Securing Against Ransomware Through MITRE ATT&CK– It’s Too Late If They Exfiltrate

Introduction

The cybersecurity industry is seeing a rapid rise in ransomware and the growing trail of destruction caused by such attacks. While many have provided technical details and breakdowns of the malware family, there has not yet been a comprehensive discussion regarding the network communication aspects of the threat.

At first, it may seem that the network is unimportant since ransomware is executed locally, on the endpoint. However, network traffic can provide several early warning signs of this activity, giving defenders the time to disrupt the attack before significant damage is done.

Based on detections from the Arista NDR platform across a wide variety of customer environments, this whitepaper documents how and what to look for while network threat hunting for ransomware threat actors. This paper also maps the guidance to the MITRE ATT&CK framework.

A Short History of Ransomware

Ransomware continues to be one of the more difficult attacks to defend. It is used by advanced actors and highly organized cyber criminals looking to take advantage of and extort victims. In 2021, Gartner estimated that only 1% of global governments have rules around ransomware, with a forecast for that to grow to 30% by 2025.

While it has been around for some time, 2021 witnessed substantial and widespread impact due to ransomware. Approximately 37% of global organizations said they were the victim of some form of a ransomware attack in 2021, according to IDC's "2021 Ransomware Study". Security vendor BeyondTrust predicted that there will be a variation on double extortion with ransomware in 2022, as attackers try to execute more personalized attacks. To that effect, organizations and Governments worldwide have started installing appropriate response measures to stem the tide of such attacks.

https://www.idc.com/getdoc.jsp?containerId=US48093721

https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions

Ransomware as a Service

A new trend over the last few years where affiliates pay ransomware operators to launch attacks, further increasing the number of bad actors that target organizations today. These service kits are available at a trivial price and further increase an organization's attack surface.

Aligning Ransomware Defenses to the MITRE ATT&CK Framework

There are several early warning signs before exfiltration and encryption. Research shows that in most cases, three days of dwell-time elapses between these early warning signs and the detonation of the ransomware. As you would expect, intervention in a critical three-day period can significantly contain the damage.

So, how does a security team find these weak but important early warning signals? In our experience, while some organizations have endpoint security detection and response (EDR), and a few have the right level of logging, it takes a combination of EDR, logging, and network monitoring (NDR) to really have full visibility into such threats. Unfortunately, all too often we find that organizations struggle to monitor their network and therefore miss many of the early warning indicators that are apparent from observing the ransomware actors. We are sharing these indicators to help others benefit from early detection. We've even broken it down by MITRE category to help with operationalizing the information.

Finding Initial Access in the Network

With ransomware actors there are several initial access vectors, such as phishing attachments and links, supply chain compromise, external-facing remote access such as Microsoft's Remote Desktop Protocol (RDP), and access via valid accounts. All of these can be discovered while network threat hunting across the traffic. Furthermore, given this represents the actor's earliest foray into the environment, detecting this initial access is the organization's best bet to significantly mitigate the impact.

The following infographic is the format we will use throughout this paper. The first column of the graphic represents the MITRE ATT&CK category. The next column contains the specific MITRE techniques (with IDs) that have been observed in the wild with ransomware. Finally, we provide a list of early warning signs to help drive the network threat hunting process.

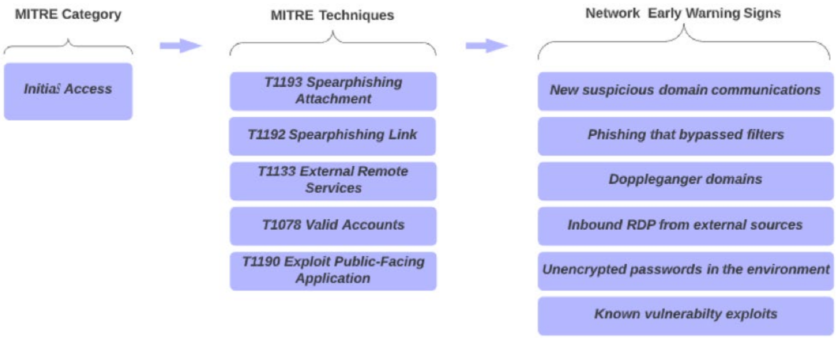

MITRE Category
MITRE Techniques
Network Early Warning Signs
Initial Access
T1193 Spearphishing Attachment
T1192 Spearphishing Link
T1133 External Remote Services
T1078 Valid Accounts
T1190 Exploit Public-Facing Application
New suspicious domain communications
Phishing that bypassed filters
Doppleganger domains
Inbound RDP from external sources
Unencrypted passwords in the environment
Known vulnerabilty exploits

Figure 1: Attackers finding Initial Access on the network

https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

Based on MITRE techniques, here are a few recommendations:

Phishing Techniques

As a network analyst, start by reviewing internet-bound traffic and look for previously unseen domains. Another useful source of information is domains that the user population may have submitted to an abuse channel. Finally, there are plenty of lists of known Maze IOCs that existing network security tools should hopefully already be flagging, but it doesn't hurt to look for those too. In fact, you get bonus points for hunting based on underlying domain infrastructure such as nameservers, registrars etc.

Doppelganger Domains

Expanding on the phishing techniques the network can provide a good view into usage of doppelganger domains in the environment. Ideally, security teams should look for typo squatting for the most common organizational / third party domains in use as well as globally popular ones like the Alexa top 500.

Inbound RDP

It is important to monitor all inbound remote access protocol connections as well as any evidence of scanning or brute force activity. In addition, this activity can be compared to an expected list of all external facing user accounts and the activity of those accounts on the network.

Exposed Passwords and Password Stores

In its simplest form, monitor SMB, FTP, HTTP and other protocol connections to both internal and external devices looking for password files stores, clear text passwords in transit, HTTP Basic authentication, Base64 and other obfuscated passwords in the URI and traffic payload, etc. All of these are useful to uncover systems and processes that use or store weak passwords perhaps in combination with insecure authentication methods. These findings should be considered for remediation, or at the very least have some compensating controls applied.

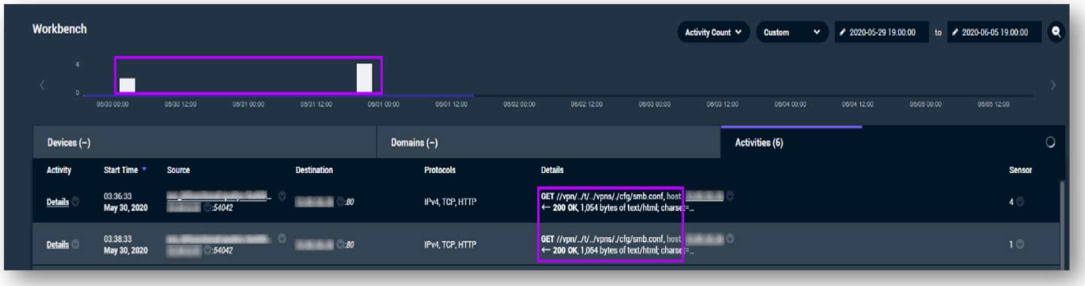
Known Vulnerabilities

Detecting exploitation of vulnerabilities across the network can usually be done by first identifying if the exploitable device and version exists in the environment, and then validating if any successful malicious activity has occurred. For instance, exploitation of the Citrix NetScaler Vulnerability (CVE-2019-19781)[4] involves hunting for a URI string such as “//vpn/../t/../vpns/./cfg/smb.conf “ followed by a HTTP POST request and then a HTTP GET for an XML file.

Supply Chain Compromise

Adversaries may manipulate products or product delivery mechanisms to compromise data or the system at the consumer of those products. It is therefore important to have complete visibility into the organization's entire software supply chain. While supply chain compromise can impact any component of hardware or software, attackers looking to gain execution have often focused on malicious additions to legitimate software in the software distribution or update channels.

Figure 2 shows an example of hunting for URI strings to identify exploitation of the Citrix NetScaler vulnerability.

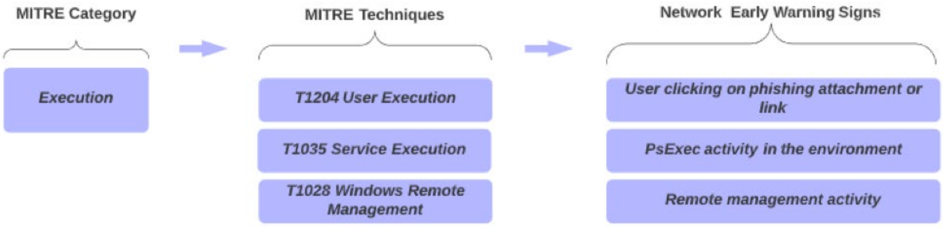


Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	03:36:33 May 30, 2020	[redacted] [redacted] :54042	[redacted] :80	IPv4, TCP, HTTP	GET //vpn/../t/../vpns/./cfg/smb.conf, host [redacted] ← 200 OK, 1,054 bytes of text/html; charse=...	4
Details	03:38:33 May 30, 2020	[redacted] [redacted] :54042	[redacted] :80	IPv4, TCP, HTTP	GET //vpn/../t/../vpns/./cfg/smb.conf, host [redacted] ← 200 OK, 1,054 bytes of text/html; charse=...	1

Figure 2: Threat hunting for attempts to exploit the Citrix NetScaler vulnerability (CVE-2019-19781)

Find the Execution Across the Wire

Next, let's dive into the common characteristics of ransomware actors at the execution phase. Using the same rubric as above, the figure below presents common early warning signs, including users tricked into clicking a phishing link or attachment, or when certain tools such as PsExec are used in the environment.



MITRE Category

Execution

MITRE Techniques

T1204 User Execution

T1035 Service Execution

T1028 Windows Remote Management

Network Early Warning Signs

User clicking on phishing attachment or link

PsExec activity in the environment

Remote management activity

Figure 3: Early warning signs at the execution stage

Hunting for Execution uncovers:

Phishing Techniques

It is possible to identify and then track those users who are prone to this type of activity. This kind of information may be gleaned through phishing related training and monitoring the historical trend of users who fall victim to phishing attacks. In addition, it is important to monitor and hunt for suspicious connections as described in the Initial Access section. Examine request headers to identify suspect phishing domains that may have bypassed email filters and successfully accessed attacker infrastructure. Furthermore, we can then validate if and how much data was downloaded.

PsExec Usage

PsExec leaves several characteristic network fingerprints behind. In the simplest form, it would involve hunting for filenames like PsExec across SMB. However, this is clearly a method that can be easily evaded, so security teams would do well to use more sophisticated techniques. For example, they could look for a chain of activities like File Input Output (IO) over SMB that uses PsExec to extract contents, and then later executes on another device. It is also important to look for the underlying techniques used since those are also used by other tools such as scshell.

Remote Management

To identify potential adversarial remote management we can look at devices that connect to the SVCCTL service and then perform CREATE, READ, WRITE, CLOSE actions. In addition, this list can be filtered to exclude known good systems that are part of legitimate business processes, where the behavior is therefore expected.

https://awakesecurity.com/blog/citrix-gateway-vulnerability-cve-2019-19781-analysis/

If I Persist Then I Exist

Adversaries using ransomware rely on several common techniques, such as a web shell on internet-facing systems and the use of valid accounts obtained within the environment. Once the adversary has a persistence foothold, it starts to become increasingly difficult to mitigate impact. Web shell activity, as well as potentially compromised accounts can be reliably identified on the network, often before there is significant impact.

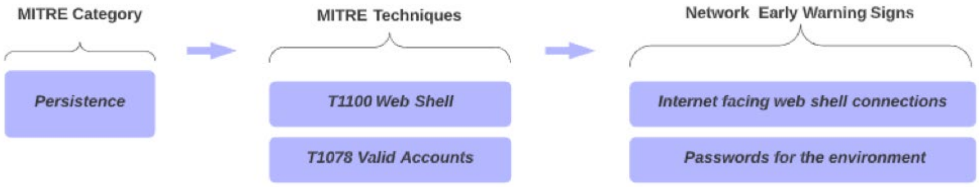

MITRE Category
Persistence
MITRE Techniques
T1100 Web Shell
T1078 Valid Accounts
Network Early Warning Signs
Internet facing web shell connections
Passwords for the environment

Figure 4: How an adversary establishes a persistent foothold

Hunting for Persistence techniques can highlight:

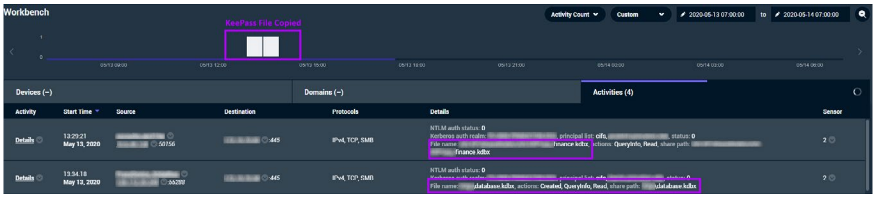
Web Shells

Detecting a web shell is a little more complex and may require more advanced monitoring or threat hunting across the traffic. First off, hunt for somewhat unique device activity connections (e.g. atypical ports, browser user agents, etc.) from external sources to external facing devices. Additionally, identify uncommon device connections with successful HTTP requests, that appear similar to script activity and have a limited number of connections to the device, relative to other known web servers, etc.

KeePass Stores

The actors of Maze also look for KeePass files. This is an important lead indicator. The attackers will look for unencrypted passwords, and that's why it is vital for security teams to hunt for this behavior too. For instance, hunt for attacker's searching for password stores by reviewing URIs or password related documents across SMB shares in the environment. It is important to especially pay attention to any activity involving both a read and copy of those files. Any user account involved in such activity can then be investigated in greater detail especially if the behavior is an outlier.

Figure 5 shows two examples of hunting for this behavior: one of a finance KeePass file and the other of a database KeePass file store being copied off a system drive.



Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	13:29:21 May 13, 2020	[redacted] [redacted] :50156	[redacted] :445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted]finance.kdbx, actions: QueryInfo, Read, share path: [redacted]finance.kdbx	2
Details	13.34.18 May 13, 2020	[redacted] [redacted] :56288	[redacted] :445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted]database.kdbx, actions: Created, QueryInfo, Read, share path: [redacted]database.kdbx	2

Figure 5: Threat hunting for attempts to read and copy password stores

What Is That New Privileged Activity?

As an adversary gains higher levels of access it becomes significantly more difficult to pick up additional signs of activity in the environment. For example, techniques used for persistence like privileged activity can often go undetected unless caught on the network. We elaborate on how these manifest as privilege escalation.

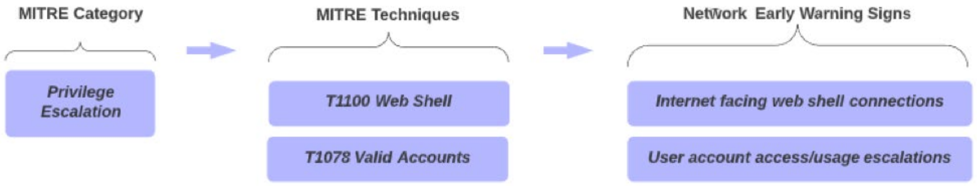

MITRE Category
Privilege Escalation
MITRE Techniques
T1100 Web Shell
T1078 Valid Accounts
Network Early Warning Signs
Internet facing web shell connections
User account access/usage escalations

Figure 6: Taking advantage of privileged access to the enterprise network

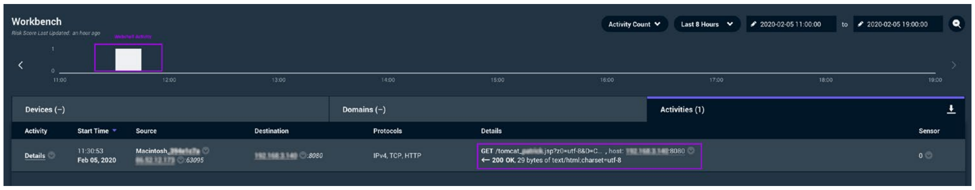
Web Shells

As mentioned above in the If I Persist Then I Exist section, discovering a web shell requires consolidating several data points. To help isolate and speed up the process, it might help to limit the focus to external facing web and gateway systems.

Escalating Access

Almost every organization has some poor hygiene when it comes to storing unencrypted passwords. Since the attacker looks for password files across an environment, the threat hunter can use the network security tools to monitor for the access and remote copy of password files across SMB. This can be done by searching the network SMB traffic for variants of the term "passw" with common extensions such as doc, txt, xls, docx, xlsx, csv, jpg, etc. This data can be used to detect and clean up the hygiene issues and prevent large scale access to valid accounts by requiring all these passwords to be put in secure password storage.

Figure 7 uncovers Apache Tomcat web shell activity with a script in the URL.



Workbench

Risk Score Last Updated: an hour ago

Activity Count | Last 8 Hours | 2020-02-05 11:00:00 to 2020-02-05 19:00:00

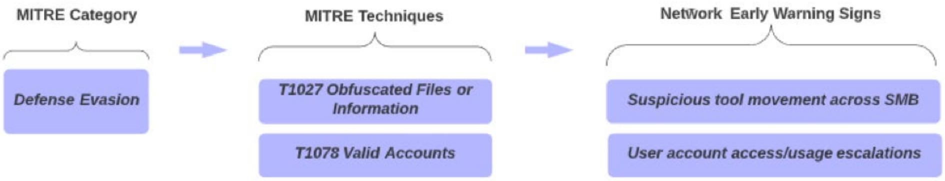
Devices (–) | Domains (–) | Activities (1)

Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	11:30:53 Feb 05, 2020	Macintosh_[redacted] [redacted] :63095	[redacted] :8080	IPv4, TCP, HTTP	GET /tomcat_[redacted].jsp?z0=utf-8&D=C... , host: [redacted]:8080 ← 200 OK, 29 bytes of text/html;charset=utf-8	0

Figure 7: Threat hunting for web shells on the network

Signs of Defense Evasion

To hide files and their access to different systems, adversaries rename files, encode, archive, and use other mechanisms to hide their tracks. Even with those techniques there are few early warning signs to detect the adversary trying to avoid detection. In fact, we would argue that attempts at evasion are in themselves highly suspicious.



MITRE Category
MITRE Techniques
Network Early Warning Signs
Defense Evasion
T1027 Obfuscated Files or Information
T1078 Valid Accounts
Suspicious tool movement across SMB
User account access/usage escalations

Figure 8: Early warning signs of adversaries trying to avoid detection

A few common network threat hunting approaches include:

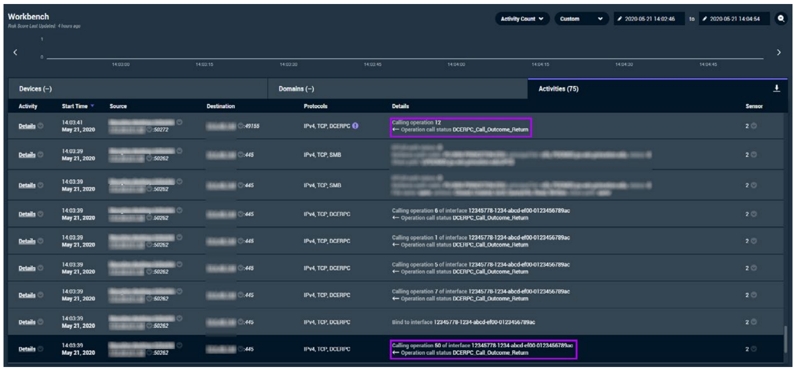
Obfuscated Tools and More

As an adversary attempts to gain more access to the environment, the actor may copy different tools across shares. In some cases, we can detect this activity by hunting across all the SMB file activity for known attack tools. We can look for certain tools by certificate issuer name, we can hunt for unknown protocol TCP sessions in coordination with attack tool port usage, and we can also hunt for isolated devices with few activities (e.g. few devices with few activities that appear to be using the tools / protocols in question).

New Account Creation

In many cases an adversary will also create new user accounts as a mechanism to blend in with normal activity. These behaviors can be discovered during a threat hunt looking for the SAMR UUID and user creation actions such as opnum 12 SamrCreateUserInDomain and opnum 50 SamrCreateUser2InDomain in DCERPC network traffic.

Figure 9 shows an example of how the creation of a new user account manifests in network traffic. This action was likely performed with the net use or similar command from a workstation to another device that is not a domain controller.



Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	14:03:41 May 21, 2020	[redacted] [redacted] :50272	[redacted] :49155	IPv4, TCP, DCERPC	Calling operation 12 ← Operation call status DCERPC_Call_Outcome_Return	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, SMB	[redacted]	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, SMB	[redacted]	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, DCERPC	Calling operation 6 of interface 12345778-1234-abcd-ef00-0123456789ac ← Operation call status DCERPC_Call_Outcome_Return	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, DCERPC	Calling operation 1 of interface 12345778-1234-abcd-ef00-0123456789ac ← Operation call status DCERPC_Call_Outcome_Return	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, DCERPC	Calling operation 5 of interface 12345778-1234-abcd-ef00-0123456789ac ← Operation call status DCERPC_Call_Outcome_Return	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, DCERPC	Calling operation 7 of interface 12345778-1234-abcd-ef00-0123456789ac ← Operation call status DCERPC_Call_Outcome_Return	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, DCERPC	Bind to interface 12345778-1234-abcd-ef00-0123456789ac	2
Details	14:03:39 May 21, 2020	[redacted] [redacted] :50262	[redacted] :445	IPv4, TCP, DCERPC	Calling operation 50 of interface 12345778-1234-abcd-ef00-0123456789ac ← Operation call status DCERPC_Call_Outcome_Return	2

Figure 9: User account creation as seen from the network

Early Warnings of Credential Access

Hunting for credential abuse such as brute force of accounts is one early warning sign. Additionally, there are several defensive controls that can be put in place to help limit or restrict access to credentials. The threat hunter can enable this process by providing situational awareness of network hygiene including specific attack tool usage, attempts to misuse credentials, weak passwords, and insecure password storage.

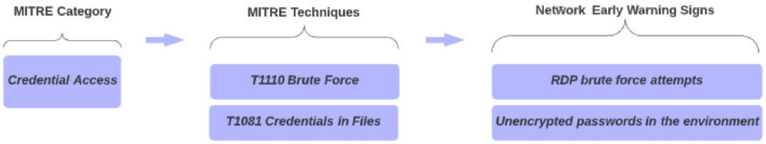

MITRE Category
MITRE Techniques
Network Early Warning Signs
Credential Access
T1110 Brute Force
T1081 Credentials in Files
RDP brute force attempts
Unencrypted passwords in the environment

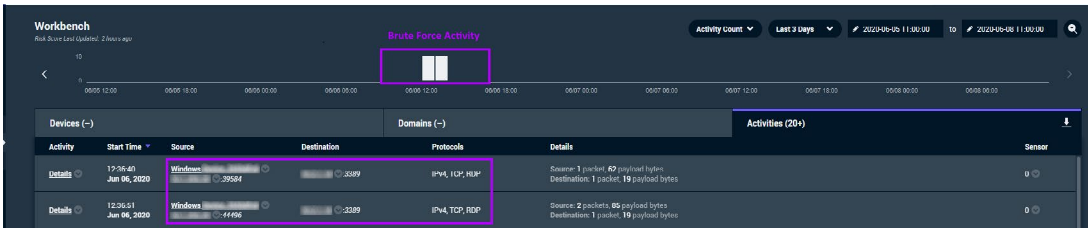
Figure 10: Credential abuse warning signals

As we can see from the MITRE mappings, some of the following can be used to help detect signs of the adversary in the environment.

RDP Brute Force

After excluding expected vulnerability scanners and other similar services it is possible to hunt through RDP network activity and identify brute force attacks on exposed ports via frequency analysis.

For instance, figure 11 shows how RDP brute force can stick out on a network activity timeline and can then be reviewed for maliciousness.



Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	12:36:40 Jun 06, 2020	Windows [redacted] [redacted] :39584	[redacted] :3389	IPv4, TCP, RDP	Source: 1 packet, 62 payload bytes Destination: 1 packet, 19 payload bytes	0
Details	12:36:51 Jun 06, 2020	Windows [redacted] [redacted] :44496	[redacted] :3389	IPv4, TCP, RDP	Source: 2 packets, 85 payload bytes Destination: 1 packet, 19 payload bytes	0

Figure 11: Threat hunting for RDP brute force activity

Credentials in Files or Extracted by Tools

The previous sections talked extensively about ways to hunt for the usage of KeePass or other files containing passwords as well as detect users copying these files over protocols such as SMB on the network. In addition, we also discussed how a threat hunter can identify potential obfuscated tool activity or the use of PsExec and PowerShell, if a tool is used to copy passwords from important systems and file shares. The key preventative recommendation is dealing with the password file problem ahead of time.

The Signs of Discovery are Everywhere

When reviewing the ransomware adversary’s internal reconnaissance efforts, we find the number and types of methods used for discovery are numerous. There are enumeration approaches, usage of specific tools and several collection methods that fall into this category. Each of these leaves their own trail of evidence that can be identified before the exfiltration and encryption occurs.

When reviewing the ransomware adversary’s internal reconnaissance efforts, we find the number and types of methods used for discovery are numerous. There are enumeration approaches, usage of specific tools and several collection methods that fall into this category. Each of these leaves their own trail of evidence that can be identified before the exfiltration and encryption occurs.

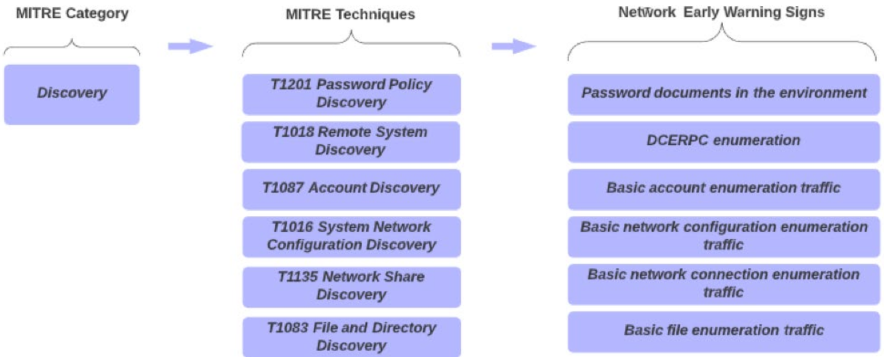

MITRE Category
MITRE Techniques
Network Early Warning Signs
Discovery
T1201 Password Policy Discovery
T1018 Remote System Discovery
T1087 Account Discovery
T1016 System Network Configuration Discovery
T1135 Network Share Discovery
T1083 File and Directory Discovery
Password documents in the environment
DCERPC enumeration
Basic account enumeration traffic
Basic network configuration enumeration traffic
Basic network connection enumeration traffic
Basic file enumeration traffic

Figure 12: Signals to discover ransomware before exfiltration or encryption

As displayed in the examples below, there are many early warning signs for discovery activity.

Password Policy Documents

Similar to how we find the password stores, a threat hunt can identify the password policy documents in the environment and look for those being copied via SMB. We can also cross reference that with other information such as when the device downloading this information first appeared on the network. This helps for instance to exclude new hires that might be downloading the document.

DCERPC Password Policy Enumeration

Other methods of enumeration and harvesting can also be used to identify password policies. For example, we can threat hunt across DCERPC connections looking for opnum 44 over SMB, which is the method SamrGetUserDomainPasswordInformation.

DCERPC Computer Name Enumeration

As part of discovery an adversary will map out the environment looking for important systems. One method is to enumerate device names. Network threat hunters can look for the adversary by searching through the DCERPC traffic for the “wkssvc” string and opnum 30, which is the NetrEnumerateComputerNames method.

Account Enumeration

Similar to other methods of hunting for users performing enumeration, it is also possible to hunt for the following behaviors:

- Opnum 11 the LsarEnumerateAccounts method
- Opnum 35 the LsarEnumerateAccountsWithUserRight method
- Opnum 36 the LsarEnumerateAccountRights method

Network Configuration Enumeration

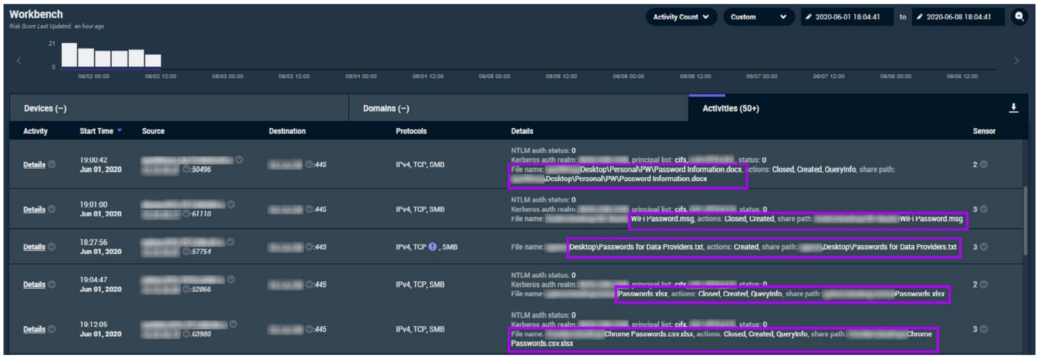
Hunting for adversaries that are mapping out the network configuration can be done by looking for network connections to the following.

- RPC interface UUID SRVSVC protocol with method NetrServerTransportEnum opnum 26 to identify the ports
- RPC interface UUID WKSSVC protocol with method NetrWkstaTransportEnum opnum 5 for workstation ports

File Enumeration

A ransomware adversary such as those with Maze will obtain file and directory listings to help collect data prior to encryption. Hunting with DCERPC can be used to identify this adversarial behavior as well, specifically by identifying RPC interface calls to "srvsvc" with opnum 9, which is the NetrFileEnum method.

Figure 13 shows how both an attacker and a threat hunter can find multiple clear text password stores in different formats such as personal passwords in word and text files. Additionally, we are also able to find stores such as those that are part of data providers or Chrome / browser systems. Clearly, all of these must be protected from the adversary.

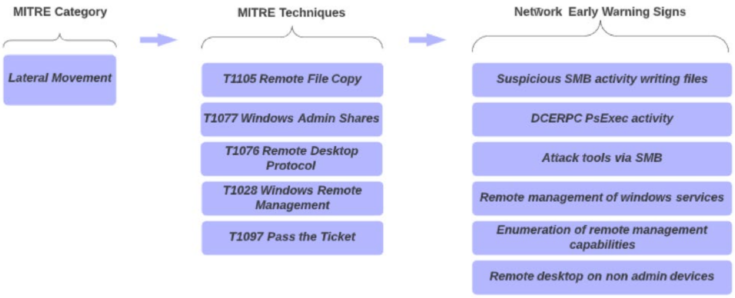


Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	19:00:42 Jun 01, 2020	[redacted] [redacted]:50496	[redacted]:445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted]Desktop\Personal\PW\Password Information.docx, actions: Closed, Created, QueryInfo, share path: [redacted]\Desktop\Personal\PW\Password Information.docx	2
Details	19:01:00 Jun 01, 2020	[redacted] [redacted]:61110	[redacted]:445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted]Wi-Fi Password.msg, actions: Closed, Created, share path: [redacted]Wi-Fi Password.msg	3
Details	18:27:56 Jun 01, 2020	[redacted] [redacted]:57754	[redacted]:445	IPv4, TCP ! , SMB	File name: [redacted]Desktop\Passwords for Data Providers.txt, actions: Created, share path: [redacted]\Desktop\Passwords for Data Providers.txt	3
Details	19:04:47 Jun 01, 2020	[redacted] [redacted]:52866	[redacted]:445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted]Passwords.xlsx, actions: Closed, Created, QueryInfo, share path: [redacted]Passwords.xlsx	2
Details	19:12:05 Jun 01, 2020	[redacted] [redacted]:63980	[redacted]:445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted]Chrome Passwords.csv.xlsx, actions: Closed, Created, QueryInfo, share path: [redacted]Chrome Passwords.csv.xlsx	3

Figure 13: Password stores across the network

Lateral Movement Warning Signs

Threat actors rely on lateral movement techniques to understand the environment and spread through the network. This is especially true in the case of ransomware, where data needs to be collected and prepared prior to enforcing the encryption. With some ransomware like Maze, the actors appear to hijack legitimate RDP sessions and perform many staging activities, all of which provide us with early warning signs.



MITRE Category
MITRE Techniques
Network Early Warning Signs
Lateral Movement
T1105 Remote File Copy
T1077 Windows Admin Shares
T1076 Remote Desktop Protocol
T1028 Windows Remote Management
T1097 Pass the Ticket
Suspicious SMB activity writing files
DCERPC PsExec activity
Attack tools via SMB
Remote management of windows services
Enumeration of remote management capabilities
Remote desktop on non admin devices

Figure 14: Lateral movement warning signals

Given the plethora of lateral movement techniques observed in ransomware attacks, we can use some of the following methods to detect threat activity in the environment.

Suspicious SMB Activity

This includes for instance suspicious file activity such as multiple batch and archive file writes that typically occur prior to the encryption. It is possible to hunt for this activity based on thresholds and outlier analysis for the number of writes associated with common Maze file types such as bat, zip, 7z, etc.

DCERPC PsExec Activity

Leveraging relevant knowledge of DCERPC UUID methods and opnum details, it is possible to hunt for usage of PsExec in the environment.

Attack Tools Across SMB

As previously explained in the Signs of Defense Evasion section, an actor may copy different tools across shares. In some cases, we can detect this activity by reviewing all the SMB file activity for known attack tools or archives that may contain attack tools such as Mimikatz, PowerSploit / PowerView, or tscon. This can be done by reviewing activity for known file hashes across the network, or by using regular expression (regex) patterns.

WinRM

As mentioned in the initial access section, it is possible to hunt for potential adversarial remote management by reviewing devices that connect to the SVCCTL service. In addition, it is also possible to hunt across HTTP POST request connections using the Microsoft WinRM Client user agent. Similarly, it is worth looking at similar activity for PowerShell and Cobalt beacons. Finally, for remote tscon hijack sessions the threat hunt can review the RPC Interface UUID SVCCTL protocol with the following methods.

- RCreateServiceW (Opnum 12)
- RCreateServiceA (Opnum 24)
- RCreateServiceWOW64A (Opnum 44)
- RCreateServiceWOW64 (Opnum 45)

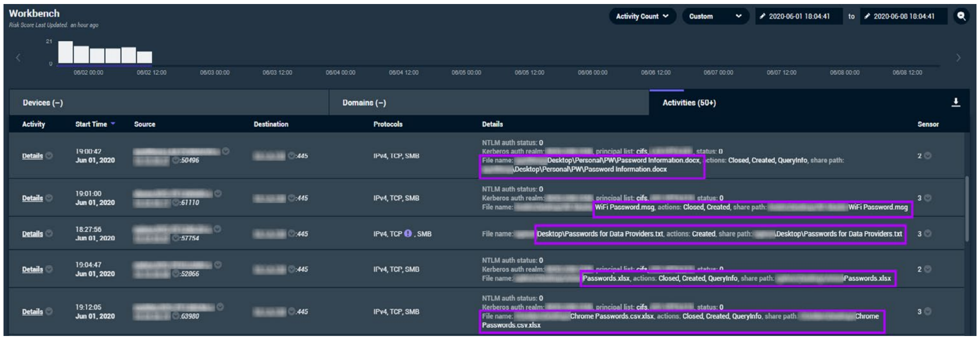
Enumeration of Management Capabilities

Hunting for adversaries that are enumerating remote management capabilities on the network can be done by looking at DCEPRC Interface UUID MGMT protocol with method inq_princ_name opnum 4.

Non-Admin Remote Desktop

The network offers us a good way to look for remote desktop (termsrv) activity. This activity can then be filtered for the behavior showing up on non-administrator systems. This method works particularly well for organizations with specific naming conventions that can be used to filter out devices based on the client name or other string values.

For example, in Figure 15 we see a hunt for the user agent "Microsoft WinRM Client" that identifies PowerShell activity.



Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	19:00:42 Jun 01, 2020	[redacted] [redacted] :50496	[redacted] :445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted]Desktop\Personal\PW\Password Information.docx, actions: Closed, Created, QueryInfo, share path: [redacted]\Desktop\Personal\PW\Password Information.docx	2
Details	19:01:00 Jun 01, 2020	[redacted] [redacted] :61110	[redacted] :445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted] status: 0 File name: [redacted] WiFi Password.msg, actions: Closed, Created, share path: [redacted] WiFi Password.msg	3
Details	18:27:56 Jun 01, 2020	[redacted] [redacted] :57754	[redacted] :445	IPv4, TCP, SMB	File name: [redacted] Desktop\Passwords for Data Providers.txt, actions: Created, share path: [redacted]\Desktop\Passwords for Data Providers.txt	3
Details	19:04:47 Jun 01, 2020	[redacted] [redacted] :52866	[redacted] :445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted] Passwords.xlsx, actions: Closed, Created, QueryInfo, share path: [redacted] Passwords.xlsx	2
Details	19:12:05 Jun 01, 2020	[redacted] [redacted] :63980	[redacted] :445	IPv4, TCP, SMB	NTLM auth status: 0 Kerberos auth realm: [redacted], principal list: cifs, [redacted], status: 0 File name: [redacted] Chrome Passwords.csv.xlsx, actions: Closed, Created, QueryInfo, share path: [redacted] Chrome Passwords.csv.xlsx	3

Figure 15: Hunting for Windows Remote Management activity

Collection Before the Exfiltration

The collection of data is typically used for understanding the environment or in preparation for exfiltration. We have seen the ransomware actors use tools and batch scripts to collect information. They then package up this data into.bat files or archives using the .7z or .exe extensions, all which show traces on the network.

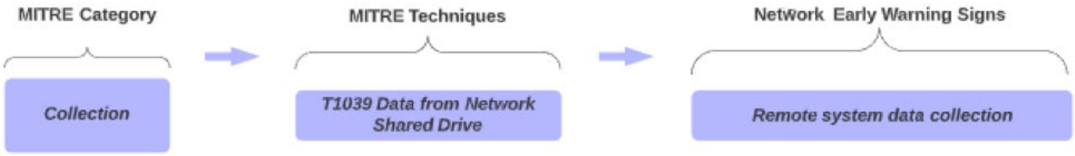

MITRE Category
MITRE Techniques
Network Early Warning Signs
Collection
T1039 Data from Network Shared Drive
Remote system data collection

Figure 16: Data collection before exfiltration

As an example, it is possible to identify similar collection activity associated with ransomware on the network.

Remote system data collection

Hunt for SMB writes of batch file activity followed by copy activity using common archive file extensions.

C2 Warning Signs

Many adversaries will use common ports or remote access tools to try and obtain and maintain command and control (C2) activity. Ransomware actors are no different. Arista has seen evidence of these standard methods as well as ICMP tunnels to connect to the attacker infrastructure.

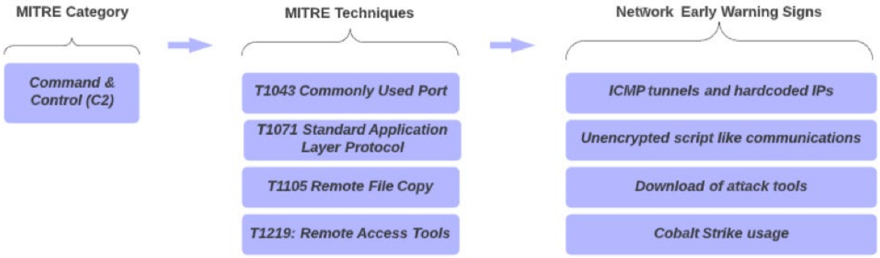

MITRE Category
MITRE Techniques
Network Early Warning Signs
Command & Control (C2)
T1043 Commonly Used Port
T1071 Standard Application Layer Protocol
T1105 Remote File Copy
T1219: Remote Access Tools
ICMP tunnels and hardcoded IPs
Unencrypted script like communications
Download of attack tools
Cobalt Strike usage

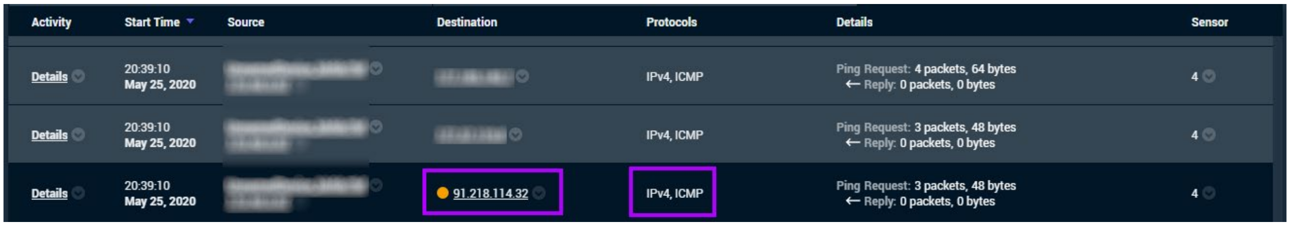
Figure 17: How an ransomware attacker obtains command and control

Below are a few examples of the C2 early warning signs.

ICMP Tunnels and Hardcoded IPs

For some of the C2, Maze actors reveal themselves through patterns in the traffic like ICMP tunneling. For instance, these tunnels are usually destined to hardcoded IPs. However, it is also possible to go beyond ICMP and search for hardcoded IP connections while filtering out proxy and gateway devices and hunting for atypical traffic patterns such as non-browser originating HTTP traffic.

Figure 18 shows an example of a Maze ransomware C2 site being contacted via an ICMP tunnel.



Activity	Start Time	Source	Destination	Protocols	Details	Sensor
Details	20:39:10 May 25, 2020	[redacted]	[redacted]	IPv4, ICMP	Ping Request: 4 packets, 64 bytes ← Reply: 0 packets, 0 bytes	4
Details	20:39:10 May 25, 2020	[redacted]	[redacted]	IPv4, ICMP	Ping Request: 3 packets, 48 bytes ← Reply: 0 packets, 0 bytes	4
Details	20:39:10 May 25, 2020	[redacted]	● 91.218.114.32	IPv4, ICMP	Ping Request: 3 packets, 48 bytes ← Reply: 0 packets, 0 bytes	4

Figure 18: ICMP Tunnel used by Maze Ransomware for command and control

Unencrypted Script-Like Communications

The network also offers a good way to identify randomized script-like communications that Maze often uses for command and control (C2). Typically, this C2 is relatively unique compared to other network activities. We can therefore hunt for requests to domains and IPs that look like they were made by scripts, and share certain criteria such as: less than 5 devices performing these HTTP requests, less than 20 devices with the same user agent etc.

Download of Attack Tools

There are traces of attack tools in HTTP requests. The actors of Maze will often download mimi.zip. Threat hunters can use regex to identify string patterns in URIs, or the search can use hashes. In addition, it is also possible to hunt for certain file sizes and types downloaded from hardcoded IPs and potential suspicious domains.

Cobalt Strike Usage

A Cobalt strike BEACON and FTP to cobalt directories such as "cobalt_uploads" have also been observed to be associated with Maze actors in the wild. Identifying FTP directories with uploads and downloads to cobalt is one mechanism that can be hunted for across the network. In addition, the BEACON and call back to servers have specific traffic patterns and the sites themselves can act as IOCs.

Minimize Exfiltration

As you guessed from the title of this paper, if the hunt is focused on the exfiltration phase, then one might argue we are already late in the attack cycle. At this stage, the risk of exposure of sensitive data in the public realm is dire and many network early warning signs have been missed. However, there is still an opportunity to minimize the impact.

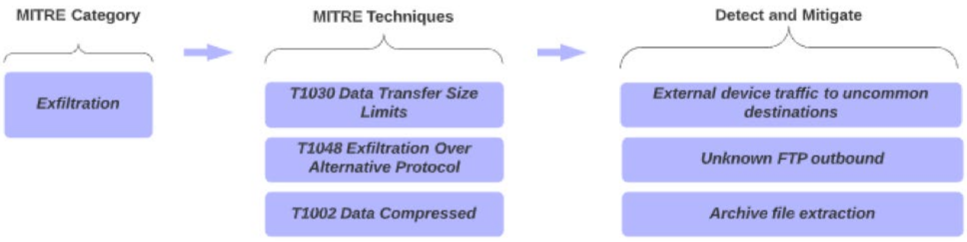


Figure 19: Data Exfiltration early warning signs

Ransomware actors use a few key exfiltration techniques. Some of the common ones described below can be leveraged to detect the exfiltration.

External Device Traffic

Three good methods that can be used to hunt for external device traffic include: looking for large transfers to external destinations, looking for use of non-browser traffic to notable domains, and looking for devices pushing data to an internal system. While the last one may seem strange, in many cases we observe external devices push data down to stage it prior to exfiltration.

Unknown FTP Outbound

Similar to hunting for attack tools, we can look for usage of WinSCP in the organization. We can also quickly review all FTP connections and identify those that are outliers e.g. occur from a limited number of systems only and to uncommon external destinations.

Archive File Extraction

Threat hunting for exfiltration of archives is like hunting for exfiltration of encrypted data. As an analyst look for certain activities such as archives uploaded to hard coded external, suspicious, or uncommon IP addresses for the environment.

Too Late - Containment is the Last Resort

At this point, the strategy moves from early warning to containing impact. The important focus at this point is to stop the spread and mitigate the damage.

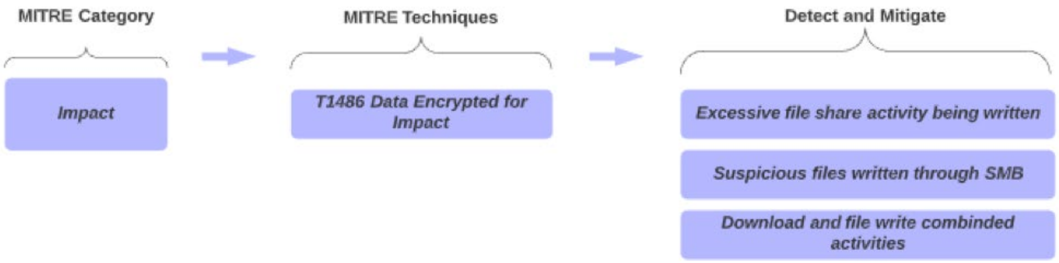

MITRE Category
MITRE Techniques
Detect and Mitigate
Impact
T1486 Data Encrypted for Impact
Excessive file share activity being written
Suspicious files written through SMB
Download and file write combinded activities

Figure 20: Containing ransomware impact

Some of the key mechanisms the network can use to detect impact are:

Excessive file share writes

When executing ransomware there is usually a chain of activities that occur over a short period of time. As observed with Maze the attackers deploy a series of batch scripts and text files across the environment. It is possible to hunt for activity like this and other similar file share writes by looking across SMB for a series of activities and different file types like zip, doc, tmp, bat, txt, etc.

Suspicious file writes via SMB

When ransomware writes there is usually a file name like DECRYPT, encrypted, recover, etc. and in the case of Maze, DECRYPT-FILES.html or DECRYPT-FILES.txt.

Combination download and write

Another key trait used by adversaries of ransomware is to quickly pull down the files and then push them to multiple hosts. We can detect this activity across the network by hunting for HTTP or other downloads with certain file extensions followed by SMB writes to multiple hosts across the network.

Summary

Ransomware is never good news when it shows up at your doorstep. However, with disciplined network threat hunting and monitoring, it is possible to identify a ransomware attack quite early in the lifecycle. Many of the early warning signs are visible on the network and threat hunters would be well served to identify these to help mitigate impact.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor

Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard

#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062

Appendix A: References

- https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions
- https://www.crowdstrike.com/resources/reports/global-security-attitude-survey-2021/
- https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts#
- https://info.corvusinsurance.com/2021-corvus-risk-insights-index

Appendix B: Cheat Sheets

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	What to hunt for?
Initial Access	T1193 Spearphishing Attachment T1192 Spearphishing Link	• Previously unseen or newly registered domains, unique registrars. • Doppelgangers of your organization / partner domains or the Alexa top 500
	T133 External Remote Services	• Inbound RDP from external devices
	T1078 Valid Accounts	• Exposed passwords across SMB, FTP, HTTP, and other clear text usage
	T1190 Exploit Public-Facing Application	• Exposure and exploit of known vulnerabilities
Execution	T1024 User Execution	• Suspicious email behaviors from users and associated downloads
	T1035 Service Execution	• File IO over SMB using PsExec, extracting contents on one system and then later on another system
	T1028 Windows Remote Management	• Remote management connections excluding those from known good devices
Persistence	T1100 Web Shell	• Unique activity connections (e.g. atypical ports and user agents) from external connections
	T1078 Valid Accounts	• Remote copy of KeePass file stores across SMB or HTTP
Privilege Escalation	T1100 Web Shell	• Web shells on external facing web and gateway systems
	T1078 Valid Accounts	• Remote copy of password files across SMB (e.g. files with "passw")
Defense Evasion	T1027 Obfuscated Files or Information	• Adversary tools by port usage, certificate issuer name, or unknown protocol communications
	T1078 Valid Accounts	• New account creation from workstations and other non-admin used devices
Credential Access	T110 Brute Force	• RDP brute force attempts against known username accounts
	T1081 Credentials in Files	• Unencrypted passwords and password files in the environment

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	What to hunt for?
Discovery	T1201 Password Policy Discovery	• Devices copying the password policy off file shares • Enumeration of password policy
	T1018 Remote System Discovery T1087 Account Discovery T1016 System Network Configuration Discovery T1135 Network Share Discovery T1083 File and Directory Discovery	• Enumeration for computer names, accounts, network connections, network configurations, or files
Lateral Movement	T1105 Remote File Copy T1077 Windows Admin Shares	• Suspicious SMB file write activity • PsExec usage to copy attack tools or access other systems • Attack tools copied across SMB
	T1076 Remote Desktop Protocol T1028 Windows Remote Management T1097 Pass the Ticket	• HTTP POST with the use of WinRM user agent • Enumeration of remote management capabilities • Non-admin devices with remote desktop (termsrv) activity
Collection	T1039 Data from Network Share Drive	• Suspicious or uncommon remote system data collection activity
Command & Control (C2)	T1043 Common Used Port T1071 Standard Application Layer Protocol	• ICMP callouts to IP addresses • Non-browser originating HTTP traffic • Unique device HTTP script like requests
	T1105 Remote File Copy	• Downloads of remote access tools
	T1219 Remote Access Tools	• Cobalt strike BEACON and FTP to directories with cobalt in the name
Exfiltration	T1030 Data Transfer Size Limits	• External device traffic to uncommon destinations
	T1048: Exfiltration over Alternative Protocol	• Unknown FTP outbound
	T1002: Data Compressed	• Archive file extraction
Impact	T1486: Data Encrypted for Impact	• Excessive and outlier file share writes • Suspicious file writes via SMB e.g. using the word DECRYPT • Combination of downloads and file writes