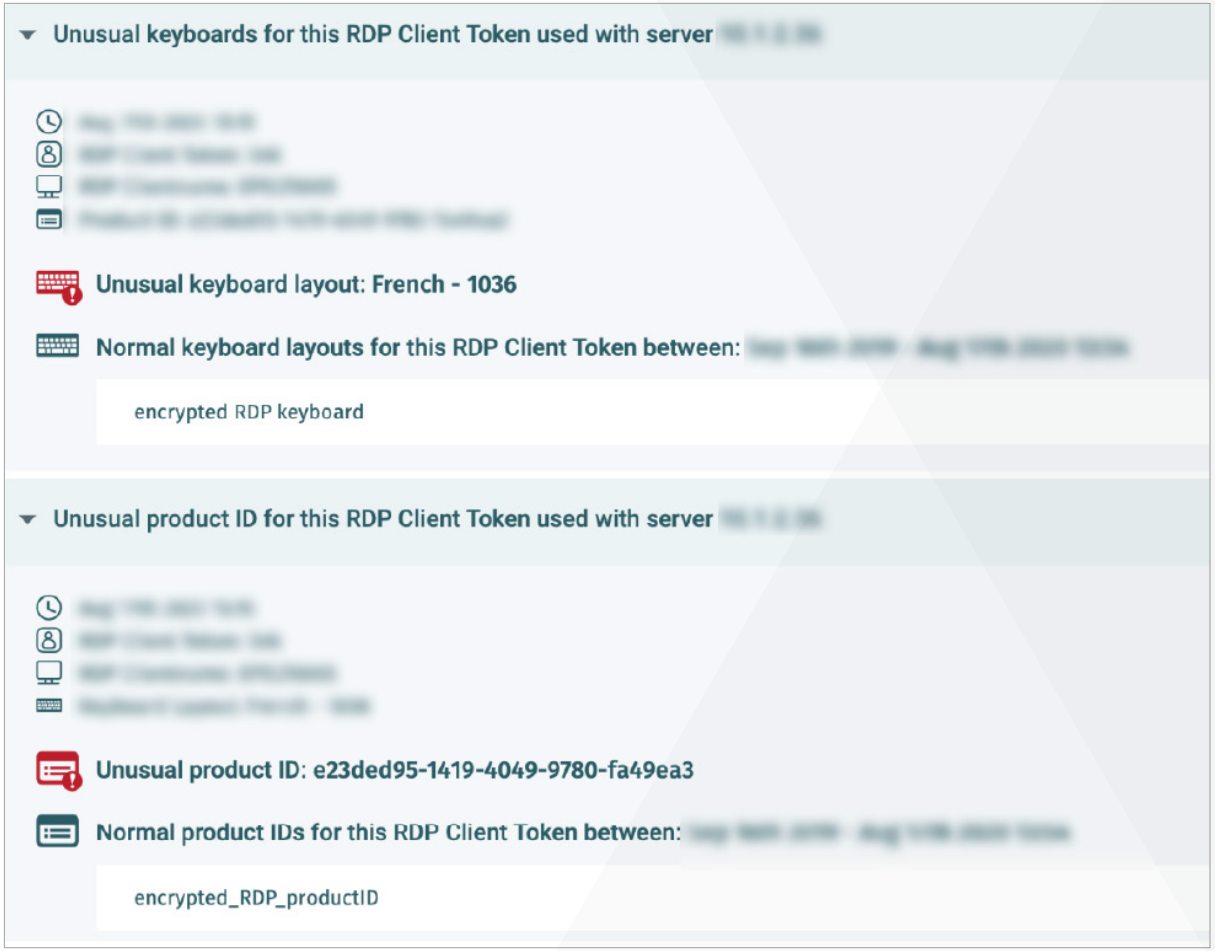


All detections involved in the customer account

Other events

Some suspicious RDP detections occurred at the time of the attack, but they might be legitimate.

Vectra recommended validation at this point (connection from XXXX to YYYY):

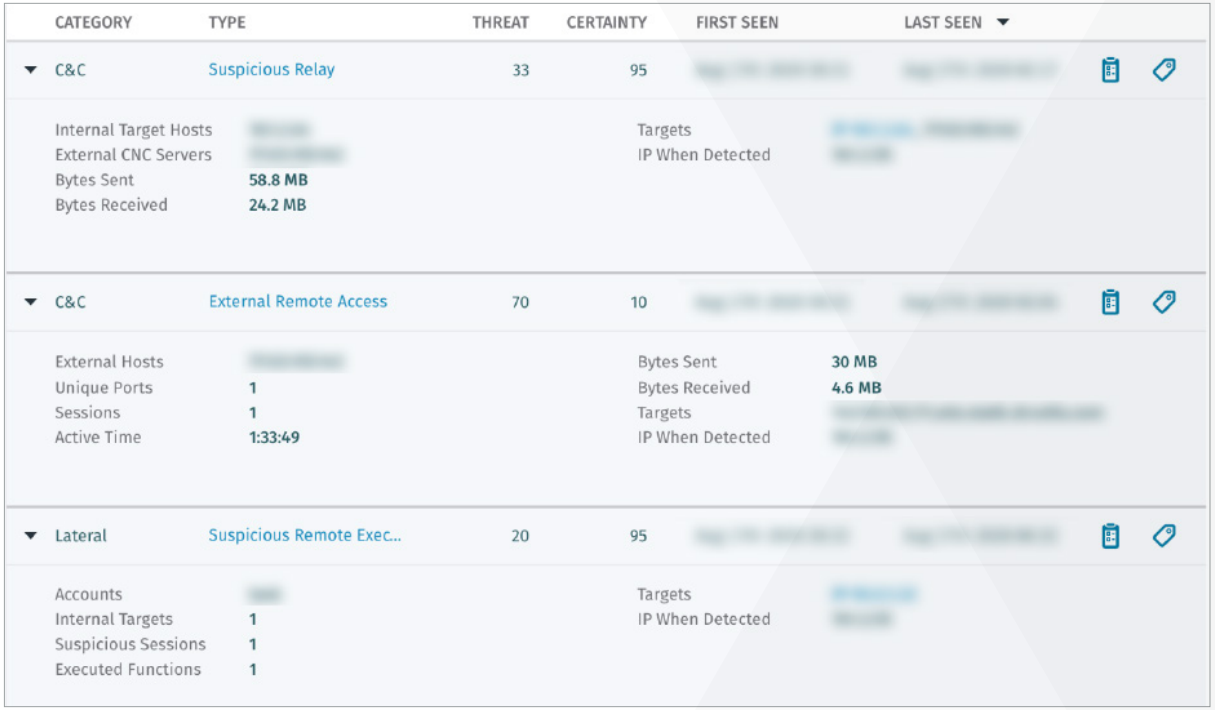


External communications

One of the infected hosts was observed communicating with a known malicious IP address in Ukraine that has been associated with Sodinokibi malware.

Communication occurred through Port tcp:53.

These detections are concerning due to the amount of data sent to the outside.

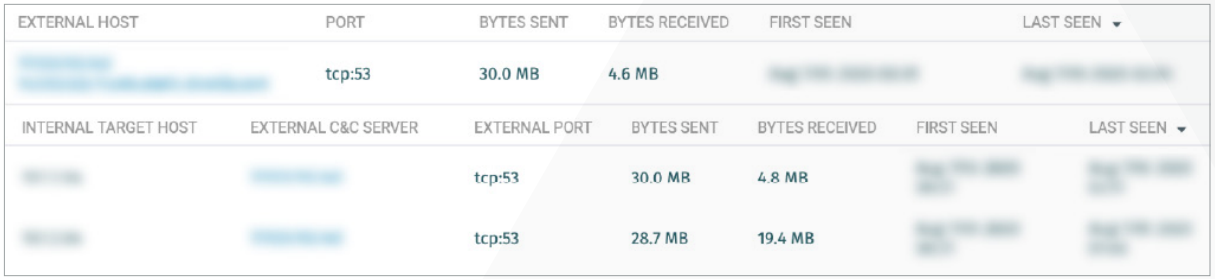


Communication to external IP address

After gaining more information from the Vectra customer, the attack appears to be related to Maze ransomware.

Maze is manually operated. The external Ukraine IP, despite its association with another malware family, may still have been used for command-and-control communications and data exfiltration.

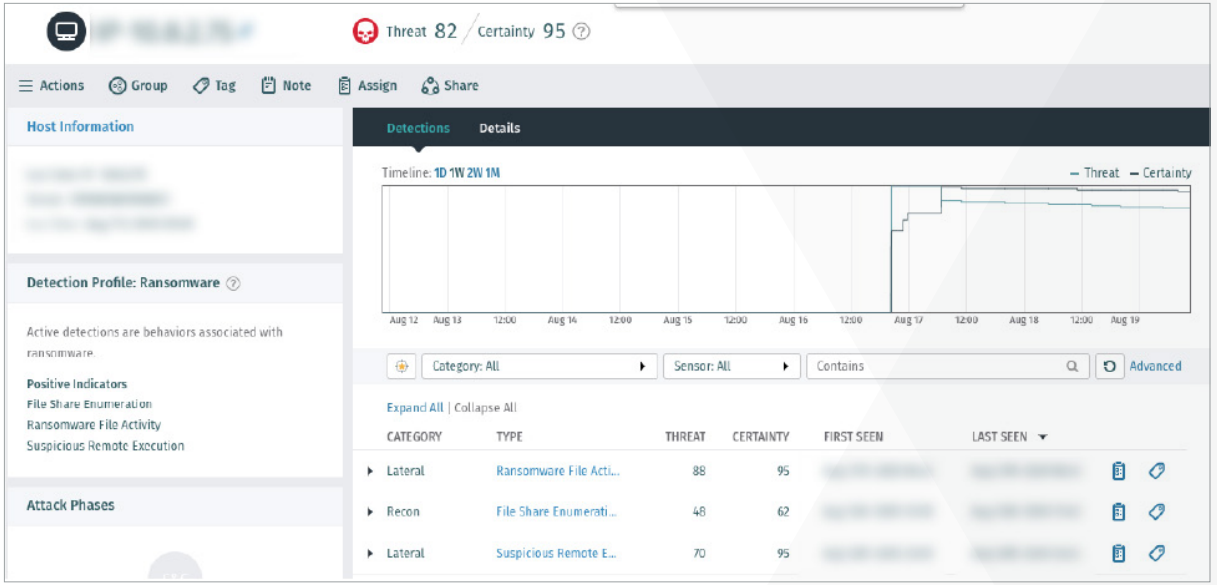
Vectra recommended analyzing communications with this external host, if possible.



Suspicious relay detection on DNS

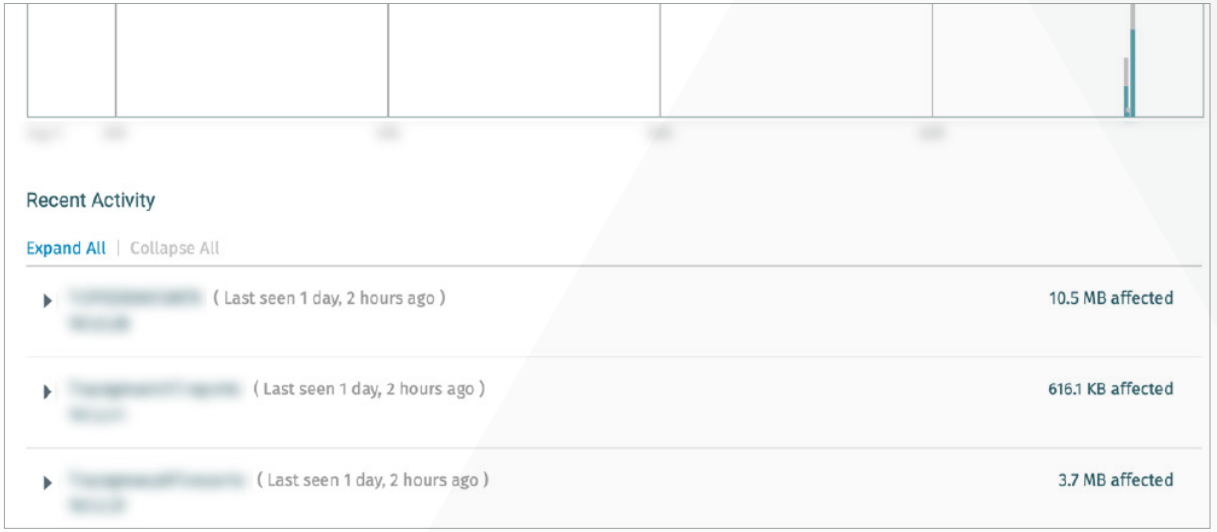
Ransomware analysis

Ransomware detonation occurred on one host (IP-X.X.X.X.):



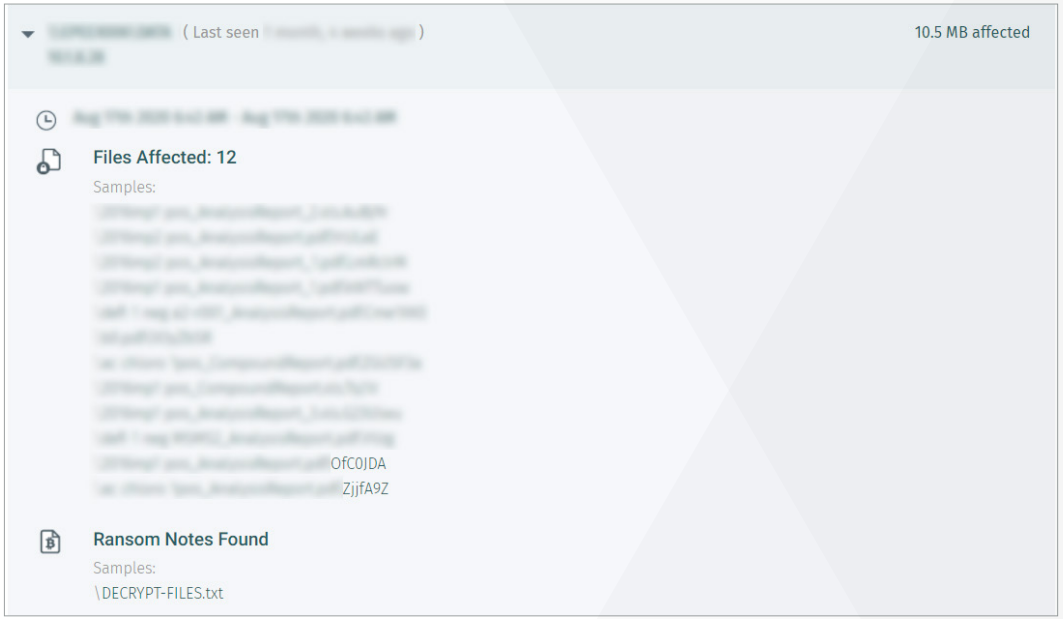
Host view and detection associated

This host showed several lateral movement and reconnaissance steps prior to the ransomware attack.



Ransomware detection

Detection details – extension and ransom note title – are compatible with Maze ransomware. The ransomware also had an embedded function to hit several of the known Maze command-and-control machines. These should be monitored for access to evaluate potential data leaks.



Detection details

Binary analysis

The customer provided Vectra with the binaries used during the attack and performed a quick binary analysis of the malicious DLL.

Sample (SHA256):
(redacted)

Analysis environment:
Windows7 SP1 VM, running on VMWare Workstation 15 Pro.

Configuration extraction

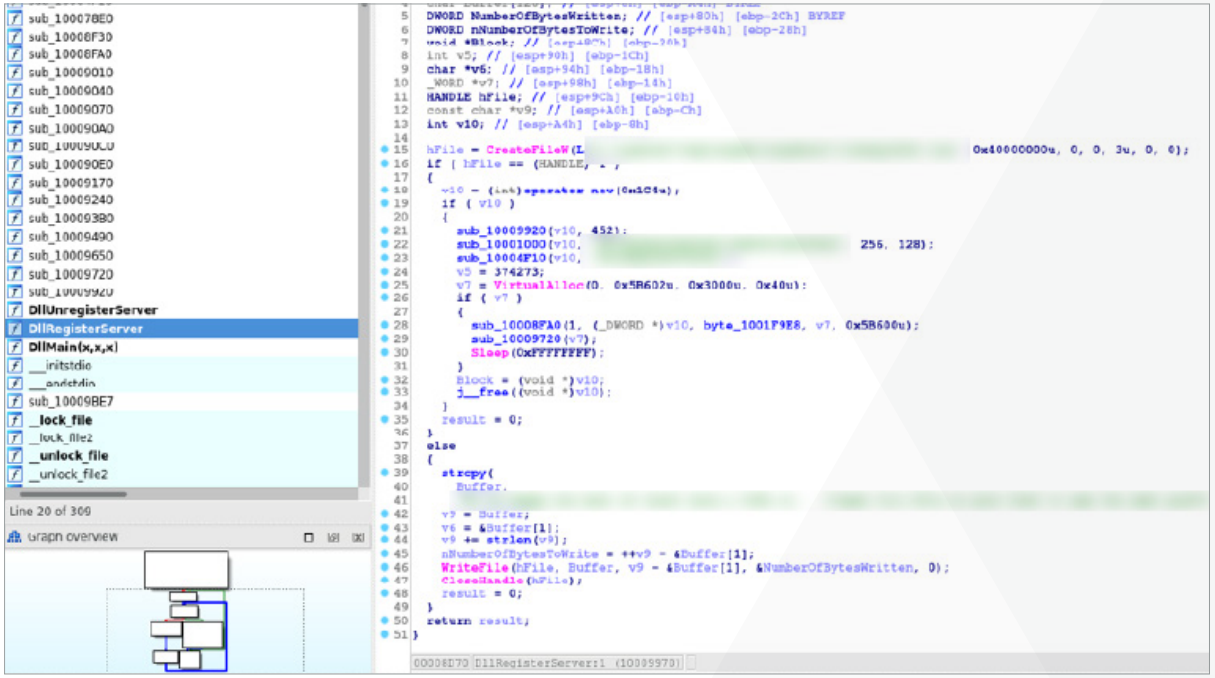
The ransomware configuration was extracted from memory during the execution and provided known Maze command-and-control information embedded in the binary:

- 91.218.114.4
- 91.218.114.11
- 91.218.114.25
- 91.218.114.26
- 91.218.114.31
- 91.218.114.32
- 91.218.114.37
- 91.218.114.38
- 91.218.114.77
- 91.218.114.79

Killswitch

Further analysis revealed a killswitch in the sample used by the attacker. The malware will not encrypt files if the file « C:\random\insulting\path.txt » exists. As a result, Vectra recommended deploying it on all machines, despite its name.

This killswitch can be found in the DllRegisterServer function when the DLL is disassembled, as shown below (pseudocode is given here for better readability).



Killswitch call in DLL

This killswitch acts as follows:

- The ransomware looks for a specific file existence: C:\random\insulting\path.txt (REDACTED)
- If it exists, it writes in it a famous actor's quote: (REDACTED)
- Once this is done, it stops its execution without encrypting anything

These functions are common. It helps malware developers to debug their own ransomware without harming themselves. For example, a language killswitch prevents certain countries being hit by the ransomware.

Vectra recommended creating this file as an empty text file, despite its offensive name, on all users' computers and servers to avoid further damage in case of an incomplete cleanup.

Vectra also recommended monitoring the use of the regsvr32 command, if possible, because it was used to launch the ransomware. Local and firewall logs should complete the elements present in this investigation.

If possible, access to this file should be monitored to identify other potentially infected hosts.

Appendix - Timeline of attack and compromised hosts

Vectra detection	Associated attacker behavior	dest_hosts	comments	MITRE ATT&CK mapping
Port sweep (reconnaissance)	• Infected internal system contacts several internal IP addresses on a few ports to find systems that run certain software that might be vulnerable to an attack	N/A	Ping scan	• T1082 System Information Discovery • T1018 Remote System Discovery • T1072 Third Party Software • T1046 Network Service Scanning • T1016 System Network Configuration Discovery
Automated replication (lateral movement)	• Compromised host that is part of a botnet tries to expand the botnet's footprint by infecting other hosts • Infected host taking part in a targeted attack spreads laterally to get closer to data it wants to exfiltrate	6 hosts	Host trying to access file shares on port 445, might be unrelated to the attack	• T1072 Software Deployment Tools • T1210 Exploitation of Remote Services
Automated replication (lateral movement)	• Compromised host that is part of a botnet tries to expand the botnet's footprint by infecting other hosts • Infected host taking part in targeted attack spreads laterally to get closer to data it wants to exfiltrate	6 hosts	Host trying to access file shares on port 445, might be unrelated to the attack	• T1072 Software Deployment Tools • T1210 Exploitation of Remote Services
Suspicious remote execution (lateral movement)	• 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	1 host	Customer account used	• 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
Suspicious remote execution (lateral movement)	• Infected host, malicious insider or red team participant controls a host to spread laterally by executing code on systems to which it has connected	3 hosts	Customer account used	• 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

Vectra detection	Associated attacker behavior	dest_hosts	comments	MITRE ATT&CK mapping
Suspicious remote execution (lateral movement)	• Infected host, malicious insider or red team participant controls a host to spread laterally by executing code on systems to which it has connected	1 host	Customer account used	• 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
Port sweep (reconnaissance)	• Infected internal system contacts several internal IP addresses on a few ports to find systems that run certain software that might be vulnerable to an attack	N/A	Port sweep on port 3389	• T1082 System Information Discovery • T1018 Remote System Discovery • T1072 Third Party Software • T1046 Network Service Scanning • T1016 System Network Configuration Discovery
Automated replication (lateral movement)	• Compromised host that is part of a botnet tries to expand the botnet's footprint by infecting other hosts • Infected host taking part in a targeted attack spreads laterally to get closer to data it wants to exfiltrate	5 hosts	Host trying to access file shares on port 445, might be unrelated to the attack	• T1072 Software Deployment Tools • T1210 Exploitation of Remote Services
Suspicious remote execution (lateral movement)	• Infected host, malicious insider or red team participant controls a host to spread laterally by executing code on systems to which it has connected	5 hosts	Customer account used	• 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
File share enumeration (reconnaissance)	• Attacker looks for data to exfiltrate or files that provide additional information to achieving attack goals	30-40 hosts	Customer account used	• T1039 Data from Network Shared Drive • T1119 Automated Collection • T1135 Network Share Discovery

Vectra detection	Associated attacker behavior	dest_hosts	comments	MITRE ATT&CK mapping
Suspicious remote execution (lateral movement)	• Infected host, malicious insider or red team participant controls a host to spread laterally by executing code on systems to which it has connected	3 hosts	Customer account used	• 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
File share enumeration (reconnaissance)	• Attacker looks for data to exfiltrate or files that provide additional information to achieving attack goals	About 30 hosts	Customer account used	• T1039 Data from Network Shared Drive • T1119 Automated Collection • T1135 Network Share Discovery
External remote access (command and control)	• Host includes malware with remote access capability (e.g. Meterpreter, Poison Ivy) connects to command-and-control server and receives commands from a human operator	External Ukrainian IP address	External Ukrainian IP address	• 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

Vectra detection	Associated attacker behavior	dest_hosts	comments	MITRE ATT&CK mapping
Suspicious relay (command and control)	• Compromised host relays information to and from a host deeper inside the network	Internal IP -> external Ukrainian IP address	External Ukrainian IP address	• T1090 Proxy • T1104 Multi-Stage Channels
Suspicious remote execution (lateral movement)	• Infected host, malicious insider or red team participant controls a host to spread laterally by executing code on systems to which it has connected	1 host	Customer account used	• 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
Ransomware file activity (lateral movement)	• Internal host is infected with a variant of ransomware	3 file servers targeted	N/A	• T1486 Data Encrypted for Impact
Automated replication (lateral movement)	• Compromised host that is part of a botnet tries to expand the botnet's footprint by infecting other hosts • Infected host taking part in a targeted attack spreads laterally to get closer to data it wants to exfiltrate	5 hosts	Host tries to access file shares on Port 445, might be unrelated to the attack	• T1072 Software Deployment Tools • T1210 Exploitation of Remote Services
Suspicious remote desktop (lateral movement)	• External foreign attacker takes control of an internal host and uses its unusual keyboard layout to connect to RDP servers and move laterally • External attacker takes control of an internal host and uses its own RDP stack to connect to internal RDP servers and move laterally	1 host	Client token: link. Might be unrelated to the attack	• T1003 OS Credential Dumping • T1078 Valid Accounts • T1212 Exploitation for Credential Access • T1552 Unsecure Credentials • T1555 Credentials from Password Stores • T1021 Remote Services

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai