Taiwan Government Targeted by Multiple Cyberattacks in April 2020

By CyCraft Technology Corp

Published: 2022-06-10 · Archived: 2026-04-05 16:26:56 UTC

Press enter or click to view image in full size

Part 2: Owlproxy Malware

In April 2020, CyCraft observed highly malicious cyber activity in several Taiwan government agencies. Some of these attacks have been attributed to the same threat actor due to similar techniques, tactics, and procedures — the most important of which is the utilization of Skeleton Keys and Owlproxy malware.

> This article is Part 2 of a series of articles. Click here to read Part 1: Waterbear Malware.

What is a Skeleton Key?

In 2014, Dell Secureworks Counter Threat Unit observed the earliest use of a digital Skeleton Key. Their observed Skeleton Key was able to bypass authentication on Active Directory (AD) systems implementing single-factor verification (T1556.001 Modify Authentication Process: Domain Controller Authentication). Using this method, much like how a physical Skeleton Key can open any door in a house, a digital Skeleton Key gives its user unfettered access to remote access services.

In 2019, CyCraft observed a possible China-sponsored APT group, APT Chimera, target the Taiwan semiconductor industry in a year-long campaign. Chimera added extracted key code snippets from both Mimikatz and Dumpert to their customized Skeleton Key. The Chimera Skeleton Key sought to bypass API monitoring, which is widely used in anti-virus and EDR products, by directly invoking syscalls and implementing high-level API logic.

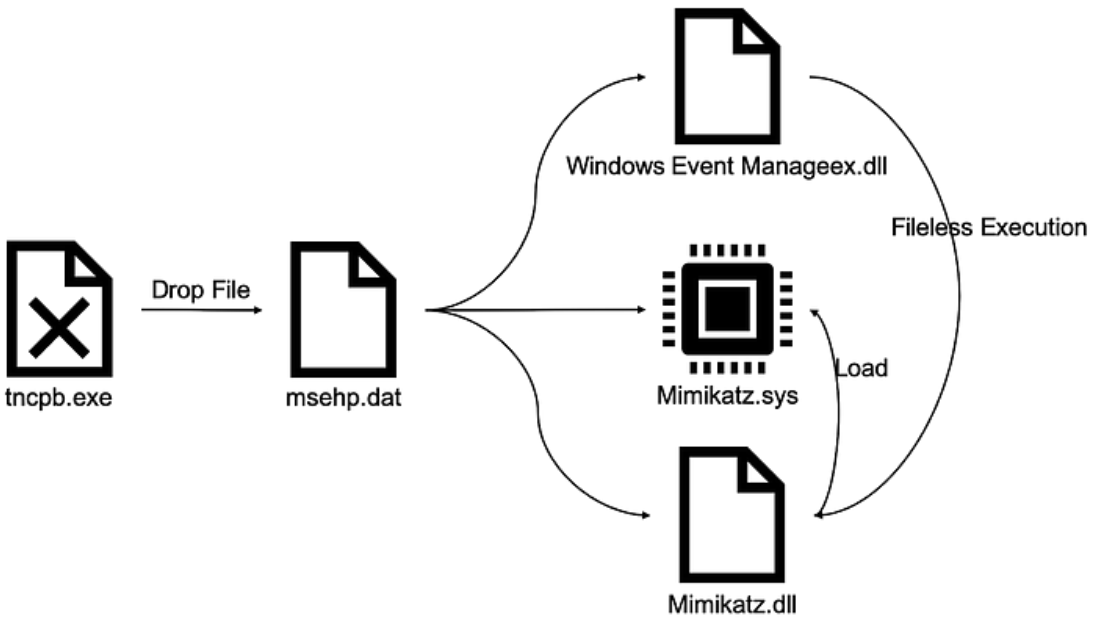
> "Even though several of the April 2020 attacks use the same techniques as APT Chimera, available evidence and artifacts in the April 2020 attacks do not suggest attribution to APT Chimera. However, this does suggest that China-based APT groups may share malware, tools, or even similar techniques. This sharing of tools, techniques, and malware adds difficulty to the attribution process."
> -C.K. Chen, CyCraft Senior Researcher

What is Owlproxy?

Owlproxy is one of the primary malware discovered in several of the April 2020 incidents. In order to bridge the internet and intranet, the threat actor used this malware with backdoor functionality to tunnel in and out of the network. This backdoor functionality enables threat actors to launch any commands directly into the target system. While the program database (PDB) information is resident in the binary, the malware's name, Owlproxy, comes from the project name of the PDB file.

How to inject a Skeleton Key

Press enter or click to view image in full size



The malware, tncpb.exe, would first drop msehp.dat, which also contained Windows Event Manageex.dll, Mimikatz.dll and Mimikatz.sys (with the name WinHelp.sys). While Windows Event Manageex.dll was loading, it would also invoke Mimikatz.dll for a Skeleton Key. If it fails to open lsass, Mimikatz.sys would be loaded as the

alternative to unprotect Isass.exe (T1003.001 OS Credential Dumping: LSASS Memory). As a result, the Skeleton Key would be injected, and the attackers could then gain unfettered access to the domain endpoints.

wmipd.dll

The wmipd.dll is the main remote administration tool (RAT) in this attack. The most important characteristic of this malware is that it is an HTTP proxy (T1071.001 Application Layer Protocol: Web Protocols) with backdoor functionality. This malware can be accessed via port 80 to execute commands (T1059.003 Command and Scripting Interpreter: Windows Command Shell) and proxy traffic in and out of the victim's network.

File Metadata

md5: cb1f2894cd35b173140690b0a608d4b6
sha1: d744fb9adbd2d79c6016044de4a75e6c4f3fefb0
sha256:5b3ca2aacfa0996275c7a116bc2b14a03161b264ba4c699a55a5d19b8677969b
family: Owlproxy (family name first designated by TrendMicro)
filetype: PE32+ executable (DLL) (GUI) x86–64, for MS Windows
pdb: F:\project\owl\isapi\x64\Release\iisdll.pdb

Behavior

wmipd.dll uses WinHTTP API to create an HTTP server on port 80 with these endpoints:

```
http[:]//+:80/servlet/ (General backdoor, execute any commands)http[:]//+:80/servlet/pp/ (HTTP to tc
```

IOC

```
file_path: %WINDIR%\System32\Windows Event Manageex.dllhttp[:]//127.0.0[.]1/servlet/http[:]//127.0.0
```

Stage One: tncpb.exe

The first stage malware tncpd.exe will drop msehp[.]dat, which further contains Windows Event Manageex.dll, Mimikatz.dll, and WinHelp[.]sys (Mimikatz.sys). The mission of tncpb[.]exe is to load Windows Event Manageex[.]dll — the linchpin of the attack.

Stage Two: Windows Event Manageex.dll

This malware has been designed for persistence. After it is dropped by tncpb.exe, Windows Event Manageex.dll self-installs. The previous stage malware (tncpb.exe) is then deleted (T1070.004 Indicator Removal on Host: File Deletion). The next stage malware (Mimikatz.dll), designed for credential access, is then triggered.

File Metadata

filename: Windows Event Manageex.dll
md5: d770a361646a0463f597c127e0705265
sha1: d0c5baaa4aa4163ab6f6792ad5c394bca455f33a
sha256:2adc730d232583a2efecce8b13598eb23791440f47295fa1afede26be1d6e070
filetype: PE32+ executable (DLL) (GUI) x86–64, for MS Windows

Behavior

1. Windows Event Manageex.dll self installs.
2. Windows Event Manageex.dll uses CreateThead() to delete tncpb.exe at location: C:\$Recycle.Bin\tncpb.exe (T1074.001 Data Staged: Local Data Staging).
3. Execute Mimikatz[.]dll in memory.
4. Windows Event Manageex.dll uses CreateThread() to drop C:\Windows\system32\Windows Event Manageex.dll (Mimikatz.sys) from msehp.dat#3(x)
5. Windows Event Manageex.dll deletes C:\$Recycle.Bin\tncpb.exe (T1070.004 Indicator Removal on Host: File Deletion
   T1074.001 Data Staged: Local Data Staging)

IOC

```
event: “Global\\Microsoft Windows CriticalRestore Event”file_path: $SystemDirectory\wbem\msehp.dat
```

Stage Three: Mimikatz.DLL

A customized modification of the original Mimikatz, Mimikat.dll was designed to specifically inject the Skeleton Key to allow the attackers persistent, unfettered Lateral Movement across the network. This was an interesting approach as Skeleton Keys aren’t typically used for credential access. Once injected, the modified Skeleton Key modifies the original execution logic of lsass.exe and then injects the backdoor password. This malicious behavior is similar to legit user behavior, which helps this particular technique evade detection. In case the injection fails (cannot gain access to lsass.exe), an alternative approach is taken; the kernel driver WinHelp.sys is installed and unprotects lsass.exe, allowing the DLL malware to inject the Skeleton Key once again. Once the Skeleton Key injection is successful, the kernel driver will be unloaded.

File Metadata

filename: msehp.dat#4
md5: 3838d0f1cb10f04632a6ca7fd79c3d0d
sha1: 6641ff84b0d00431cd4bbdc9f6dee185fe137c22
sha256:d88fdf1204e13472e8df87dc8e7a9d8a931e22658b88d48f510e56bc171e8938
filetype: PE32+ executable (DLL) (console) x86–64, for MS Windows
family: mimikatz

Behavior

1. Inject Skeleton Key (first attempt)

```
If successful:
     createEvent(L"Global\\Debug_Windows_Dump_Event")
If signature not found:
     createEvent(L"Global\\Windows_MemoryDump_Event")
If OpenProcess failed:
     load mimikatz driver (WinHelp.sys)
     Unprotect lsass.exe
     Inject Skeleton Key again
     Unload mimikatz driver
```

2. Delete mimikatz driver

IOC

```
file_path: $SystemDirectory\wbem\msehp.datfile_path: $SystemDirectory\Drivers\WinHelp.sys
```

WinHelp.sys

WinHelp.sys is the Mimikatz driver used to unprotect lsass[.]exe.

File Metadata

md5: c3a077bc0e4095d68569817b51bea7a2
sha1: e4c9ba7299f2e201295e882ff528d2a0b89d382b
sha256:75c5cc5c9e07b04d8f68b5788a4514d294be607431f37bb04f6e5d93b9936c74
filetype: PE32+ executable (native) x86–64, for MS Windows
pdb: u:\skeleton\mimikatz-master_20170107\mimidrv\objfre_wnet_amd64\amd64\mimidrv[.]pdb

IOC

```
cert_serial: 5f78149eb4f75eb17404a8143aaeaed7cert_fingerprint: 31e5380e1e0e1dd841f0c1741b38556b252e6
```

Certificate

The certificate embedded in the driver is signed by 上海域联软件技术有限公司 (Shanghai Yulian Software Technology Co., Ltd.).

MITRE ATT&CK®

The following MITRE ATT&CK techniques were observed in this attack.

Execution

T1059.003 Command and Scripting Interpreter: Windows Command Shell

Defense Evasion

T1070.004 Indicator Removal on Host: File Deletion
T1556.001 Modify Authentication Process: Domain Controller Authentication

Credential Access

T1556.001 Modify Authentication Process: Domain Controller Authentication
T1003.001 OS Credential Dumping: LSASS Memory

Collection

T1074.001 Data Staged: Local Data Staging

Command And Control

T1071.001 Application Layer Protocol: Web Protocols

Mitigation

1. Add listed IOCs to preventative solution blacklists.

2. Adjust detection and response solutions to detect listed IOCs.

3. Scan network for port 80 in non-server endpoints.

4. Remove Skeleton Keys*
**Be sure to first remove any malware that will inject the Skeleton Key, including Windows Event Manageex.dll as it is self-installing. Then, reboot the endpoint to clean up the modified memory.*

> This article is Part 2 of a series of articles. Click here to read Part 1: Waterbear Malware.

Follow Us

Blog | LinkedIn | Twitter | Facebook | CyCraft

When you join CyCraft, you will be in good company. CyCraft secures government agencies, police and defense organizations, Fortune Global 500 firms, top banks and financial institutions, critical infrastructure, airlines, telecommunications, hi-tech firms, and SMEs.

We power SOCs using innovative CyCraft AI technology to automate information security protection with built-in advanced managed detection and response (MDR), global cyber threat intelligence (CTI), smart threat intelligence gateway (TIG), security operations center (SOC) operations software, auto-generated incident response (IR) reports, system-wide network Health Check, and Secure From Home services.

Additional Related Resources

- Learn how we detected and defeated a China-sponsored APT targeting Taiwan's high-tech ecosystem. Read our full analysis and malware reversal.
- Using ATT&CK for CTI Training | MITRE ATT&CK®
- ATT&CK Evaluations: Understanding the Newly Released APT29 Results
- CyCraft Classroom: MITRE ATT&CK vs. Cyber Kill Chain vs. Diamond Model
- Quantifying the MITRE ATT&CK Round 2 Evaluation
- CyCraft CEO, Benson Wu, and CyCraft Global Project Manager, Chad Duffy, speak on the latest MITRE ATT&CK Evaluations. Read their thoughts on our results and the philosophy powering CyCraft.
- Has your organization shifted to a Work From Home environment? Learn how to receive Three FREE months of our Secure From Home Service.
- Our Enterprise Health Check drops your mean dwell time down from 197 days to under 1 day without false positives or false negatives. Know with confidence if hackers have penetrated your enterprise.

READY FOR A DEMO?

Contact us directly for more details: contact@cycraft.com
