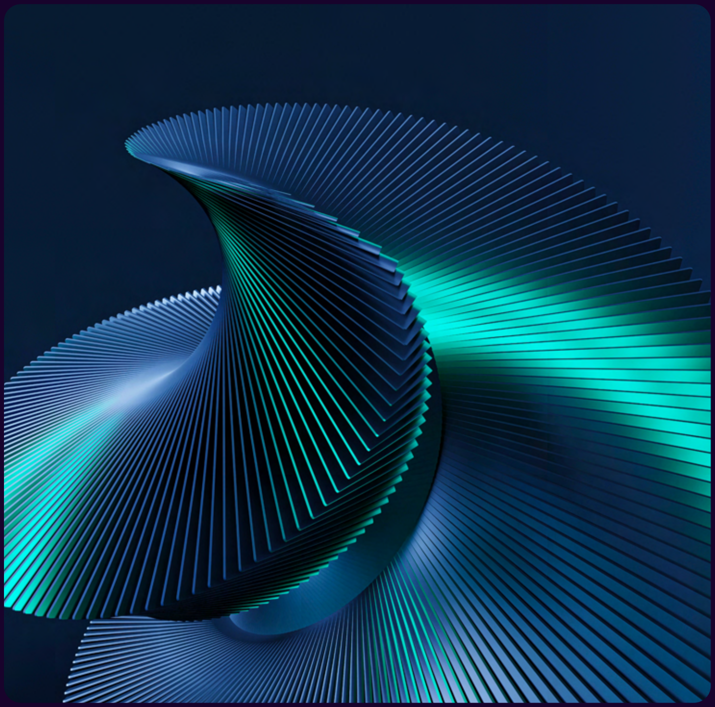
LOGPOINT

EMERGING THREATS PROTECTION REPORT

The Shapeshift of BianLian Ransomware into Encryption-less Extortionists



www.logpoint.com

FOREWORD

BianLian ransomware, coded in Go language and compiled as a 64-bit Windows system; made its debut in June 2022, with a double-extortion approach, infiltrating victim networks with a primary focus on critical infrastructure sectors in the United States and Australia, encrypting their systems, and then leveraging stolen data to demand ransom under the threat of public exposure. When Avast released a powerful decryptor capable of neutralizing the ransomware's encryption, BianLian made a significant shift in their modus operandi and responded by adapting their strategy; transitioning to a new form of extortion that no longer involved encrypting systems and solely focused on the theft of sensitive data, using it as leverage to extort their targets.

Rabindra Dev Bhatta

Logpoint Security Research

Rabindra Dev Bhatta is an Associate Security Analytics Engineer at Logpoint and is currently in his final year of a Master's degree in MSc. IT & Applied Security with a major in Cybersecurity. With a passion for cybersecurity and expertise in threat detection, Rabindra actively contributes to enhancing defense capabilities against multiple threat groups. His combination of academic knowledge and practical experience makes him a valuable asset in combating evolving cyber threats.

TABLE OF CONTENTS

ABOUT LOGPOINT EMERGING THREATS PROTECTION

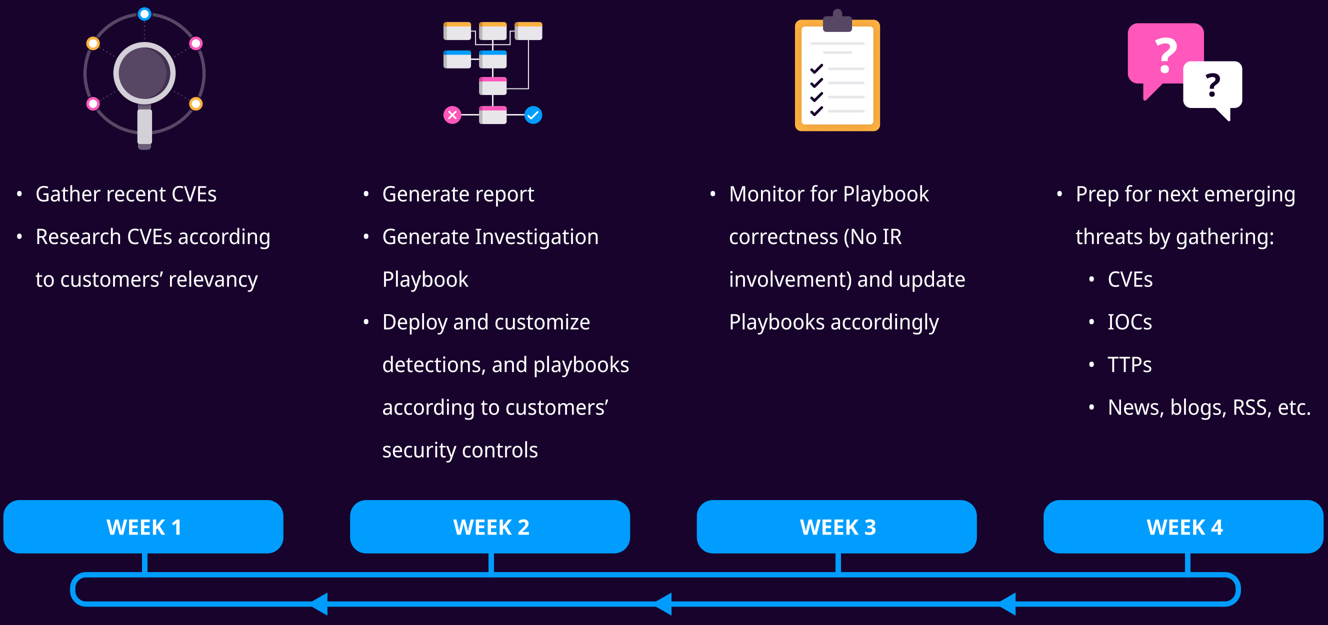
The realm of cybersecurity is in a constant state of flux, with the threat landscape constantly evolving and new risks and vulnerabilities being uncovered regularly. Unfortunately, not every organization possesses the necessary resources or expertise to effectively combat these ever-changing threats. To address this critical need, Logpoint offers a comprehensive solution - **Emerging Threats Protection**.

Emerging Threats Protection is a managed service provided by Logpoint through our team of seasoned security researchers, boasting extensive expertise in the realms of threat intelligence and incident response. With profound knowledge and skills, we ensure that you stay up-to-date with the latest threats, enabling you to stay one step ahead of potential attacks.

Beyond mere information dissemination, we go the extra mile by creating customized detection rules and developing tailor-made playbooks specifically designed to assist you in promptly investigating and mitigating emerging incidents. By leveraging our expertise, you gain a valuable partner in your cybersecurity journey, helping you navigate the complex and ever-evolving landscape of digital threats.

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

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



WEEK 1

- Gather recent CVEs
- Research CVEs according to customers' relevancy

WEEK 2

- Generate report
- Generate Investigation Playbook
- Deploy and customize detections, and playbooks according to customers' security controls

WEEK 3

- Monitor for Playbook correctness (No IR involvement) and update Playbooks accordingly

WEEK 4

- Prep for next emerging threats by gathering:
  - CVEs
  - IOCs
  - TTPs
  - News, blogs, RSS, etc.

INFECTION CHAIN

The infection chain of the BianLian ransomware group involves a series of carefully orchestrated steps that enable its infiltration and subsequent data exfiltration from the target network. Understanding this chain is essential for organizations to develop effective defense strategies against this malicious software.

The infection generally starts with initial compromise, often initiated through phishing emails or malicious downloads, and also sometimes through the exploitation of vulnerabilities. Once a user interacts with a malicious attachment or link, the ransomware gains a foothold in the system, allowing it to establish a persistent presence.

After gaining initial access, the BianLian ransomware group exploits PowerShell and Windows Command Shell, abusing their capability to disable antivirus tools, perform discovery, and execute malicious code on victim machines. It seeks to exploit vulnerabilities to elevate its access level and gain control over critical resources.

The threat actors create new users in the system and add them to the Remote Desktop Users group to be later used for lateral movement in the target network. Following that, they inhibit detection by disabling **antivirus tools**, specifically Windows Defender, Anti-Malware Scan Interface (AMSI), and Sophos EPP, if present in the system; and spread laterally across the network leveraging tools like **Remote Desktop Protocol (RDP)** and **PsExec**. This lateral movement allows the ransomware to maximize its impact and infect as many devices as possible.

Once the BianLian ransomware has successfully traversed the network, it proceeds to exfiltrate valuable data present in the compromised systems utilizing **File Transfer Protocol (FTP)**, the Rclone tool commonly used for **synchronizing files with cloud storage**, and Mega file-sharing service for **exfiltrating victim data over web services**. Before the release of its decryptor, BianLian also utilized sophisticated encryption algorithms to encrypt the files and render them inaccessible, demanding a ransom in exchange for the decryption key.

During the exfiltration and encryption process, the ransomware often communicates with command-and-control (C&C) servers, sending information about the compromised systems and receiving instructions from the threat actors. These communication channels enable the ransomware operators to maintain control over the infected network and facilitate the ransom payment process.

Overall, the infection chain of the BianLian ransomware involves initial compromise through phishing or downloads, lateral movement, data exfiltration, communication with C&C servers, and final demand for ransom.

TECHNICAL ANALYSIS

The infection chain or the cyber-kill chain employed by the BianLian ransomware group has been extensively explained in the following section.

Initial Access

The common method of initial access, **phishing emails**, and exploitation of **leaked/compromised credentials** of **external facing remote services** like Remote Desktop Protocol (RDP), remains a prominent approach for the BianLian ransomware threat actors. Further, BianLian actors have also been actively found to exploit vulnerabilities in **public-facing applications**:

- Microsoft Exchange server vulnerabilities, namely - ProxyShell vulnerability chain: **CVE-2021-34473**, **CVE-2021-34523**, **CVE-2021-31207** to drop web-shell or ngrok payload into the web server
- SonicWall VPN devices

Execution & Persistence

Right after the threat actors find their way into the target system, they start exploiting **PowerShell** and **Windows Command Shell**, abusing their capability to disable antivirus tools, perform discovery, and execute malicious code on victim machines.

They begin executing Powershell commands to create and run a **scheduled task** with "SYSTEM" privileges, which runs `cmd.exe` which again uses `crundll32.exe` to execute the DLL file `netsh.dll` exactly at 04:43.

```
schtasks.exe /RU SYSTEM /create /sc ONCE /<user> /tr "cmd.exe /crundll32.exe c:
\programdata\netsh.dll,Entry" /ST 04:43
```

To maintain persistence, they **create/activate a local administrator account** and also add it to the local Remote Desktop Users group using the command `net.exe`.

```
net.exe localgroup "Remote Desktop Users" <user> /add
```

Also, they **modify the password of existing administrator accounts**.

```
net.exe user <admin> <password> /domain
```

Defense Evasion

The actors leverage **PowerShell** and **Windows Command Shell** to notoriously inhibit detection by disabling **antivirus tools**, specifically Windows Defender and Anti-Malware Scan Interface (AMSI).

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','
NonPublic,* Static').SetValue($null,$true)
```

In some instances, the Deployment Image Servicing and Management (DISM) executable file, `dism.exe` was exploited, to remove the Windows Defender feature.

```
dism.exe /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoRestart
```

Additionally, (if present) they **modify the Windows Registry** values to disable tamper protection for the following Sophos services; additionally allowing them to uninstall these services.

- SAVEnabled

```
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos Endpoint *
Defense\TamperProtection\Config" /t REG_DWORD /v SAVEnabled /d 0 /f
```

- SEDEenabled

```
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos Endpoint *
Defense\TamperProtection\Config" /t REG_DWORD /v SEDEnabled /d 0 /f
```

- SAVService services

```
reg.exe ADD * HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sophos\SAVService\TamperProtection /t
REG_DWORD /v Enabled /d 0 /f
```

They also modify the registry values to disable user authentication for RDP connections

```
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal *
Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f
```

and enable a user to receive help from Remote Assistance, so that, they can exploit the process for their use.

```
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /* v
fAllowToGetHelp /t REG_DWORD /d 1 /f
```

Further, they proceed with modifying the firewall rules using the `netsh.exe` command, to allow RDP traffic by adding new rules to the Windows firewall that allow incoming RDP traffic and enable a pre-existing Windows firewall rule group named Remote Desktop.

```
netsh.exe advfirewall firewall add rule "name=allow RemoteDesktop" dir=in * protocol=TCP localport=<port num> action=allow
```

```
netsh.exe advfirewall firewall set rule "group=remote desktop" new enable=Yes
```

Credential Access

The BianLian group utilizes valid accounts for lateral movement and subsequent activities within targeted networks. They employ the Windows Command Shell to discover **unsecured credentials** on the local machine and store them in locations like the `\Music` folder to avoid detection.

```
findstr /spin "password" *.* >C:\Users\training\Music\<file>.txt
```

and also extract credentials from the **LSASS memory**.

```
cmd.exe /Q /c for /f “tokens=1,2 delims= “ ^%A in (‘”tasklist /fi “Imagename eq lsass.exe” | find “lsass””’) do rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump ^%B \Windows\Temp\<file>.csv full
```

The group also downloads a tool called RDP Recognizer to brute force RDP passwords or identify vulnerabilities, and attempts to access the **NTDS.dit** Active Directory domain database.

During an investigation, the FBI observed the BianLian group employing a portable executable version of an **Impacket** tool called secretsdump.py to facilitate lateral movement to a domain controller and extract credential hashes from it. Impacket, a Python toolkit for network protocol manipulation, allowed the threat actors to execute commands on remote devices using the necessary Windows management protocols typically present in enterprise networks.

```
dump.exe -no-pass -just-dc user.local/<fileserver.local>\@<local_ip>
```

Discovery

BianLian threat actors employ a combination of OS native commands and compiled tools that they download into the victim's environment to gather information about the target's infrastructure. Some of the tools utilized by the BianLian group include:

- **Advanced Port Scanner** - A network scanner tool that performs active scanning of the network to identify open ports and gather additional information about the computers connected to the network.
- **SoftPerfect Network Scanner** - A network scanner tool that allows users to gather information about the network infrastructure, including the availability of devices, open ports, and access to shared folders.
- **PingCastle** - An Active Directory (AD) enumeration tool that can generate an AD map providing a visual representation of the trust relationships within the AD hierarchy and identify potential vulnerabilities.
- **SharpShares** - A multithreaded C# .NET assembled tool that enumerates accessible network shares in a domain.

```
s.exe /threads:50 /ldap:all /verbose /outfile:c:\users\<user>\desktop\1.txt
```

Additionally, the native Windows tools and command shell exploited during the discovery process are:

- `quser.exe` is used to query the **currently logged-in user**. The query has parameters that enable it to execute behind the back and direct its output to the `\Windows\Temp` directory.

```
cmd.exe /Q /c quser 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1
```

- The domain controller is queried time and again to retrieve information on the list of **domain trusts**, the users and **groups** in the domain, the **accounts and computers** in the domain admins group, and the domain computers group.

```
nltest /dclist
nltest /domain_trusts
```

```
net user /domain
```

```
net group /domain
net group 'Domain Admins' /domain
net group 'Domain Computers' /domain
```

Lateral Movement

PsExec and **RDP** are extensively used for lateral movement in the network. The user accounts created and added to the RDP group in the execution and persistence phase, along with **modified Windows firewall rules** in the defense evasion phase, aid to achieve lateral movement.

During one of the investigations, the FBI discovered a forensic artifact named `exp.exe` on a compromised system, believed to be an exploitation tool that takes advantage of the Netlogon vulnerability (**CVE-2020-1472**) and establishes a connection with a domain controller.

```
exp.exe -n <fileserver.local> -t <local_ip>
```

Collection

The FBI also discovered another artifact named `system.exe` on the compromised systems, a malware that **enumerates registry** and files and allows copying of the **clipboard data** of users.

Besides, the threat actors also actively scan the network and systems for possible important files (from the perspective of the organization under attack), which according to their ransom note refer to - financial, client, business, technical, and personal files.

Command & Control

It has been observed that the BianLian ransomware group used a tailored approach i.e. **deploying a custom backdoor**, developed in the Go language, specific to each victim, to establish command and control over compromised systems. An artifact named def.exe an example of a possible backdoor developed by the group was found in one of the systems.

Additionally, they install **remote management and access software**, such as TeamViewer, Atera Agent, SplashTop, or AnyDesk. By incorporating these tools, the group ensures long-term access to the compromised systems, enabling them to exert control, monitor activities, and execute commands as required.

Exfiltration

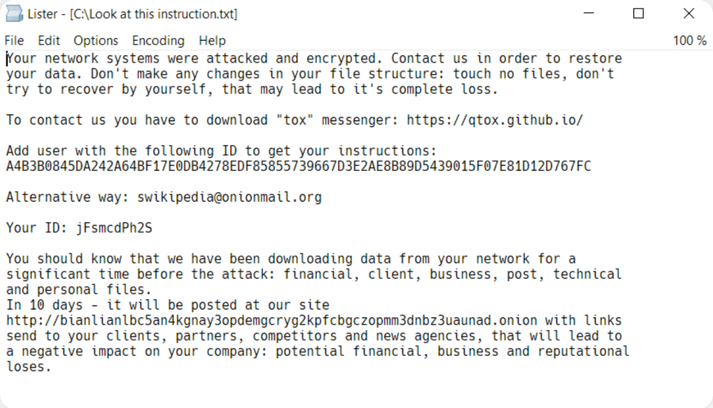
The BianLian group employs PowerShell scripts to search for sensitive files, which they subsequently exfiltrate for data extortion. For data exfiltration, the BianLian group utilizes **File Transfer Protocol (FTP)** and the Rclone tool, commonly used for **synchronizing files with cloud storage**. The FBI has observed the installation of Rclone and other files in generic and often overlooked folders like "programdata\vmware" and music folders. Furthermore, the Australian Cyber Security Centre (ACSC) has noted the group's utilization of the Mega file-sharing service for **exfiltrating victim data over web services**.

Recently, after **Avast** released a power decryptor tool, the group has switched to a pure extortion-only strategy with no system encryption and has intensified it even further.

Impact

Before January 2023, the group would **encrypt** the files with complex algorithms that made use of **AES-256 in CBC mode**, after exfiltration, as part of their double extortion strategy. For the same, the BianLian group employed an encryptor called `encryptor.exe` that modified the encrypted files by appending the ".bianlian" extension. The ransomware previously employed by the BianLian group **does not encrypt files from the beginning to the end** i.e. in a continuous manner. Instead, it utilizes a fixed file offset that is hard-coded within the binary to determine the starting point for the encryption process. Although the specific offset may vary across different samples, none of the identified samples encrypt data from the very start of the files. This unconventional approach suggests a deliberate strategy to selectively encrypt specific portions of the targeted files rather than the entire contents.

Once the important files, according to the ransom note, financial, client, business, technical, and personal files have been exfiltrated and encrypted, a ransom note - `Look at this instruction.txt` file pops up in each affected directory, notifying the users about the incident that happened in their system, channel to contact the attackers, ID generated by the attackers for the particular victim and information on the payout deadline which usually is 10 days.


Lister - [C:\Look at this instruction.txt]
File Edit Options Encoding Help
100 %

```
Your network systems were attacked and encrypted. Contact us in order to restore
your data. Don't make any changes in your file structure: touch no files, don't
try to recover by yourself, that may lead to it's complete loss.

To contact us you have to download "tox" messenger: https://qtox.github.io/

Add user with the following ID to get your instructions:
A4B3B0845DA242A64BF17E0DB4278EDF85855739667D3E2AE8B89D5439015F07E81D12D767FC

Alternative way: swikipedia@onionmail.org

Your ID: jFsmcdPh2S

You should know that we have been downloading data from your network for a
significant time before the attack: financial, client, business, post, technical
and personal files.
In 10 days - it will be posted at our site
http://bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad.onion with links
send to your clients, partners, competitors and news agencies, that will lead to
a negative impact on your company: potential financial, business and reputational
loses.
```

BianLian Threat Note - “Look at this instruction.txt“

Once the encryption is complete the ransomware deletes itself.

```
cmd /c del <sample_exe_name>
```

DETECTION USING LOGPOINT CONVERGED SIEM

With the right tools and adequate visibility, detecting and responding to threats becomes more manageable at any stage of the infection. Logpoint's Converged SIEM platform, with powerful query capabilities, offers organizations an effective solution to identify and respond to the BianLian ransomware threat. With Logpoint's user-friendly query language covering all aspects, from simple query search to advanced aggregated, correlated, or regex-based search; security analysts can create focused searches to pinpoint indicators of compromise and potential BianLian infections.

To aid analysts in monitoring BianLian's malicious activities within their network, we have developed a set of purpose-built queries tailored to this specific threat. By leveraging Logpoint's capabilities and utilizing these queries, organizations can bolster their defense against BianLian and proactively defend their networks.

Log Sources Needed

To ensure the effectiveness of the provided detection queries, it is important to have relevant logs from specific sources. While certain logs are automatically generated, others may require manual configuration. By ensuring that logs from critical systems, network devices, and security solutions are properly configured and collected, organizations can gather the necessary data to support the execution of the detection queries. The following log sources are vital for effective detection:

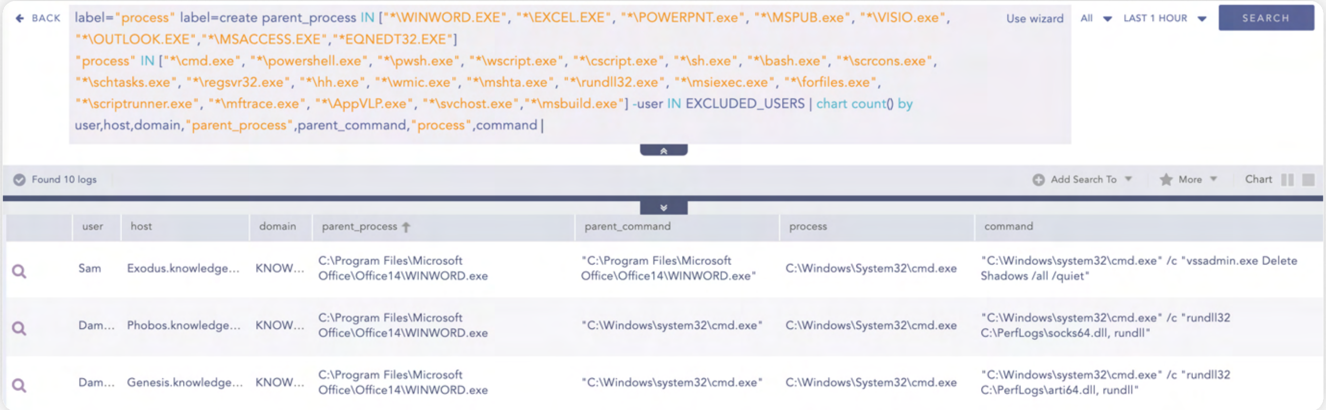
1. **Windows**
    - Process Creation with Command Line Auditing explicitly **enabled**
    - PowerShell Script Block Logging explicitly **enabled**
    - Registry Auditing explicitly **enabled**
2. **Windows Sysmon**
3. **Firewall**
4. **IDS/IPS**

Initial Access

1. Microsoft Office Product Spawning Windows Shell

A very common method among the BianLian threat actors - spearphishing, is still the most adopted technique to exploit the human element and infiltrate the target system. Therefore, we can be on the lookout for “Microsoft Office Product Spawning Windows Shell“

```
label="Process" label=Create
parent_process IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.exe", "*\MSPUB.exe",
"*\VISIO.exe", "*\OUTLOOK.EXE","*\MSACCESS.EXE","*EQNEDT32.EXE", "*\Onenote.exe"]
"process" IN ["*\cmd.exe", "*\powershell.exe", "*\pwsh.exe", "*\wscript.exe",
"*\cscript.exe", "*\sh.exe", "*\bash.exe", "*\scrcons.exe", "*\schtasks.exe",
"*\regsvr32.exe", "*\hh.exe", "*\wmic.exe", "*\mshta.exe", "*\rundll32.exe",
"*\msiexec.exe", "*\forfiles.exe", "*\scriptrunner.exe", "*\mftrace.exe", "*\AppVLP.exe",
"*\svchost.exe","*\msbuild.exe"]
```



```
label="process" label=create parent_process IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.exe", "*\MSPUB.exe", "*\VISIO.exe",
"*\OUTLOOK.EXE","*\MSACCESS.EXE","*EQNEDT32.EXE"]
"process" IN ["*\cmd.exe", "*\powershell.exe", "*\pwsh.exe", "*\wscript.exe", "*\cscript.exe", "*\sh.exe", "*\bash.exe", "*\scrcons.exe",
"*\schtasks.exe", "*\regsvr32.exe", "*\hh.exe", "*\wmic.exe", "*\mshta.exe", "*\rundll32.exe", "*\msiexec.exe", "*\forfiles.exe",
"*\scriptrunner.exe", "*\mftrace.exe", "*\AppVLP.exe", "*\svchost.exe","*\msbuild.exe"] -user IN EXCLUDED_USERS | chart count() by
user,host,domain,"parent_process",parent_command,"process",command |
```

Found 10 logs

user	host	domain	parent_process	parent_command	process	command
Sam	Exodus.knowledge...	KNOW...	C:\Program Files\Microsoft Office\Office14\WINWORD.exe	"C:\Program Files\Microsoft Office\Office14\WINWORD.exe"	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c "vssadmin.exe Delete Shadows /all /quiet"
Dam...	Phobos.knowledge...	KNOW...	C:\Program Files\Microsoft Office\Office14\WINWORD.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c "rundll32 C:\PerfLogs\socks64.dll, rundll"
Dam...	Genesis.knowledge...	KNOW...	C:\Program Files\Microsoft Office\Office14\WINWORD.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c "rundll32 C:\PerfLogs\arti64.dll, rundll"

2. Microsoft Exchange ProxyShell Vulnerability

We have also observed BianLian exploiting the Microsoft Exchange server's ProxyShell vulnerability for initial access into the system. Therefore, suspicious activities can be monitored through, "Exchange ProxyShell Pattern Detected"

```
norm_id=* ((url="*/autodiscover.json*" url IN ["*/powershell*", "*/mapi/nspi*", "*/EWS*", "*X-Rps-CAT*"]) OR
url IN ["*autodiscover.json?@*", "*autodiscover.json%3f@*", "*%3f@foo.com*", "*Email=autodiscover/autodiscover.json*", "*json?@foo.com*"])
```

and "Successful Exchange ProxyShell Attack"

```
norm_id=* (url="*/autodiscover.json*" url IN ["*/powershell*", "*/mapi/nspi*", "*/EWS*", "*X-Rps-CAT*"]
status_code IN [200, 301])
```

3. Remote Access Tool: Ngrok

In some instances, the threat actors have exploited the vulnerabilities to deploy a lightweight remote access solution such as `ngrok` as the follow-on payload in the target system. Such instances can be detected with, "Ngrok Execution"

```
label="Process" label=Create
(("process"="*\ngrok.exe" command IN ["* tcp *", "* http *", "* authtoken *"])
OR (command="* start *" command="*--all*" command="*.yml*" command="*--config*")
OR (command IN ["* tcp 139*", "* tcp 445*", "* tcp 3389*", "* tcp 5985*", "* tcp 5986*"]))
```

and "Ngrok RDP Tunnel Detected"

```
norm_id=WinServer
((event_source IN ["Microsoft-Windows-TerminalServices-LocalSessionManager", "Microsoft-Windows-TerminalServices-RemoteConnectionManager"]) OR (channel=Security event_id=4779))
(source_address="::%16777216" OR eventxml.address="::%16777216")
| rename eventxml.address as source_address
```

Our previous publication, "**Hunting and remediating ngrok tunnels using Logpoint**", offers security analysts with valuable resources to the ability to enhance their detection capabilities for Ngrok tunnels a step further.

Execution & Persistence

1. Scheduled Task Creation

Once into the system, like much other modern ransomware, BianLian too creates a scheduled task to gain persistence and execute the dropped malicious payload recursively with system privileges at a certain predetermined time and date across the infected environment. So, we can search for recently created un-authorized scheduled tasks with, “Scheduled Task Creation Detected”

```
(label="Process" label=Create "process"="*\schtasks.exe" command="* /create *" -user IN EXCLUDED_USERS)
OR (label="Registry" label="Key" label="Map"
"target_object"="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\*"
-target_object IN ["*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\UpdateOrchestrator*"]
event_type=CreateKey)
```

The query also tracks Symson registry events (Event ids 12, 13, 14) to detect any modifications in the registry.

2. Local User Creation & Addition in Privilege Group

Suspicious creation of local users has been identified as a common tactic employed by BianLian in their campaigns for persistence. New unauthorized users are created with elevated privileges i.e. once the user accounts are created they are then added to the local group - `Remote Desktop Users`.

Hunting for the creation and addition of unauthorized user accounts in the local group is crucial to detect and remove the persistence mechanism of the adversary, and can be done with, “Account Created for Persistence Detected“

```
label="Process" label=Create "process" IN ["*\net.exe","*\net1.exe"]
command="*net*" command="*user*" command="*/add*"
```

and “Account Manipulated for Persistence Detected“

```
label="Process" label=Create "process" IN ["*\net.exe","*\net1.exe"]
command="net*localgroup*/add*"
```

Defense Evasion

1. Windows Defender Bypass

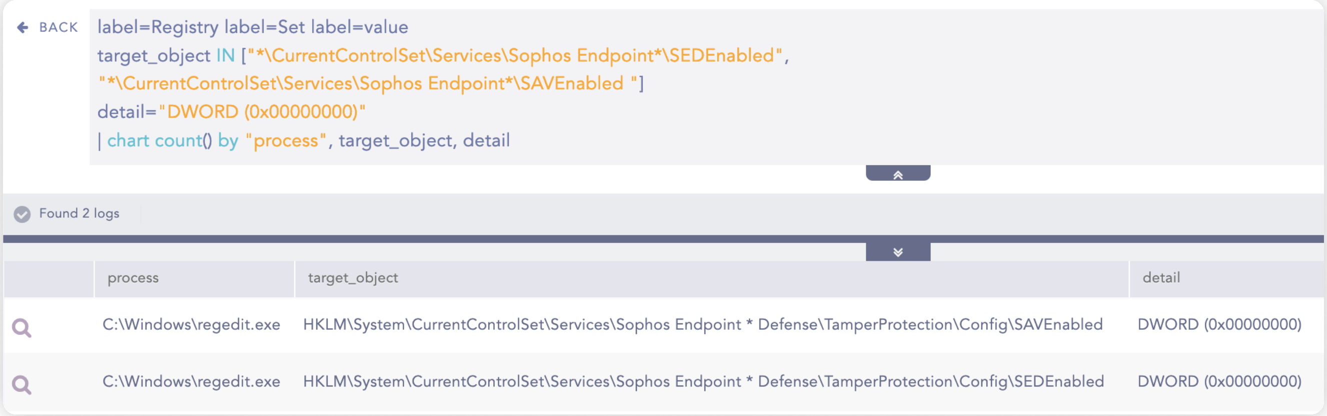
In an attempt to evade native defenses and maintain stealth for its future activities, BianLian threat actors begin to modify the registry values of Microsoft Windows Defender which could otherwise possibly detect its activities and trigger alerts. Hence, making the detection of such nasty acts our top priority with “Windows Defender Antivirus Disabled via Registry Modification”.

```
label="process" label="create" "process"="*\reg.exe"
command IN ["*SOFTWARE\Microsoft\Windows Defender\*",
"*SOFTWARE\Policies\Microsoft\Windows Defender Security Center*",
"*SOFTWARE\Policies\Microsoft\Windows Defender\*"]
((command = "*add*" command = "*d 0*"
command IN ["*DisallowExploitProtectionOverride*", "*EnableControlledFolderAccess*",
"*MpEnablePus*", "*PUAProtection*", "*SpynetReporting*", "*SubmitSamplesConsent*",
"*TamperProtection*"])
OR
(command = "*add*" command = "*d 1*"
command IN ["*DisableAntiSpyware*", "*DisableAntiSpywareRealtimeProtection*",
"*DisableAntiVirus*", "*DisableArchiveScanning*", "*DisableBehaviorMonitoring*",
"*DisableBlockAtFirstSeen*", "*DisableConfig*", "*DisableEnhancedNotifications*",
"*DisableIntrusionPreventionSystem*", "*DisableIOAVProtection*",
"*DisableOnAccessProtection*", "*DisablePrivacyMode*", "*DisableRealtimeMonitoring*",
"*DisableRoutinelyTakingAction*", "*DisableScanOnRealtimeEnable*",
"*DisableScriptScanning*",
"*Notification_Suppress*", "*SignatureDisableUpdateOnStartupWithoutEngine*"]))
```

2. Registry Modification to Disable Sophos EPP Services

Further, they move on to make changes in the registry value of Sophos Endpoint Protection to disable tamper protection services and finally remove the EPP from the system. This can be detected with “Sophos EPP Registry Modification“,

```
label=Registry label=Set label=value
target_object IN ["*\CurrentControlSet\Services\Sophos Endpoint*\SEDEnabled",
"*\CurrentControlSet\Services\Sophos Endpoint*\SAVEnabled "]
detail="DWORD (0x00000000)"
```



```
label=Registry label=Set label=value
target_object IN ["*\CurrentControlSet\Services\Sophos Endpoint*\SEDEnabled",
"*\CurrentControlSet\Services\Sophos Endpoint*\SAVEnabled "]
detail="DWORD (0x00000000)"
| chart count() by "process", target_object, detail
```

Found 2 logs

	process	target_object	detail
	C:\Windows\regedit.exe	HKLM\System\CurrentControlSet\Services\Sophos Endpoint * Defense\TamperProtection\Config\SAVEnabled	DWORD (0x00000000)
	C:\Windows\regedit.exe	HKLM\System\CurrentControlSet\Services\Sophos Endpoint * Defense\TamperProtection\Config\SEDEnabled	DWORD (0x00000000)

3. RDP Registry Modification

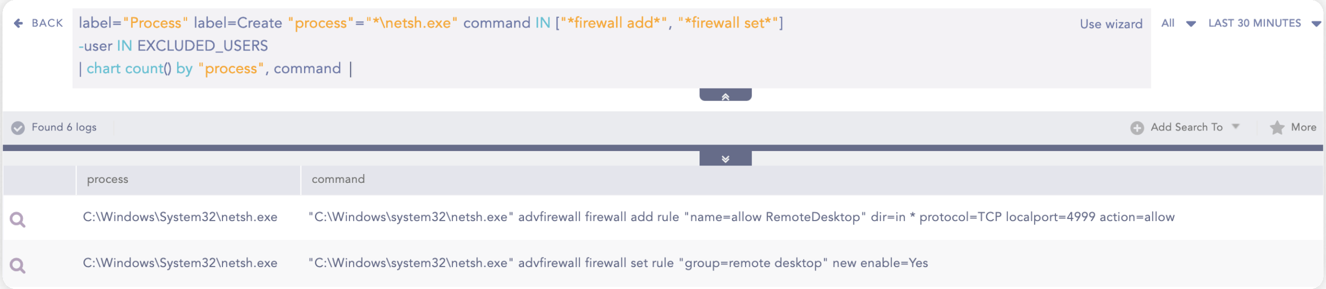
RDP being their major mode of action, the threat actors modify the registry values to disable user authentication for RDP connections and enable a user to receive help from Remote Assistance, so that, they can exploit the process for their use. Hence, such modifications need to be actively monitored with “RDP Registry Modification“.

```
label=Registry label=Value label=Set
target_object IN ["*\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication",
"*\CurrentControlSet\Control\Terminal Server\fDenyTSConnections"]
detail="DWORD (0x00000000)" -user IN EXCLUDED_USERS
```

4. Firewall Rule Addition

They achieve a level of smooth RDP connections by introducing new firewall rules in the system meant to permit any or all kinds of RDP traffic to and from the system. This kind of addition to firewall rules can be detected with “Firewall Rule Addition via Netsh Detected“

```
label="Process" label=Create "process"="*\netsh.exe"
command IN ["*firewall add*", "*firewall set*"]
-user IN EXCLUDED_USERS
| chart count() by "process", command
```



```
label="Process" label=Create "process"="*\netsh.exe" command IN ["*firewall add*", "*firewall set*"]
-user IN EXCLUDED_USERS
| chart count() by "process", command |
```

Found 6 logs

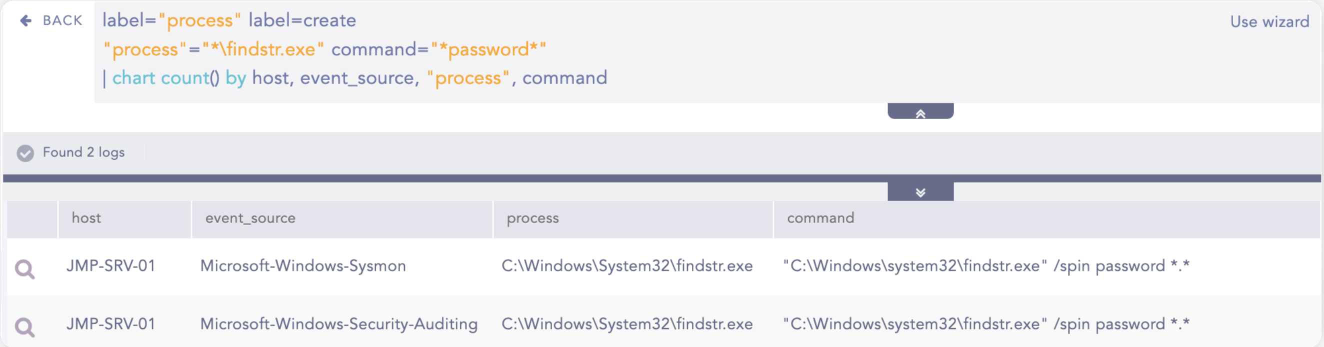
process	command
C:\Windows\System32\netsh.exe	"C:\Windows\system32\netsh.exe" advfirewall firewall add rule "name=allow RemoteDesktop" dir=in * protocol=TCP localport=4999 action=allow
C:\Windows\System32\netsh.exe	"C:\Windows\system32\netsh.exe" advfirewall firewall set rule "group=remote desktop" new enable=Yes

Credential Access

1. Active Search for Password Files

The BianLian ransomware group has been found to extensively exploit legitimate credentials obtained through scanning target systems for unsecured credentials through the findstr.exe system binary. These actions can be detected by the following query,

```
label="process" label=create
"process"="*\findstr.exe" command="*password*"
```



```
label="process" label=create
"process"="*\findstr.exe" command="*password*"
| chart count() by host, event_source, "process", command
```

Found 2 logs

host	event_source	process	command
JMP-SRV-01	Microsoft-Windows-Sysmon	C:\Windows\System32\findstr.exe	"C:\Windows\system32\findstr.exe" /spin password *.*
JMP-SRV-01	Microsoft-Windows-Security-Auditing	C:\Windows\System32\findstr.exe	"C:\Windows\system32\findstr.exe" /spin password *.*

2. Credential Harvest

Further, the cyber threat group has been observed using the `MiniDump` export function from `comsvcs.dll`, executed via `rundll32`, to perform a memory dump from lsass. The activity of invoking comsvcs.dll through rundll32 can be detected through the process creation even with the query,

```
label="process" label=create
("process"="*\rundll32.exe" command="*comsvcs*" command="*full*"
command IN ["*24 *", "*#24*", "*#+24*", "*MiniDump*"])
OR (command="*#-4294967272*")
```

They were also found using `ntdsutil.exe` to extract data from the NTDS.dit. Such events can be detected by this query given below:

```
label="process" label=create
"process"="*\ntdsutil.exe" command="*ntds*"
```

Discovery

1. Discovery Activity with Nltest

The BianLian threat actors have time and again made use of Windows native tools to perform discovery activities and have been found to use `nltest` to enumerate target domains. It can be detected with “Reconnaissance Activity with Nltest“

```
label="Process" label=Create"process"="*\nltest.exe" file="nltestrk.exe"
((command ="*/server*" command="*/query*")  OR command IN
["*/dclist:*","*/domain_trusts*","*/trusted_domains*","*/user*","*/parentdomain*"])
```

2. Account Discovery Activity

Further, `net.exe` and `net1.exe` Windows native binaries were used to discover additional information on the accounts present in the system. The following query allows for the detection of such activities:

```
label="Process" label=Create ("process" IN ["*\net.exe","*\net1.exe"] command IN
["*net*user*","*net*group*","*get*group*","*get*ADPrinicipalGroupMembership*"])
```

Lateral Movement

1. Execution of PSExec

The BianLian ransomware group along with others is seen to be using `PSExec` for the execution of ransomware. PSExec is a lightweight telnet replacement. It is a part of Windows Sysinternals offering leverage for adversaries to execute malicious payloads through it. Defenders should actively search for the malicious execution of PSExec.

```
norm_id="WinServer" event_id=5145 share_name="IPC$"
relative_target IN ["*-stdin", "*-stdout", "*-stderr"]
-relative_target="PSEXESVC*" -user IN EXCLUDED_USERS
```

Since Wmic is also used for a similar purpose, analysts should also carefully monitor the child processes spawned by `wmic.exe`,

```
label="Create" label="Process" parent_image="*\wmic.exe"
-"process" IN ["C:\Windows\System32\conhost.exe", "C:\Windows\system32\wbem\WMIC.exe",
"C:\Windows\syswow64\wbem\WMIC.exe", "C:\Windows\system32\WerFault.exe",
"C:\Windows\SysWOW64\WerFault.exe"]
```

including proxy execution of malicious payloads via wmic.exe,

```
label="Process" label="Create"  command="*process*" command="*call*"
command="*create*" command IN ["*rundll32*","*bitsadmin*","*regsvr32*",
"*cmd.exe /c *","*cmd.exe /k *","*cmd.exe /r *","*cmd /c *","*cmd /k *",
"*cmd /r *", "*powershell*","*pwsh*","*certutil*","*cscript*","*wscript*",
"*mshta*","*\Users\Public\*", "*\Windows\Temp\*", "*\AppData\Local\*","*%temp%*",
"*%tmp%*","*%ProgramData%*","*%appdata%*","*%comspec%*","*%localappdata%"]
```

Analysts can also refer to our publication - “**Hunting for PsExec artifacts in your Enterprise**“, for comprehensive insights and techniques to effectively identify and address PsExec artifacts within their network environment.

2. Netlogon Vulnerability Exploit

The forensic artifact named `exp.exe`, deployed on the target system by the BiabnLian threat actors was discovered by the FBI and is believed to be an exploitation tool that takes advantage of the **Netlogon vulnerability** (**CVE-2020-1472**) and establishes a connection with a domain controller. The presence of the file/artifact in the system can be detected through its hash,

```
hash = "0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500" OR
hash_sha256 = "0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500"
```

Event ID 5829 is generated when a vulnerable Netlogon secure channel connection is allowed during an initial deployment phase. This can be monitored with,

```
norm_id=WinServer event_id=5829
```

Furthermore, admins can monitor event IDs 5827 and 5828, triggered when vulnerable Netlogon connections are denied, and event IDs 5830 and 5831, triggered when vulnerable Netlogon connections are allowed by the patched domain controllers via Group Policy.

Collection

Another artifact, `system.exe` discovered by the FBI on the target system offers registry enumeration capabilities to the BianLian ransomware group. It too can be detected by looking out for its hash in the system,

```
hash = "40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce" OR
hash_sha256 = "40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce"
```

Command & Control

Besides, remote management and access software, `def.exe` - a backdoor custom-built for each target has been found in the victim's systems to ensure long-term access to the compromised systems, enabling them to exert control, monitor activities, and execute commands as required. Such backdoors can be monitored through their hash in the system,

```
hash = "7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893" OR
hash_sha256 = "7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893"
```

Exfiltration

Once the actors are sure of having no obstruction, they begin exfiltrating important organizational data. We found the BianLian actors to exfiltrate data to cloud storage services like Mega, Anonfiles, and more. This can be detected with,

```
query IN ['*ufile.io*', '*userstorage.mega.co.nz*', '*.anonfiles.com*',
'*sendspace.com']
OR domain IN ['*ufile.io*', '*userstorage.mega.co.nz*', '*.anonfiles.com*',
'*sendspace.com']
```

Impact

Before the release of the decryptor, the BianLian resorted to encryption as the final act of the show, encrypting all the important files in the target system for their double extortion strategy. The execution of the encryptor file - `encryptor.exe` used for the purpose, can be monitored by scanning for the presence of its hash in the system,

```
hash = "1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43" OR
hash_sha256 = "1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43"
```

Once the process is complete, the malware deletes itself from the system. Therefore, early detection is a key factor in preventing damage to your organization.

INVESTIGATION AND RESPONSE USING LOGPOINT CONVERGED SIEM

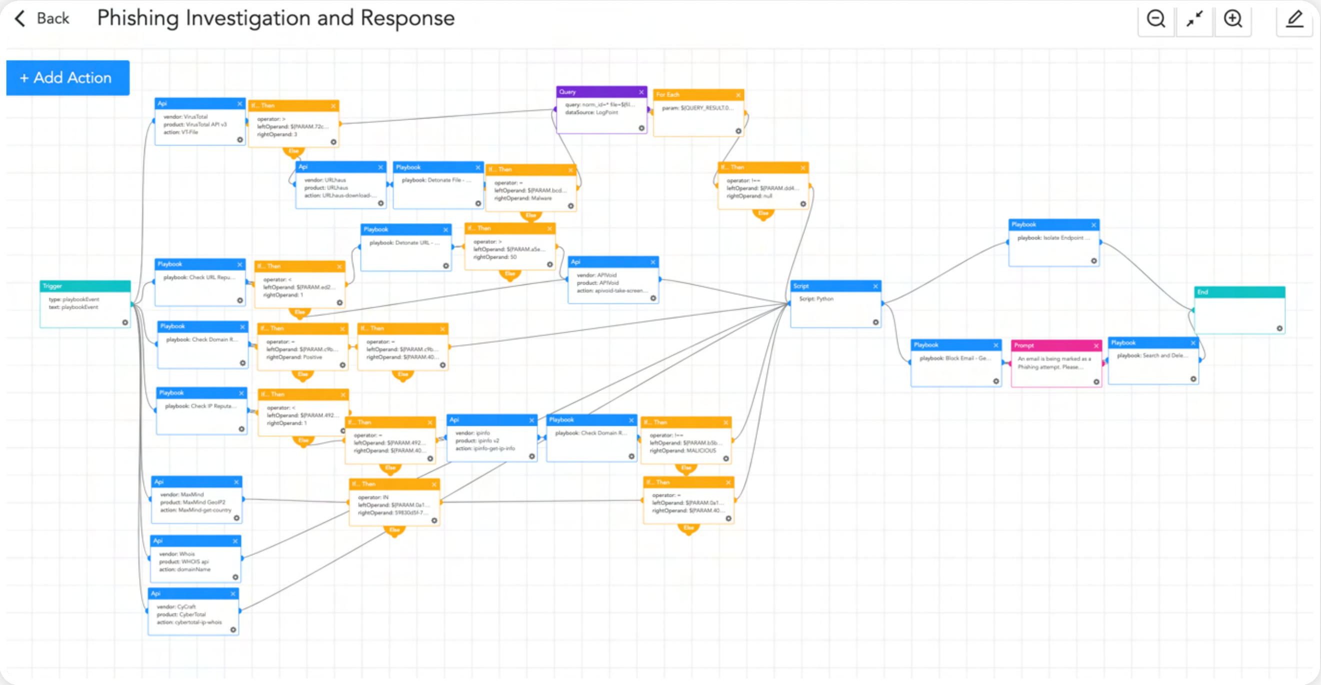
Logpoint Converged SIEM can be the weapon in your arsenal to automate detection, investigation, and response against intrusions and attacks such as the BianLian ransomware attack, and disrupt its cyber-kill chain. With an integrated security platform that encompasses SIEM (Security Information and EventManagement), SOAR (Security Orchestration, Automation, and Response), and AgentX for EDR (Endpoint Detection and Response) capabilities, organizations can greatly enhance their ability to detect and respond to threats posed by malware like BianLian ransomware.

- **Logpoint SIEM** collects, analyzes, and correlates log data from various sources, including endpoints and cloud services. Through real-time monitoring and the detection of suspicious activities and anomalous behavior patterns, SIEM enables early identification of potential BianLian infections.
- The inclusion of **SOAR** strengthens the organization's defense mechanisms by automating response actions, such as isolating affected endpoints and blocking malicious IP addresses. This streamlines the incident response process and minimizes the potential impact of BianLian's activities.
- Additionally, **AgentX** in combination with SIEM and SOAR, provides EDR capabilities to Converged SIEM, which gives detailed visibility into endpoint activities, enabling advanced threat hunting and forensic investigations with Osquery. By continuously monitoring endpoints for indicators of compromise and malicious behaviors associated with BianLian's infection chain, AgentX enables prompt identification and containment of compromised systems

Logpoint provides a wide range of useful playbooks (via SOAR) that are designed to streamline and automate various security operations and incident response tasks. These playbooks cover a broad spectrum of security use cases, including threat detection and response, compliance management, log analysis, incident handling, and more. They leverage the capabilities of Logpoint's SIEM, SOAR, and EDR (AgentX), enabling seamless integration and orchestration of security processes. Some of the useful playbooks relevant to hunting BianLian ransomware offered by Logpoint are elaborated on in the following section.

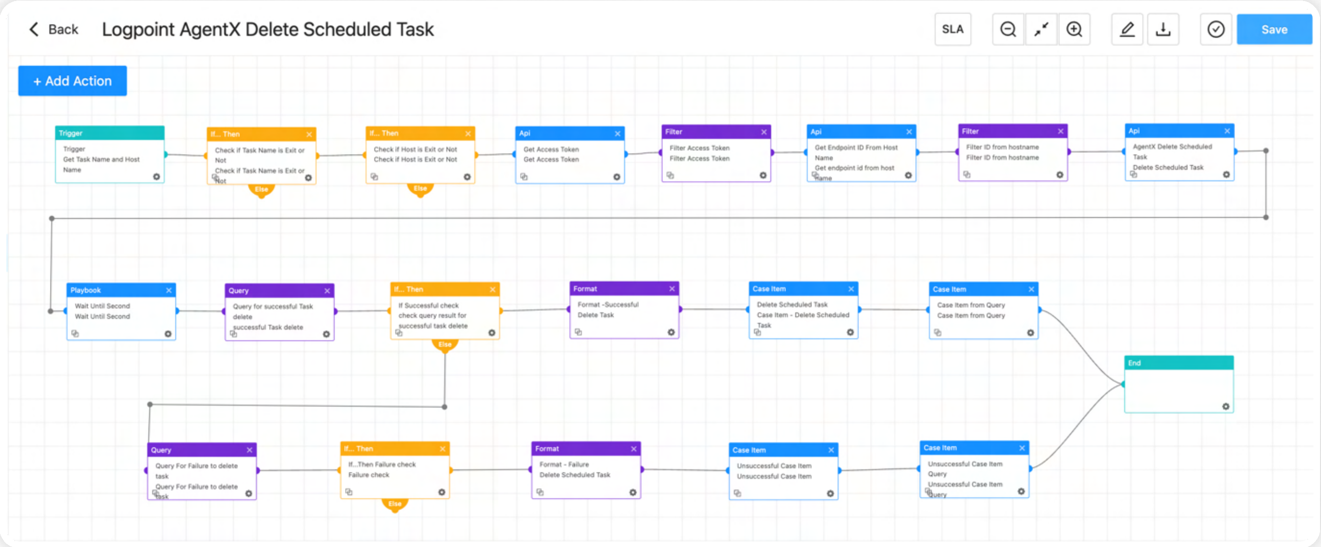
1. Phishing Investigation and Response

Social engineering, particularly phishing, is a prevalent and widely-used method for initiating cyber attacks. Phishing, even in the case of BianLian, serves as a primary technique employed by threat actors to gain initial access to the victims' machines. It is crucial to promptly detect such phishing **emails** and take necessary actions to limit or prevent potential damage. The “Phishing Investigation and Response” playbook guides investigating and remedying such phishing incidents.



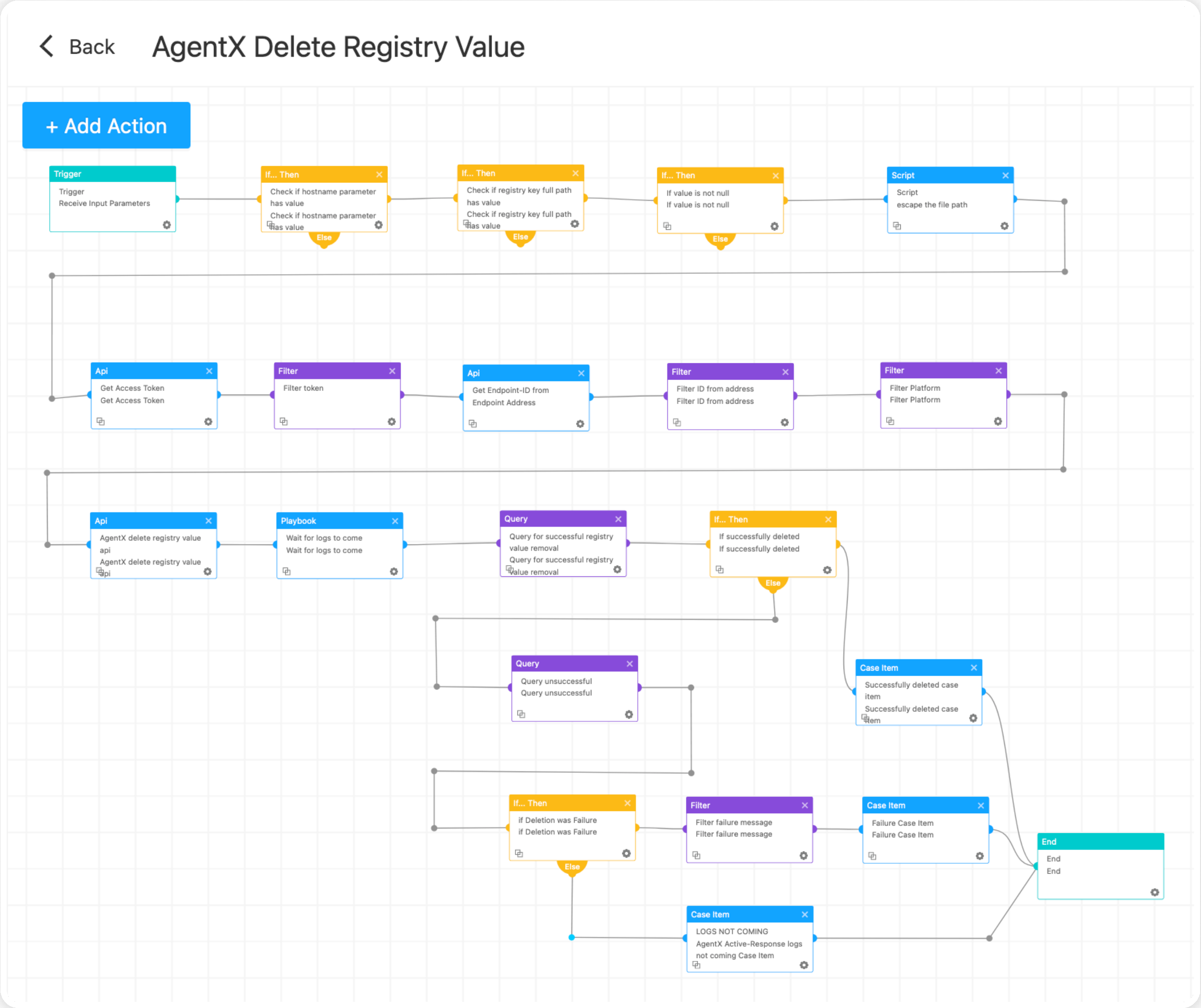
2. Logpoint AgentX Delete Scheduled Task

Ransomware like BianLian, often create scheduled tasks to maintain persistence and ensure the continuation of its malicious activities. These scheduled tasks serve as a means for the ransomware to execute at specific intervals or trigger specific events, allowing it to spread across the network, encrypt files or download additional malicious payloads. By employing the “Logpoint AgentX Delete Scheduled Task“ playbook designed to identify and delete such scheduled tasks, organizations can disrupt the ransomware's operations and minimize the potential damage inflicted upon their systems and data.



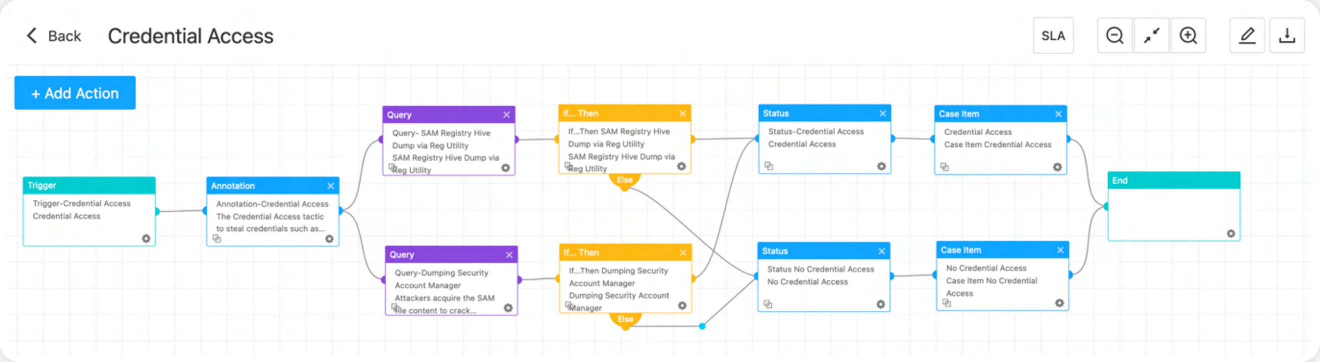
3. AgentX Delete Registry Value

Further, as part of their infection chain, BianLian often adds or modifies registry values to achieve persistence and maintain control over compromised systems. By manipulating the Windows Registry, ransomware like BianLian ensures its malicious processes run automatically upon system startup and enable the ransomware to evade detection and continue its destructive activities. With the help of the “AgentX Delete Registry Value“ playbook organizations can detect and delete such registry entries.



4. Credential Access

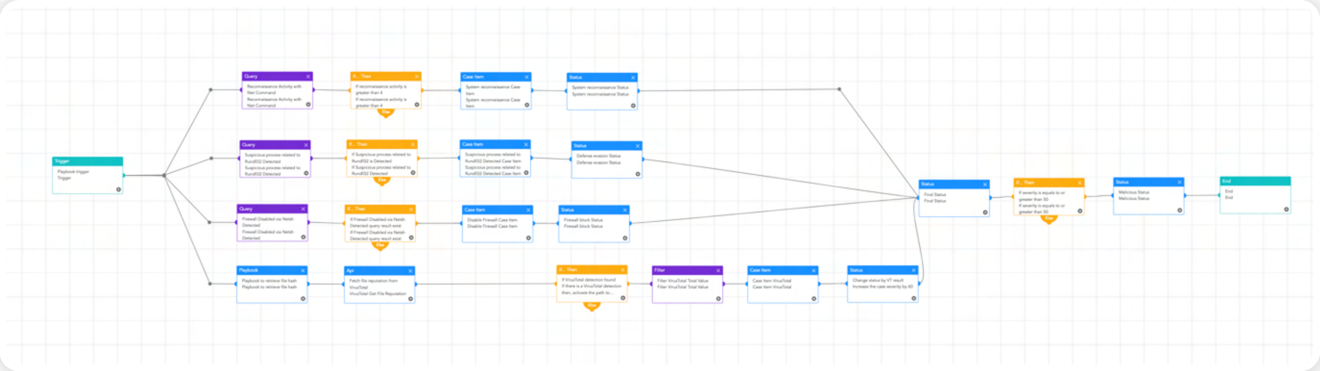
In contemporary cyber attacks, the acquisition of credentials is a common tactic employed by threat actors to escalate their privileges within a network or move laterally across systems. To proactively address this threat, security teams can utilize the "Credential Access" playbook. This playbook is designed to investigate any suspicious activity related to credential access thoroughly. By leveraging advanced detection techniques and analysis methods, security analysts can swiftly identify and respond to potential credential compromise incidents.



Back
Credential Access
SLA
+ Add Action
Trigger
Trigger-Credential Access
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
Status
Status-Credential Access
Credential Access
Case Item
Credential Access
Case Item Credential Access
End
Query
Query-Dumping Security Account Manager
Attackers acquire the SAM file content to crack...
If... Then
If...Then Dumping Security Account Manager
Dumping Security Account Manager
Else
Status
Status No Credential Access
No Credential Access
Case Item
No Credential Access
Case Item No Credential Access

5. Malicious File Investigation and Containment

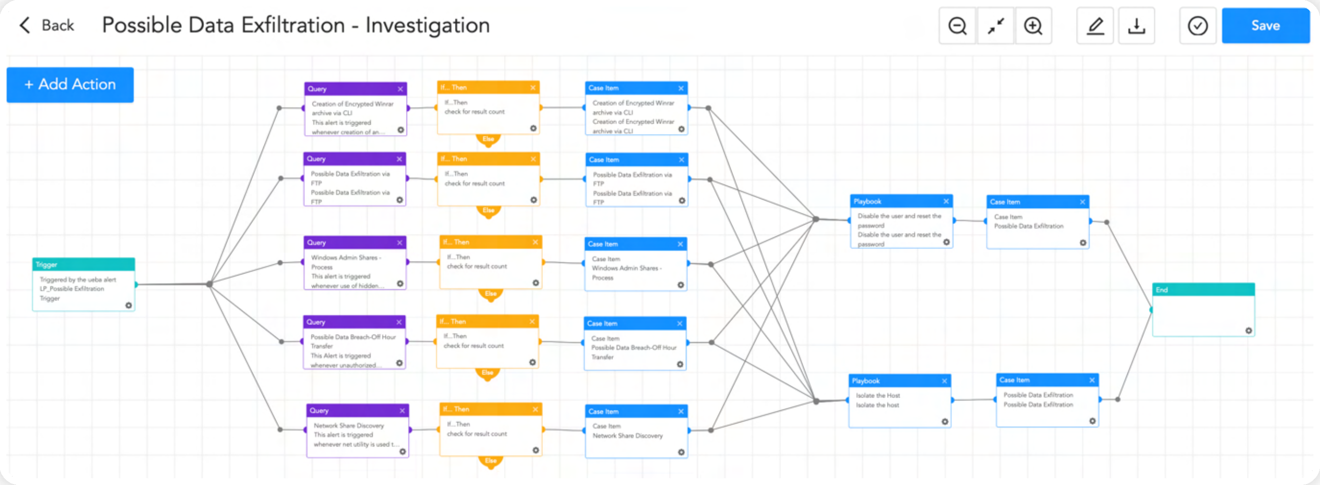
BianLian ransomware group has deployed multiple executables during the process of infection from netlogon vulnerability exploiters to registry enumerators and custom-built backdoors. Such files/executables can be investigated and contained with the “Malicious File Investigation and Containment“ playbook.



Trigger
Playbook trigger
Trigger
Query
Reconnaissance Activity with Net Command
Reconnaissance Activity with Net Command
If... Then
If reconnaissance activity is greater than 4
If reconnaissance activity is greater than 4
Else
Case Item
System reconnaissance Case Item
System reconnaissance Case Item
Status
System reconnaissance Status
System reconnaissance Status
Query
Suspicious process related to Rundll32 Detected
Suspicious process related to Rundll32 Detected
If... Then
If Suspicious process related to Rundll32 is Detected
If Suspicious process related to Rundll32 Detected
Else
Case Item
Suspicious process related to Rundll32 Detected Case Item
Suspicious process related to Rundll32 Detected Case Item
Status
Defense evasion Status
Defense evasion Status
Query
Firewall Disabled via Netsh Detected
Firewall Disabled via Netsh Detected
If... Then
If Firewall Disabled via Netsh Detected query result exist
If Firewall Disabled via Netsh Detected query result exist
Else
Case Item
Disable Firewall Case Item
Disable Firewall Case Item
Status
Firewall block Status
Firewall block Status
Playbook
Playbook to retrieve file hash
Playbook to retrieve file hash
Api
Fetch file reputation from VirusTotal
VirusTotal Get File Reputation
If... Then
If VirusTotal detection found
If there is a VirusTotal detection then, activate the path to...
Else
Filter
Filter VirusTotal Total Value
Filter VirusTotal Total Value
Case Item
Case Item VirusTotal
Case Item VirusTotal
Status
Change status by VT result
Increase the case severity by 60
Status
Final Status
Final Status
If... Then
If severity is equals to or greater than 50
If severity is equals to or greater than 50
Else
Status
Malicious Status
Malicious Status
End
End
End

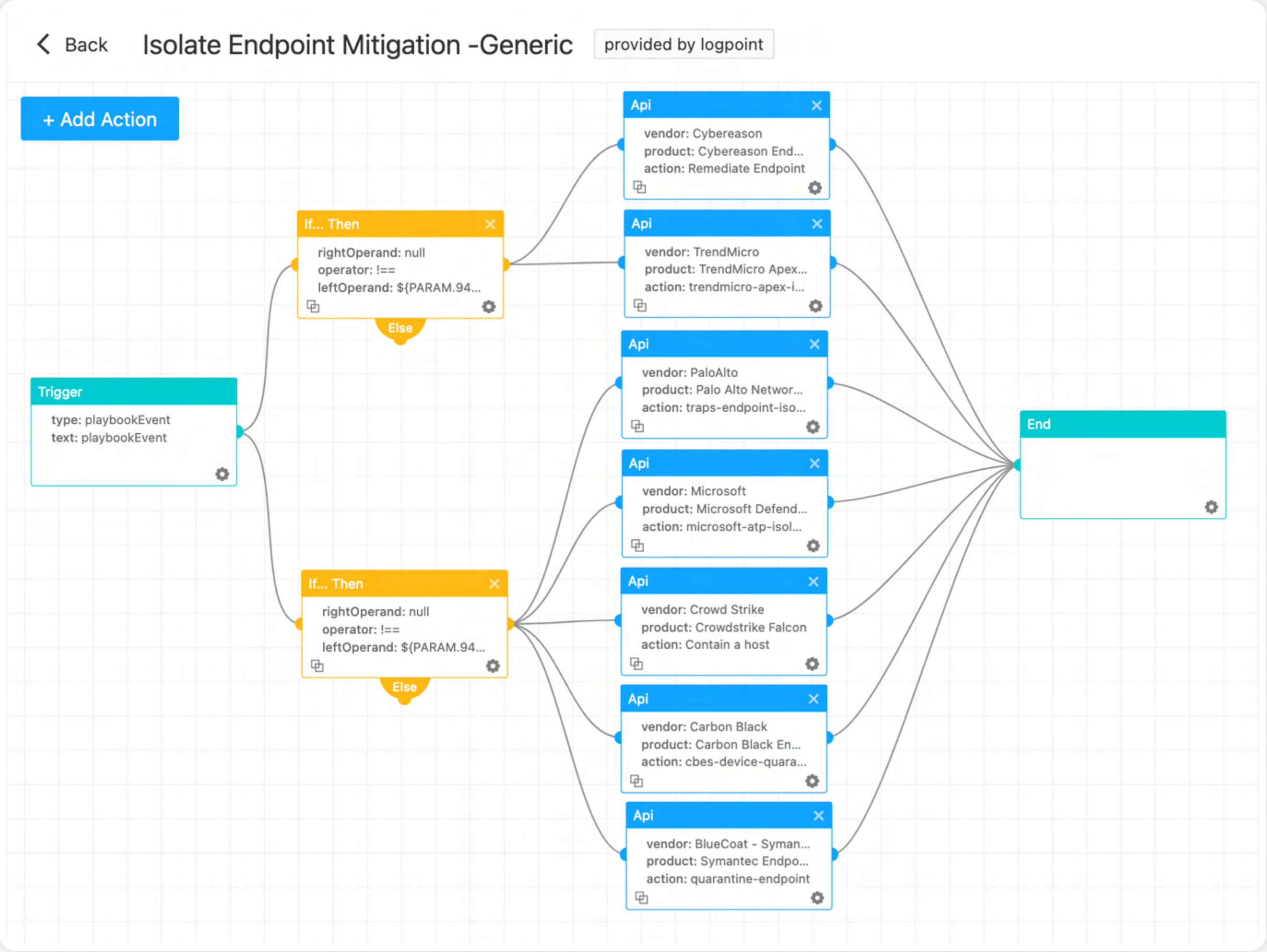
6. Possible Data Exfiltration

In contemporary cyber attacks, the acquisition of credentials is a common tactic employed by threat actors to escalate their privileges within a network or move laterally across systems. To proactively address this threat, security teams can utilize the "Credential Access" playbook. This playbook is designed to investigate any suspicious activity related to credential access thoroughly. By leveraging advanced detection techniques and analysis methods, security analysts can swiftly identify and respond to potential credential compromise incidents.


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...
Query
Possible Data Exfiltration via FTP Possible Data Exfiltration via FTP
Query
Windows Admin Shares - Process This alert is triggered whenever use of hidden...
Query
Possible Data Breach-Off Hour Transfer This Alert is triggered whenever unauthorized...
Query
Network Share Discovery This alert is triggered whenever net utility is used t...
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

7. Malicious File Investigation and Containment

In cases of suspicion of a compromised machine engaging in suspicious activities such as establishing continuous connections with a BianLian command-and-control (C&C) server or exfiltrating data, security analysts are encouraged to take proactive measures by isolating the affected host from the network. The "Isolate Endpoint Mitigation - Genric" playbook identifies the infected host and isolates it using the new Logpoint AgentX and also contains and quarantines it before it spreads to other machines.



Trigger
type: playbookEvent
text: playbookEvent

If... Then
rightOperand: null
operator: !==
leftOperand: ${PARAM.94...
Else

If... Then
rightOperand: null
operator: !==
leftOperand: ${PARAM.94...
Else

Api
vendor: Cybereason
product: Cybereason End...
action: Remediate Endpoint

Api
vendor: TrendMicro
product: TrendMicro Apex...
action: trendmicro-apex-i...

Api
vendor: PaloAlto
product: Palo Alto Networ...
action: traps-endpoint-iso...

Api
vendor: Microsoft
product: Microsoft Defend...
action: microsoft-atp-isol...

Api
vendor: Crowd Strike
product: Crowdstrike Falcon
action: Contain a host

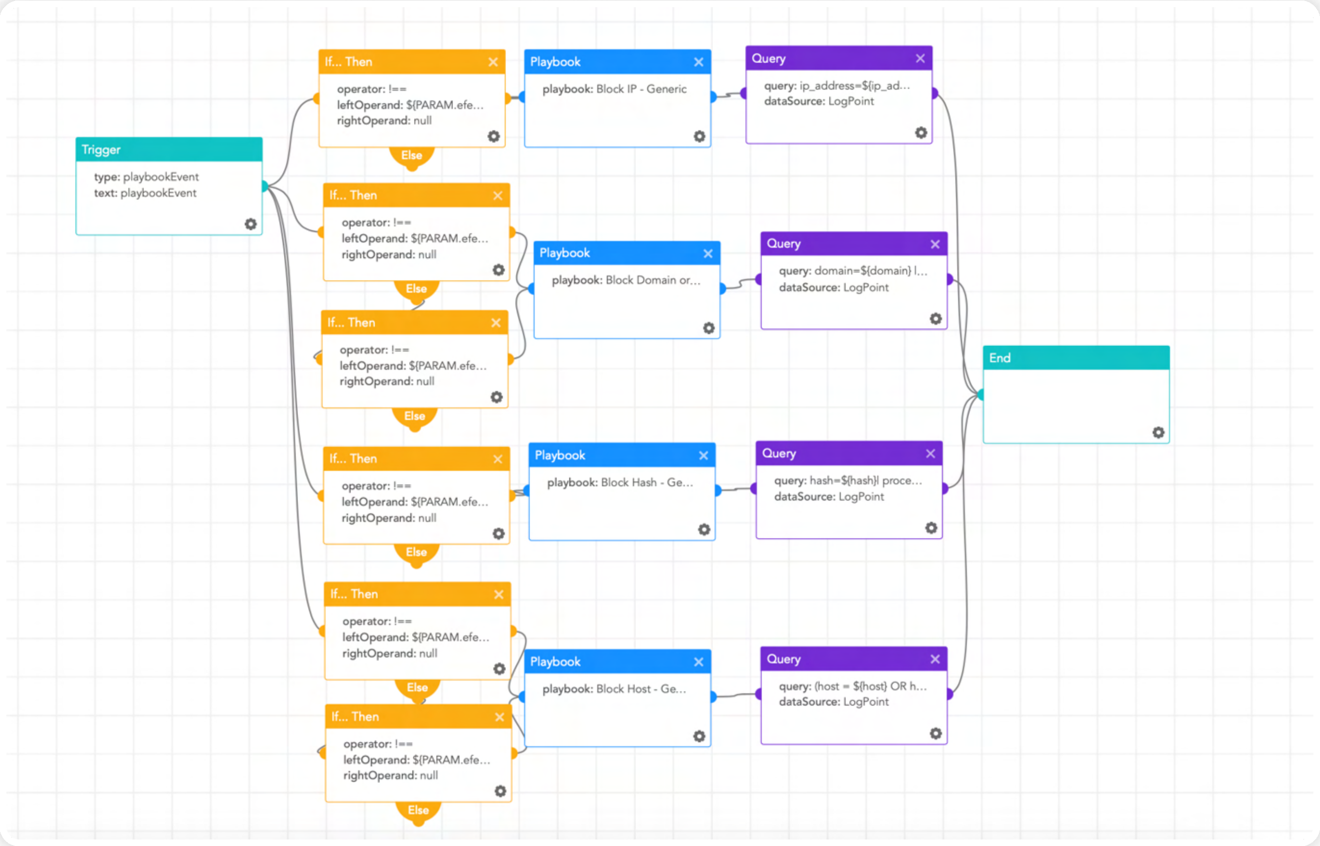
Api
vendor: Carbon Black
product: Carbon Black En...
action: cbes-device-quara...

Api
vendor: BlueCoat - Syman...
product: Symantec Endpo...
action: quarantine-endpoint

End

8. Block Indicators

Analysts can stay reassured by actively using the “Block Indicators“ playbook, to check if any IP, domain, URL, or host exists in a list of IoCs, block them, and add them to the blocked list for future detections.



RECOMMENDATION

1. **Secure and limit connections from external sources,**
   - Strictly limit the use of RDP and other remote desktop services.
   - Ensure all the traffic passes through a properly configured firewall.
   - Follow a "deny all connections by default" approach, allowing only explicitly required connections for specific system functionality.
   - Limit the number of open ports and services running on the server to minimize the attack surface.
   - Implement VPN access for remote administration and ensure it is properly configured with strong encryption and authentication methods.
2. **Extensively implement network segmentation** to prevent the spread, especially to domain controllers, and limit the impact.
3. **Disable command-line and scripting activities and permission**s preventing unauthorized exploitation of these powerful tools and reducing the attack surface.
   - Restrict the usage of PowerShell through Group Policy and grant permissions only to specific users on a case-by-case basis ensuring its usage only by authorized users.
4. **Implement application controls** to manage and control the execution of software, preventing installation and execution of portable versions of unauthorized remote access and other software.
5. **Password Policy & Hygiene**
   - Develop and extensively implement an organization-wide password policy that defines
     - immediate requirements to change the default password,
     - a globally accepted minimum password length and password expiry period,
     - the complexity involved, and more.
   - Refrain from storing passwords in plaintext formats.
6. **Strongly enforce MFA and phishing protection** for both user and administrative accounts. Adopt the practice of least privilege and time-based access, where possible.
7. **Immediately change credentials** from a non-compromised system, avoiding any similarities to previous passwords to ward off brute-force attacks.
8. **Regularly scan and assess organizational assets** for vulnerabilities and misconfigurations to patch them, and maintain updated Operating Systems, firmware, and applications.
9. **Regularly review the security posture of third-party vendors** interconnected with the organization.
10. **Develop the practice of regularly creating and maintaining offline encrypted backups** that encompass the entire organizational data infrastructure, and assure their availability through periodic restoration attempts.

11. **Conduct simulated attack scenarios** to make sure that the employees are well aware of phishing and other risks, and also to make sure that they report the incident to the internal cybersecurity team.
12. **Deploy AgentX**, to secure endpoint devices and ensure they are up-to-date, properly configured, and trigger alerts when disabled.
13. **Continuously monitor critical organizational assets** with a combination of tools such as Sysmon and **the Logpoint Converged SIEM platform**.

CONCLUSION

The BianLian ransomware continues to evolve as a formidable threat to organizations. Notably, the recent transformation i.e. the transition from a double extortion approach to pure extortion, with an intensified focus on encryption-less extortion. The changing tactics employed by the BianLian ransomware group underscore the dynamic nature of the cyber threat landscape. Organizations must, therefore, remain vigilant and adapt their security measures accordingly to effectively mitigate the risks associated with this evolving threat.

Understanding the infection chain of BianLian is crucial in developing effective defense strategies to mitigate the risk of compromise. With this report, we wish to provide our customers and readers with valuable insights into the detection and prevention measures for the BianLian ransomware infection. By leveraging converged SIEM solutions like Logpoint, organizations can proactively detect and respond to suspicious activities associated with such ransomware.

With the increasing prevalence of pure extortion and encryption-less tactics, organizations must prioritize robust security measures. By leveraging advanced detection techniques, fortifying defenses, and staying updated on emerging threats, organizations can effectively safeguard their systems and data from the ever-evolving tactics of the BianLian ransomware group.

REFERENCES

#StopRansomware: BianLian Ransomware Group | CISA

FBI confirms BianLian ransomware switch to extortion only attacks

Decrypted: BianLian Ransomware - Avast Threat Labs

Analysis 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b.exe (MD5: 36171704CDE087F839B10C2465D864E1) Malicious activity - Interactive analysis ANY.RUN

BianLian: New Ransomware variant on the rise

BianLian Ransomware Evolves into Pure Data Exfiltration-Focused Group | Cyware Hacker News

RansomGroups

BianLian Ransomware Gang Gives It a Go!

Q1 2023 Threat Landscape Ransomware Groups Splinter Swarm Professional Services Sector

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**