LOGPOINT

EMERGING THREATS PROTECTION REPORT

Deciphering Akira's Arsenal: Tactics for Uncovering and Responding

www.logpoint.com

FOREWORD

This Akira Ransomware has shown to be not only incredibly active but also remarkably adaptive since its beginning in March 2023. Initially, it targeted just Windows systems, but successive efforts have revealed a disturbing trend: the purposeful targeting of Linux servers. Furthermore, Megazord, a new and different strain of ransomware, has appeared, employing the Akira Infrastructure. Notably, Megazord's coding differs greatly from those of its predecessors, heralding the start of a new age in cyber warfare.

Swachchhanda Shrawan Poudel

Logpoint Security Research

Swachchhanda Shrawan Poudel is a cybersecurity enthusiast with a bachelor's degree in cybersecurity and certification as an ethical hacker. With an interest in both offensive and defensive security, he currently works as a Security Researcher at Logpoint, focusing on detection engineering, threat hunting, and remediation.

TABLE OF CONTENTS

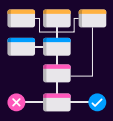
ABOUT LOGPOINT EMERGING THREATS PROTECTION

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**, as well as through the **Logpoint Help Center.** Customized investigation and response playbooks are available to all Logpoint Emerging Threats Protection customers.

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



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

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

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

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

Akira ransomware is sophisticated malicious software designed to encrypt files on a victim's system, delete shadow copies, and provide instructions for ransom payment and data recovery. It employs encryption algorithms, exclusion criteria, and a TOR-based communication system to carry out its malicious operations.

INFECTION CHAIN

Akira Group reportedly exploits CVE-2023-20269, which exists in the remote access VPN capability of Cisco ASA and FTD and may be abused remotely, without authentication, through brute force assaults.

After gaining access to the victim's machines, they first steal the victim's private data and encrypt them using their own custom-built payloads. They also employ double extortion tactics where they threaten to leak victims' data in their leakage site hosted on the dark web if the ransom is not paid.

They have also been observed using tools like AnyDesk, WinRAR, RustDesk, and PCHunter during their intrusions. These tools are often present in the victim's environment, and their misuse generally goes undetected.

TECHNICAL ANALYSIS OF MALWARE SAMPLE

Akira Ransomware has employed several malware samples during their campaigns since their initiation in March 2023. In this chapter, we will dig down some of the samples to understand and uncover their technical capability and features.

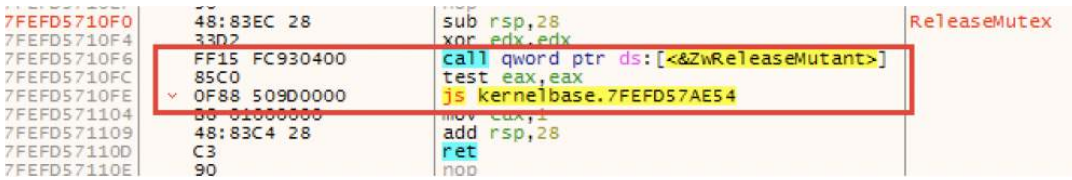
SAMPLE 1

Particulars	Value
Name	6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360.exe
Size	576KB
MD5	0885b3153e61caa56117770247be0444
SHA1	41d001e2974c9762249b93496b96250211f6e0f
SHA256	6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
SHA512	972bdace149a735de2def7019969bf602cdfd8b5cc2903ad07d6bb681342b07e78759ffaf50dc1525d68dac4aafa0c278e3ddff78e226746816e164ec0d5adb5
File Type	Win64 Executable

When executed, this sample initiates a series of steps to encrypt the victim's files and ensure that recovery is nearly impossible. Here is a breakdown of its malicious operations in chronological order:

1. Task Configuration

The ransomware begins by creating a mutex, which serves as a control mechanism for configuring various tasks. These tasks involve defining the encryption path (the location of files or folders to be encrypted) and determining the encryption percentage (the percentage of data to be encrypted).



Create Mutex (Source : Sequeretek)

2. Shadow Copy Deletion

One of its main goals is to eliminate the possibility of system recovery via shadow copies. To do this, the ransomware uses the following PowerShell command:

```
powershell.exe -Command "Get-WmiObject Win32 Shadowcopy | Remove-WmiObject”
```

This command deletes shadow copies completely, making it impossible for users to recover their data.

3. Logical Drive Enumeration

The Akira ransomware uses the API call "GetLogicalDriveStrings()" to identify the number of logical drives on the victim's machine. This information is critical for identifying prospective encryption targets.

4. File and Directory Search

The malware looks for files and folders to encrypt on the victim's machine. It uses API calls such as "FindFirstFileW()" and "FindNextFileW()" to find possible targets for encryption

5. Exclusion Criteria:

Akira ransomware avoids encrypting certain files and folders by specifying exclusion criteria based on file extensions and folder names. These exclusions include:
Exclude file extensions: *.exe, *.dll, *.sys, *.msi, *.lnk, *.akira
Exclude folders: winnt, temp, thumb, $Recycle.Bin, System volume, Information boot, ProgramData

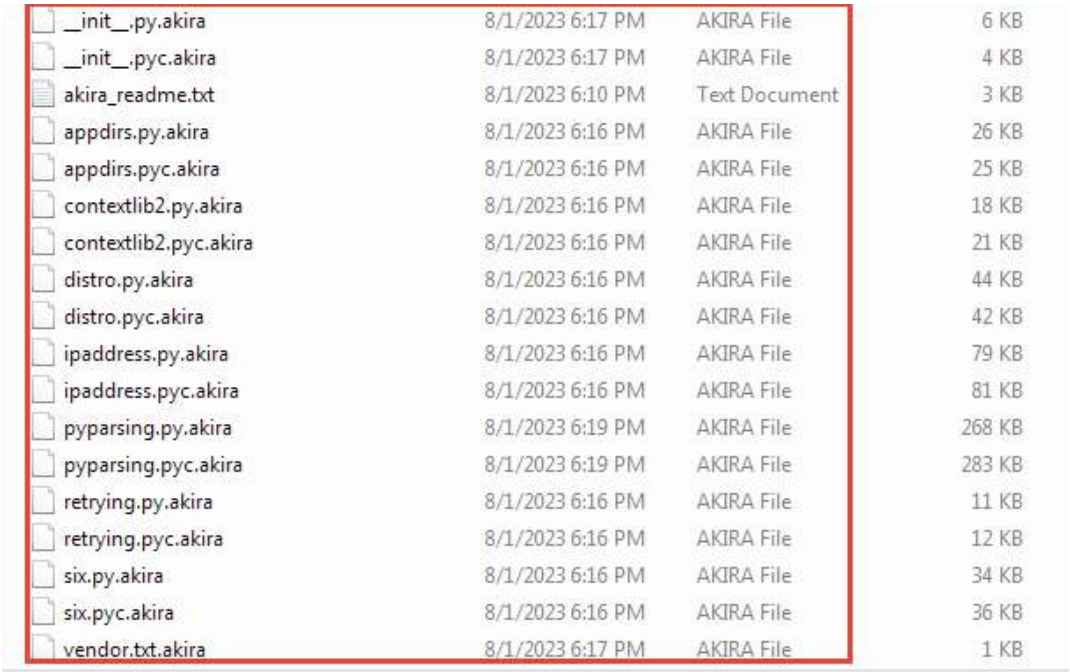
6. Encryption Process

For Windows, Akira leverages the Windows native library to leverage RSA and AES encryption methods for the encryption of data. Notably, it contains a hardcoded base64-encoded public key in its code.

Hard-coded Public Key (Source : Sequeretek)

7. Ransom Note Creation

Along with the encryption, Akira creates a text file called akira_readme.txt, which acts as a ransom letter. It is placed in several files across the victim's system. It includes directions for paying the ransom and obtaining decryption assistance.



File encrypted by Akira Ransomware

8. Ransom Payment Instructions

The ransom note provides instructions on how victims can make ransom payments. It also claims that the victims can receive "support" from the company to recover their encrypted files.

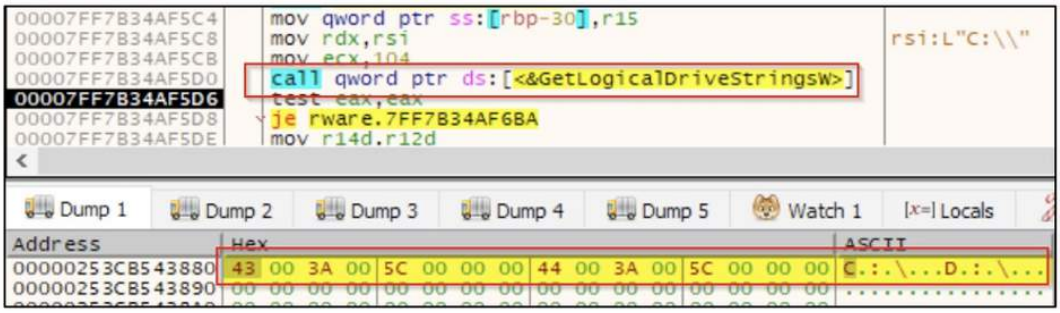
SAMPLE 2

Particulars	Value
Name	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c.bin
Size	572.50 kB
MD5	c7ae7f5becb7cf94aa107ddc1caf4b03
SHA1	923161f345ed3566707f9f878cc311bc6a0c5268
SHA256	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
SHA512	6a8cbbe8fc0d941fd5d8ba73251524078a9d3af32716ebfa2bb6398bb0ea794b2e924814ea633ed9cd0c113f7fa0bd49e48e9c0119c8a183c1cdcc388d592ad8
File Magic Description	PE32+ executable (console) x86-64, for MS Window

The behavior of this sample remains consistent with the behavior of Sample 1. Here is the breakdown of its malicious activity according to Cyble.

1. Logical Drive Enumeration

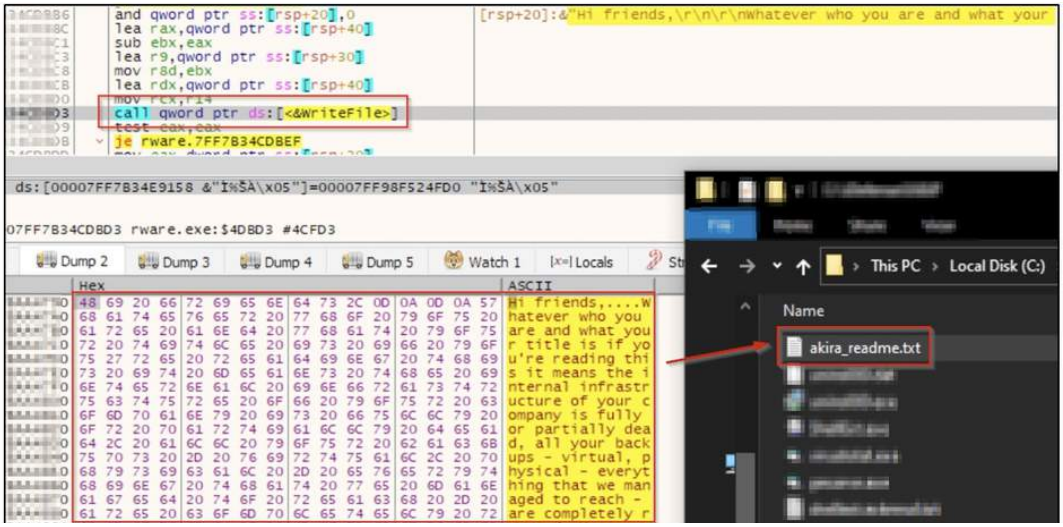
When executed, it also searches for logical drives currently available in the system through API function GetLogicalDriveStrings().



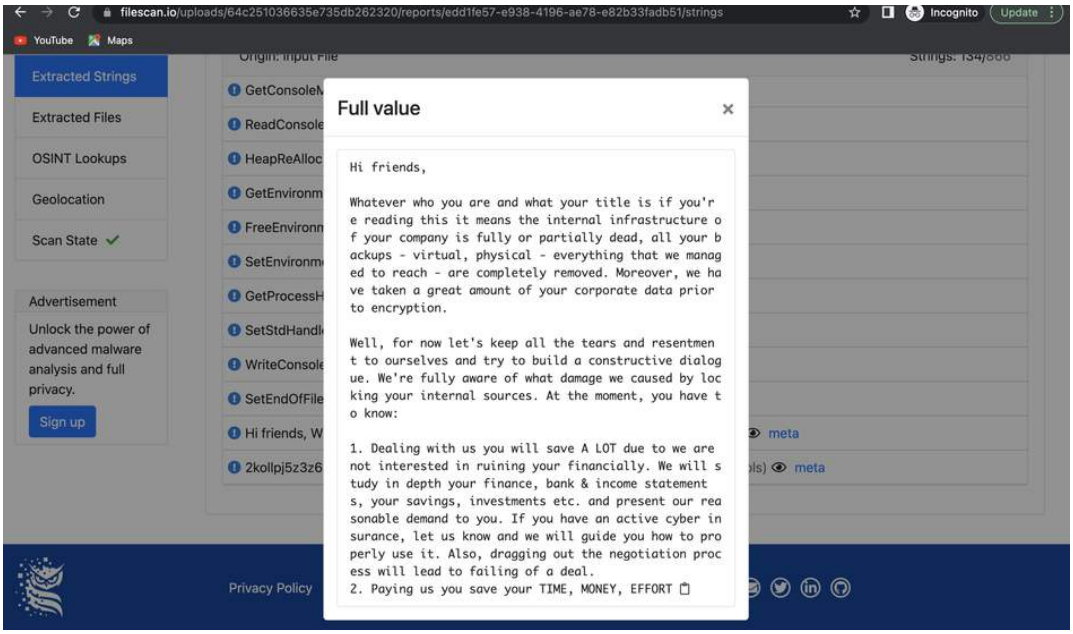
Local Drive Enumeration (Source:Cyble)

2. Ransom Note Creation

The ransomware then drops a ransom note, named “akira_readme.txt“ in multiple folders. It contains a message to the victims, which indicates that they have been hacked, and steps to follow to pay the ransom in order to decrypt their original data.



Local Drive Enumeration (Source:Cyble)



Ransom Note

3. File and Directory Enumeration

To encrypt the files, the ransomware then searches for folders and files using the API functions FindFirstFileW() and FindNextFileW(). It excludes different files/folders from encryption based on some criteria such as folder name, file name, and file extension.

File extension	File Names	Folder Names
.exe	akira.readme.txt	tmp
.dl	Bootmgr	winnt
.sys	BOOTNXT	temp
.msi	DumpStack.log.tmp	thumb
.ink	Pagefile.sys swapfile.sys ntuser.dat	$Recycle.Bin
.akira		$RECYCLE.BIN
		System Volume
		Information Boot
		Windows Trend Micro
		Program Data

4. Encryption

Windows native encryption cryptographic libraries from “Microsoft Enhanced RSA and AES Cryptographic Provider” are utilized by this sample to encrypt the victim’s machine data. As mentioned above, it excludes certain files and folders based on some criteria. Different CryptoAPI functions such as CryptAcquireContextW(), CryptImportPublicKeyInfo(), CryptGenRandom(), and CryptEncrypt() are utilized during the encryption process. The binary also includes a hardcoded base64 encoded public key.

Local Drive Enumeration (Source:Cyble)

The newly encrypted files are renamed with ".Akira" extension after successful encryption.

5. Deletion of Shadow Copies

To hinder the recovery possibility through shadow copies, it deletes shadow copies. Through WMI, it queries ShadowCopy and deletes it ultimately.

Powershell Command to delete shadow copy through WMI (Source:Cyble)

TTPS AND TOOLS DEPLOYED

In previous incidents, various security vendors and researchers have reported different Tactics, Techniques, and Procedures (TTPs) and tools employed by the Akira Ransomware, which may deviate from or are similar to the behavior observed in the samples discussed above.

In this chapter, we will meticulously review these diverse tools and TTPs used by the Akira Ransomware to ensure that no related artifacts or aspects are overlooked or omitted.

Credential Access

In May 2023, Sophos found out the adversary dumped the LSASS process memory leveraging the comsvcs.dll with proxy execution by rundll32.

```
Service Name: TcwvBcuf

Action: %COMSPEC% /Q /c cmD.Exe /Q /c for /f ""tokens=1,2 delims= "" ^%A in ('""tasklist /fi ""Imagename eq LSASS
do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\FP4.docx full"
```

According to Reconinfosec, the adversary also used the DonPAPI credential theft toolkit and mimikatz. DonPAPI is capable of "Dumping relevant information on compromised targets without AV detection.

Usage of DonPAPI (Reconinfosec)

Discovery

Akira has also been found creating a scheduled task named “Windows Update“ doing indirect directory listings according to Sophos.

```
C:\>type c:\programdata\HP\ms.bat

dir ""\\10.1.100.64\c$\ProgramData"" >> C:\programdata\HP\svr_dir.txtt"
```

They also suspect adversaries using pc_hunter to acquire detailed process and system information as they discovered adversaries' traces of online searching for pc_hunter. Alongside they also used an Advanced IP scanner possibly to discover other systems and networks. They also possibly use the net use command for network share enumeration.

Lateral Movement

To facilitate lateral movement, the attackers employed legitimate credentials for Remote Desktop Protocol (RDP) connections. They also reportedly used wmiexec for Lateral Movement.

Defense Envasion

To evade the Windows Defender, the threat actor disabled real-time monitoring and also added defender exclusions on the C:\ directory.

```
5001 - Real-time Protection was disabled
New Value">HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\
```

Command and Control

To facilitate command and control, the Akira Ransomware gang has been known to use tools like AdnyDesk and CloudFlared.

Collection

According to Sophos, they definitely have observed tools like WinRar being downloaded on compromised devices., used for data compression but haven't observed exfiltration activity.

Impact

It is now evident that they employ PowerShell to delete shadow copies, a method we also identified in the sample we examined.

DETECTION THROUGH LOGPOINT CONVERGED SIEM

To detect and remediate the threats from Ransomware such as Akira, it is crucial to detect suspicious activities in the early phase of the attack. We at Logpoint have created alerts, specially tailored to detect suspicious activities of Ransomware like Akira. Sending all the necessary Logs to Logpoint for centralized view and alerting can help detect such events and take appropriate actions in time ultimately reducing the risk and being in a good spot rather than having no visibility and getting data leaked and encrypted because of the ransomware.

Log Sources

In order to ensure the effectiveness of these queries, it is important to have relevant logs from specific sources. While some logs are logged by default, 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 provided detection queries. 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

2. Windows Sysmon

Deletion of Shadow Copies through Powershell

We can look for suspicious patterns in the command line field of process creation events to detect deletion activity of shadow copy through Powershell.

```
label="process" label=create
command IN ["*Get-WmiObject*", "*gwmi*", "*Get-CimInstance*", "*gcim*"]
command="*Win32_Shadowcopy*"
command IN ["*.Delete()*", "*Remove-WmiObject*", "*rwmi*", "*Remove-CimInstance*", "*rcim*"]
```

We can also detect such events from PowerShell native logs (i.e. event id 400, 800).

```
norm_id=WinServer event_id IN [400,800]
host_application="*Get-WmiObject*" host_application="* Win32_Shadowcopy*"
host_application IN ["*Delete()*", "*Remove-WmiObject*"]
```

Sometimes process creation events cannot detect these activities if obfuscated commands are executed. In such cases, PowerShell script block logging can be leveraged as it logs the unobfuscated command that was executed.

```
norm_id=WindowsServer norm_id=4104
script_block IN ["*Get-WmiObject*", "*gwmi*", "*Get-CimInstance*", "*gcim*"]
script_block="*Win32_Shadowcopy*"
script_block IN ["*.Delete()*", "*Remove-WmiObject*", "*rwmi*", "*Remove-CimInstance*",
"*rcim*"]
```

Creation of file encrypted by Akira Ransomware

Akira ransomware generally appends ".akira" in the file extension after encryption. Analysts can hunt for such creation of files whose extension ends with ".Akira".

```
label=file label=create path=*
file=* file="*.Akira"
```

If analysts see the cretion of such files in any host, it might have been infected by Akira Ransomware.

Usage of Cloudflared Tunnel

Installation of Cloudfared for remote access into the victim environment has been observed in the Akira Ransomware campaign. Analysts can use the following query to detect suspicious usage of **Cloudfared Tunnel** in the enterprise network.

```
label="process" label=create command="* tunnel *"
command="* run *"
command IN ["* --config *", "* --credentials-contents *",
"* --credentials-file *", "* --token *"]
```

LSASS Process memory dump via "comsvcs.dll" using rundll32

In order to obtain credentials, move laterally, and persist on the system, adversaries often dump LSASS memory. Rundll32 is a Windows native binary that is used to run Dynamic Link Library (DLLs) on the Windows operating system. Comsvcs.dll exports a function called MiniDump . When this function is called with the process ID of LSASS, we can get a minidump file containing the secret information. Analysts can hunt the LSASS process memory dump through the query below:

```
label="process" label=create ("process"="*\rundll32.exe" or file="RUNDLL32.EXE")
command="*comsvcs*"
command="*full*" command IN ["*#-*", "*#+*", "*#24*", "*24 *", "*MiniDump*"]
```

Mimikatz execution for credential access

The instance of mimikatz execution was also found for credential access. We can look for the patterns used in mimikatz commands using the following query.

```
label="Process" label=Create
command IN ["*DumpCreds*", "*mimikatz*", "*::aadcookie*", "*::detours*",
"*::memssp*", "*::mflt*", "*::ncroutemon*", "*::ngcsign*", "*::printnightmare*",
"*::skeleton*", "*::preshutdown*", "*::mstsc*", "*::multirdp*", "*rpc::*",
"*token::*", "*crypto::*", "*dpapi::*", "*sekurlsa::*", "*kerberos::*",
"*lsadump::*", "*privilege::*", "*process::*", "*vault::*", "*crypto::*",
"*misc::*", "*event::*", "*IIS::AppHost*", "*net::*","*sid::*", "*standard::*",
 "*vault::*"]
```

Usage of Impacket wmiexec

Analysts can use the following query to detect potential Impacket Lateral Movement Activity.

```
label="process" label=create
command="*cmd.exe*" command="*/c*" command="*&1'*"
(parent_process In ["*\wmiprvse.exe", "*\mmc.exe", "*\explorer.exe", "*\services.exe"]
command="*/Q*" command="*\\\\127.0.0.1\\*" )
OR (parent_command IN ["*svchost.exe -k netsvcs*", "*taskeng.exe*"]
command="*Windows\Temp\*")
```

Windows Defender Tampering

Akira Actors's attempts to disable Windows Defender were seen during the campaign's run. We can detect this through process creation and registry events. The below query can detect Windows Defender disabling events through process creation events.

```
label="process" label="create" "process"="*\reg.exe"
"command" IN ["*SOFTWARE\Microsoft\Windows Defender*",
"*\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*"]
)
```

These processes modify their respective registry values and we can track them through Symon registry events (Event IDs 12, 13, 14) to detect any modifications in the registry. we can use this awesome sigma rule to detect the creation of the scheduled task through registry events.

```
label=registry label=set
target_object IN ["*\SOFTWARE\Microsoft\Windows Defender*",
"*\SOFTWARE\Policies\Microsoft\Windows Defender Security Center*",
"*\SOFTWARE\Policies\Microsoft\Windows Defender*"]
(
detail="DWORD (0x00000001)"
target_object IN ["*\DisableAntiSpyware", "*\DisableAntiVirus",
"*\DisableBehaviorMonitoring", "*\DisableIntrusionPreventionSystem",
"*\DisableIOAVProtection", "*\DisableOnAccessProtection", "*\DisableRealtimeMonitoring",
"*\DisableScanOnRealtimeEnable",
"*\DisableScriptScanning", "*\DisableEnhancedNotifications",
"*\DisableBlockAtFirstSeen"]
)
OR
(
detail="DWORD (0x00000000)"
target_object IN ["*\App and Browser protection\DisallowExploitProtectionOverride",
"*\Features\TamperProtection", "*\MpEngine\MpEnablePus", "*\PUAProtection",
"*\Signature Update\ForceUpdateFromMU", "*\SpyNet\SpynetReporting",
"*\SpyNet\SubmitSamplesConsent",
"*\Windows Defender Exploit Guard\Controlled Folder Access\EnableControlledFolderAccess"]
)
```

LOGPOINT CONVERGED SIEM FOR INVESTIGATION AND RESPONSE

Logpoint Converged SIEM integrated security platform comprised of Logpoint SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and AgentX for EDR (Endpoint Detection and Response) capabilities. Organizations can leverage its converged security capability to detect, hunt, investigate, and remediate threats.

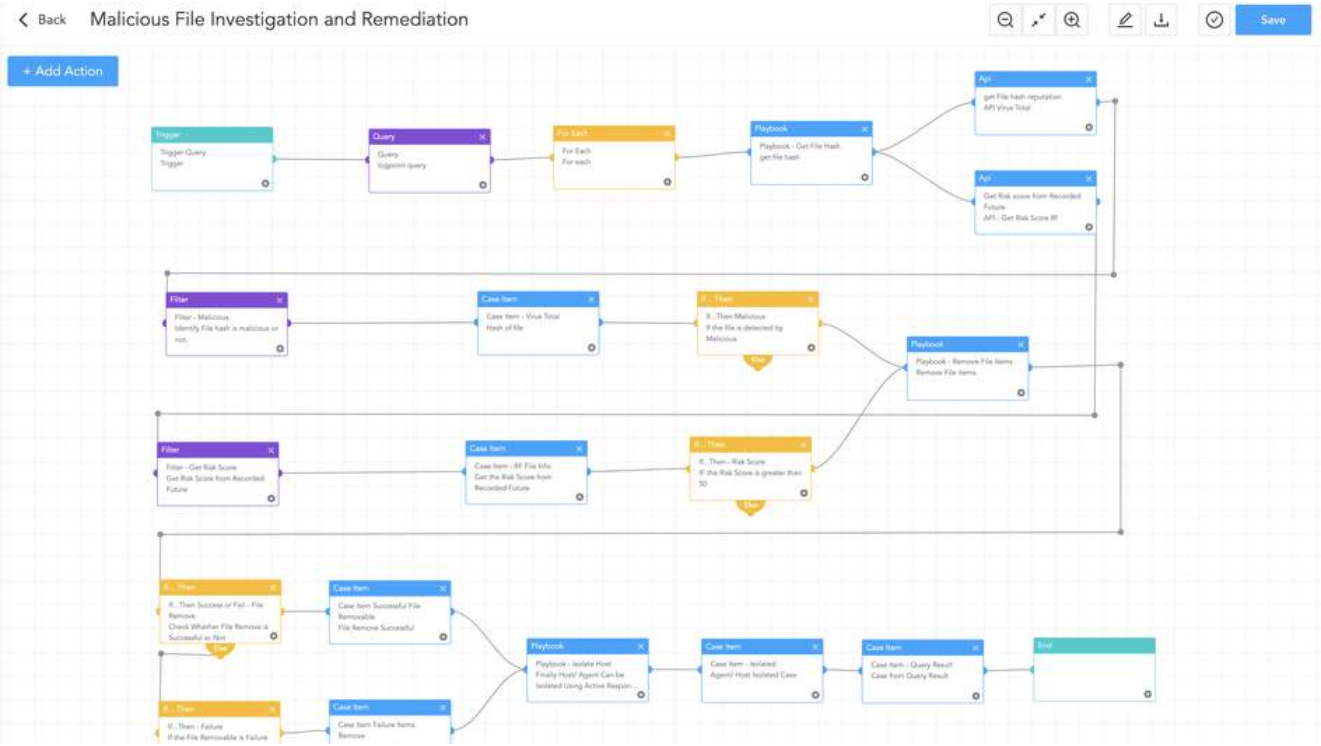
Logpoint SIEM collects and correlates the logs from multiple sources, including the host endpoints, firewall, gateway, etc. SIEM enables early detection of any suspicious behaviors from any source through real-time monitoring combined with analytics like alerts, dashboards, and search templates.

The inclusion of SOAR can be the cherry on the cake as it can strengthen the current capability of SIEM with automated investigation and response through tailor-cased playbooks for specific cases. This can streamline the incident response process and minimize the potential impact through early automated response. Agentx is the Logpoint new agent for endpoints,
which comes equipped with pre-build EDR capabilities. Not only does it provide detailed visibility into endpoint activities, but it also assists in advanced threat hunting and forensic investigations with Osquery. By continuously monitoring endpoints for indicators of compromise and malicious behaviors associated with Akira's infection chain, AgentX enables prompt identification and containment of compromised systems.

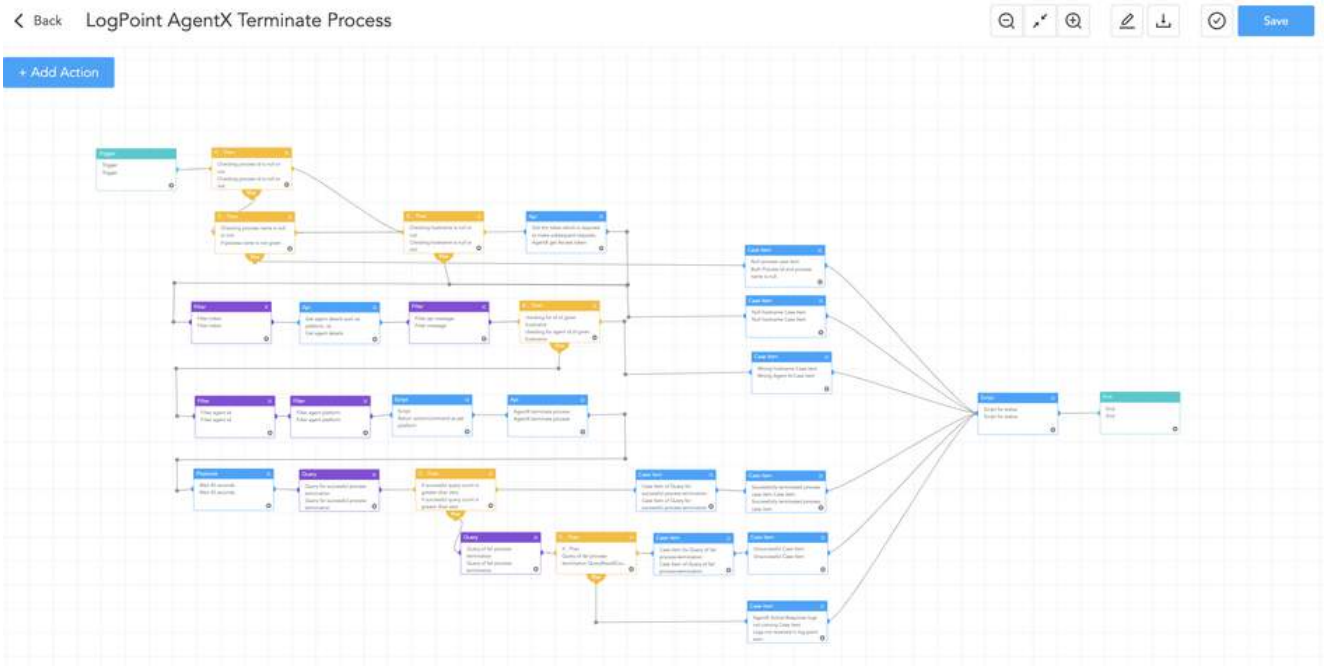
Logoint already has prebuilt playbooks that cover a broad spectrum of use cases including threat detection and response, compliance management, log analysis, incident handling, and more. Even though we offer many playbooks, only relevant playbooks that may aid in the investigation and Remediation of Akira Ransomware are elaborated upon.

Malicious File Investigation and Containment

It has been evident that Akira Ransomware deploys its binary to encrypt data on victim's machines. The 'Malicious File Investigation and Containment' has been created to deal with such abnormal binaries when they got dropped on the system. It starts by comparing the hash of the dropped file with threat intel, and if found malicious, it stops the linked process while removing the original file as well.

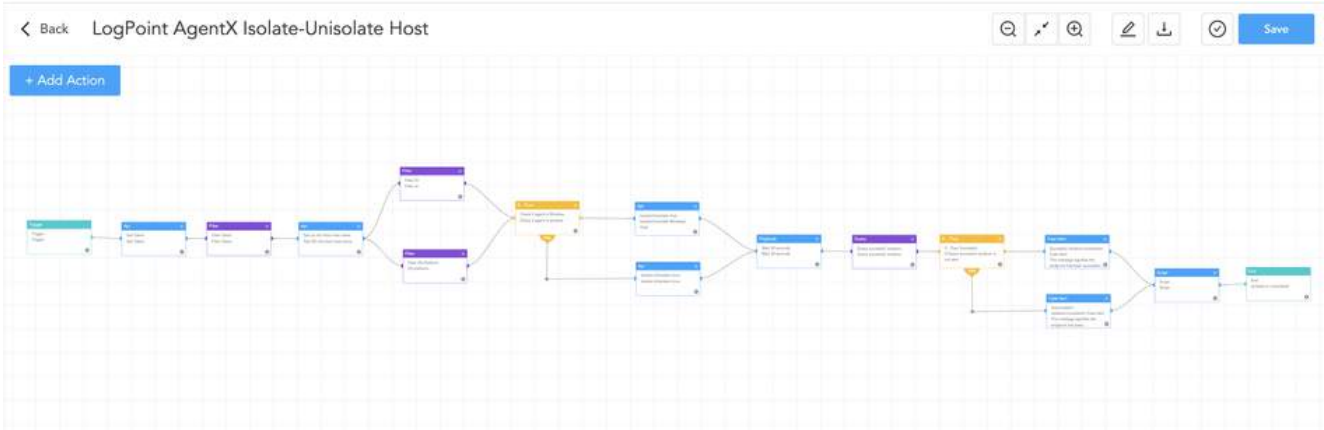


It also looks for that hash in other endpoints to look out for possible affected machines. and if found, the malicious file and processes are immediately removed to avoid the impact. The playbook uses the functionality of the "AgentX Terminate Process" and "AgentX Remove Item" playbooks to carry out these activities, allowing analysts to effectively terminate malicious processes and delete damaging files from afflicted computers.



Isolate the host

When it has been confirmed that, the specific host has been compromised by the Threat Actors and could possibly be exfiltrating data, it's important to contain that host from the network. In order to do so, 'AgentX Isolate Host' can be leveraged to isolate their host from the network. It can help to mitigate potential risks by removing the chance of infection in other hosts.



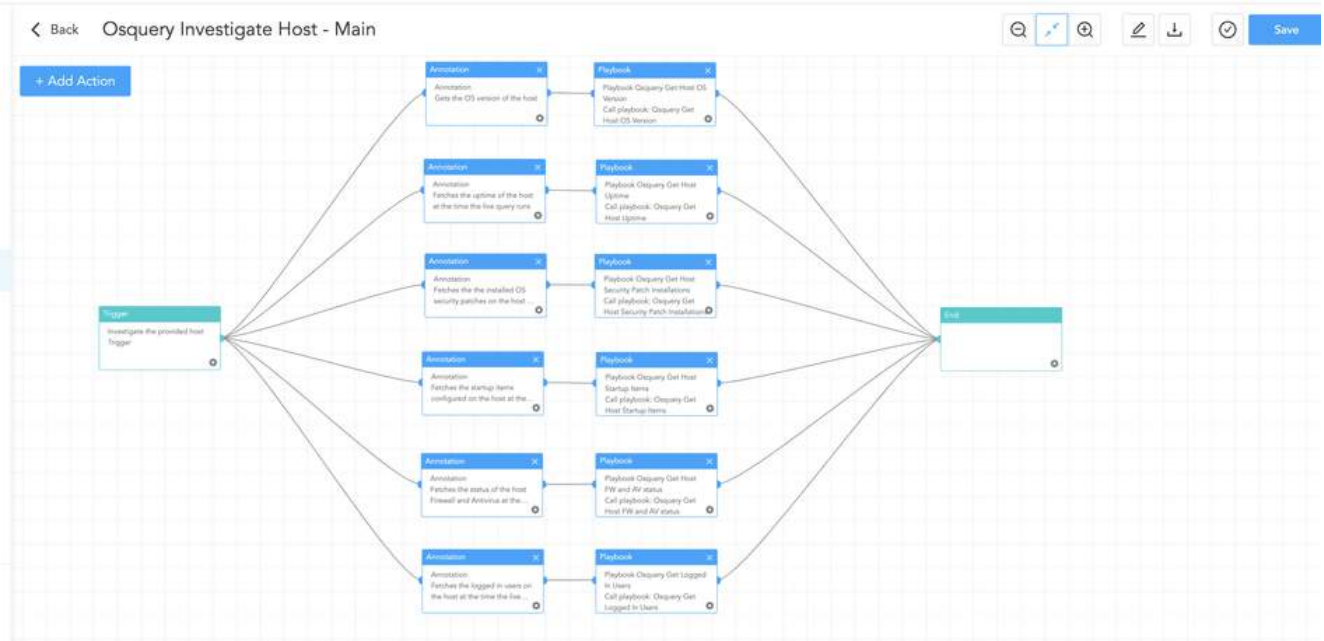
Host Investigation through Osquery

Osquery is an open-source endpoint security tool that allows for querying and monitoring various aspects of operating systems. It provides real-time and granular-level visibility on the endpoints. It comes prebuilt with AgentX. With AgentX, we also offer Osquery playbooks that can be utilized to perform the whole host investigation with just one execution.

Some of the notable ones are:

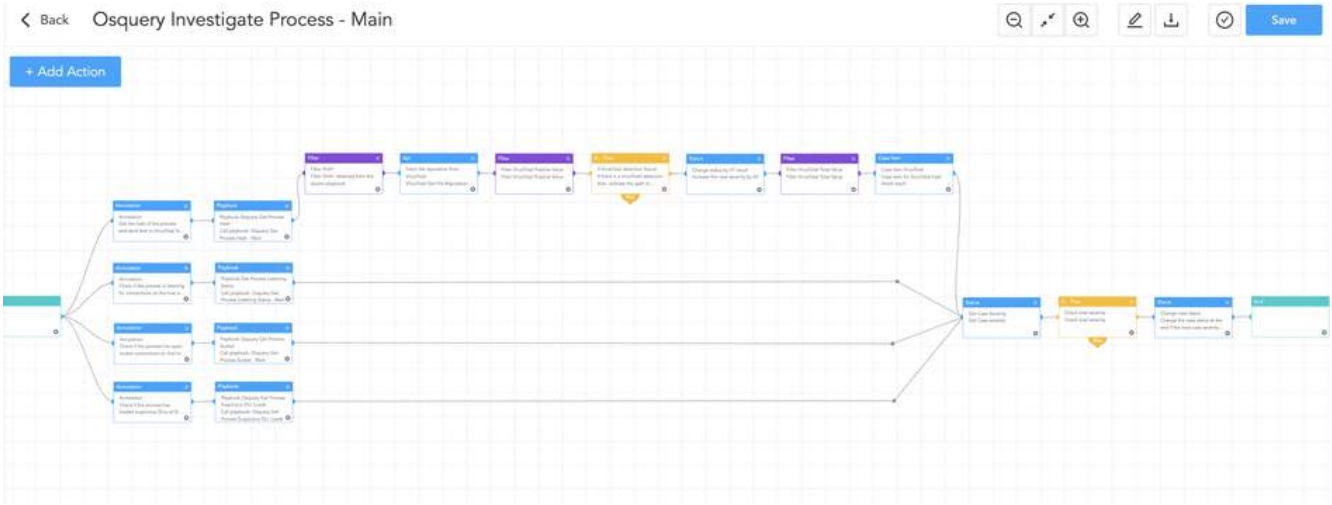
Osquery Investigate Hosth Osquery

This playbook offers a comprehensive approach by providing the OS version, system uptime, currently logged-in users, startup items, firewall status, security patch information, and more, all within one playbook.



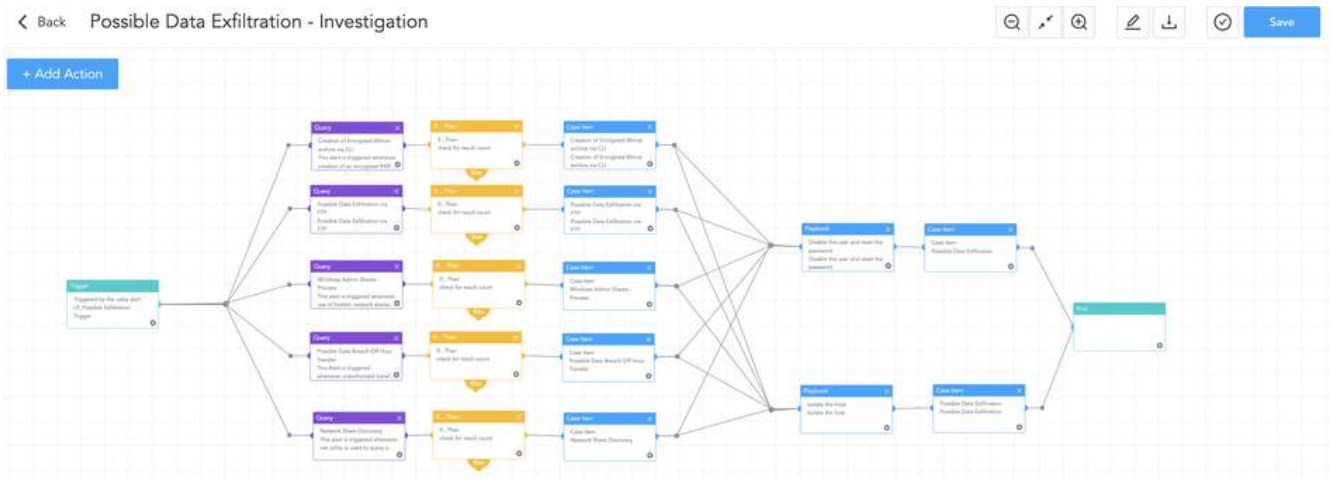
Osquery Investigate Process

The 'Osquery Investigate Process' playbook is an invaluable resource for security teams seeking to investigate a specific process on a host. This playbook enhances process investigation by assessing process hash reputation through VirusTotal integration and examining listening status and socket connections for detecting potential malicious activities and unauthorized network access. It also analyzes the loaded dynamic-link libraries (DLLs) of the process.



Possible Data Exfiltration

When a security analyst detects data exfiltration within the company network, the "Possible Data Exfiltration" playbook can be used as an investigative step. This playbook automates the investigative process to quickly discover and prevent data exfiltration by executing predetermined detection mechanisms and analysis methodologies.



RECOMMENDATION

Implement Secure Access Controls

Akira actors got into the target system by brute-forcing credentials of the MFA-disabled Cisco ASA VPN. So, it is recommended to ensure that passwords are unique and strong for all accounts, and also implement multi-factor authentication (MFA) wherever possible. Also, provide the user with just the permission that he/she is required to do for her job.

Keep Software and Systems Updated

Adversaries often exploit newly discovered vulnerabilities. Vendors often release new patches as early as a new vulnerability is discovered. So, it is advised to keep the OS or applications updated by regularly updating it. If in case, due to some reason, it is not feasible, mitigations provided by vendors should be applied. Also in other cases where many security issues need to be fixed, prioritize the issues based on severity and patch or apply mitigation accordingly.

Conduct Regular Security Awareness Training

Social engineering, Phishing in particular is the common and effective initial vector of any successful breach or attack. Organizations should provide regular training to employees on how to recognize and respond to social engineering attacks like phishing mail, including simulated exercises that replicate real-world scenarios making them aware of the latest trends and tactics of Threat Actors

Auditing of privileged accounts

Implement auditing of privileged accounts to detect unauthorized activities, such as limited-scope contractors accessing out-of-scope machines during non-working hours. Inadequate monitoring of privileged accounts can lead to their misuse, which can result in data breaches, system disruptions, and other security breaches with serious repercussions for an organization.

Employ Network Segmentation

Use network segmentation to keep important systems and sensitive data apart from the rest of the network. This helps to confine possible breaches and minimize attacker lateral movement. DMZ (Demilitarized Zone) and honeypots should be used for security isolation, Limited Attack Surface, Segmentation, and Compartmentalization.

Block unauthorized tunneling/remote access tools

Adversaries often use tunneling and remote access tools like Cloudflare ZeroTrust, ZeroTier, TailScale, etc. to gain covert access to compromised networks. So, it's recommended to block unauthorized tunneling/remote access tools.

Backup and Disaster Recovery Planning

Ensure regular offsite and onsite data backups. Employ the 3-2-1 backup policy that involves creating three copies of important data, storing those copies in two different formats or locations, and keeping one copy offsite.

Protect Volume Shadow Service

Ensure Volume Shadow Service is active with ample space, critical for ransomware recovery. Implement VSC protection with EDR solutions to detect and halt tampering, a crucial defense against ransomware attacks.

CONCLUSION

Akira has emerged as a tenacious and devastating adversary in an ever-changing field of cyber threats that has grabbed widespread notice in a short period of time. Organizations must adapt and improve their security procedures in this situation. The growing number of people falling victim to this expanding menace emphasizes the importance of the situation.

Logpoint's security operations platform, Converged SIEM, contains a range of extensive tools and capabilities for identifying, evaluating, and mitigating the impact of Akira Ransomware. With features like native endpoint solution AgentX and SOAR with pre-configured playbooks, it enables security teams to automate essential incident response procedures, gather vital logs and data, and expedite malware detection and removal operations.

In an ever-changing threat landscape, Logpoint gives organizations the tools and capabilities they need to monitor risks, build defenses, and protect against Ransomware activities like Akira.

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**