Ghost in Crypto

APT Campaign Targeting Crypto Groups

Prepared by: **Halborn**

Date of Engagement: -

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	07/25/2022	Alpcan Onaran
0.2	Document Review	07/26/2022	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com
Alpcan Onaran	Halborn	Alpcan.Onaran@halborn.com

EXECUTIVE SUMMARY

1.1 Analysis Summary

Halborn detected that a threat group may be targeting crypto groups and companies, using a modified version of Gh0st RAT (Remote Administration Tool) similar to Zergost.

Based on a recently viewed report where it is stating that “recently discovered a Remote Access Trojan (RAT) virus posted in a crypto investment public Telegram chat. The company says the purpose of this Trojan was to steal Bitcoin keys.”

We analyzed the malicious files that were used in the specified attack. The malicious file was found to be a variant of Gh0st RAT, which has the following capabilities:

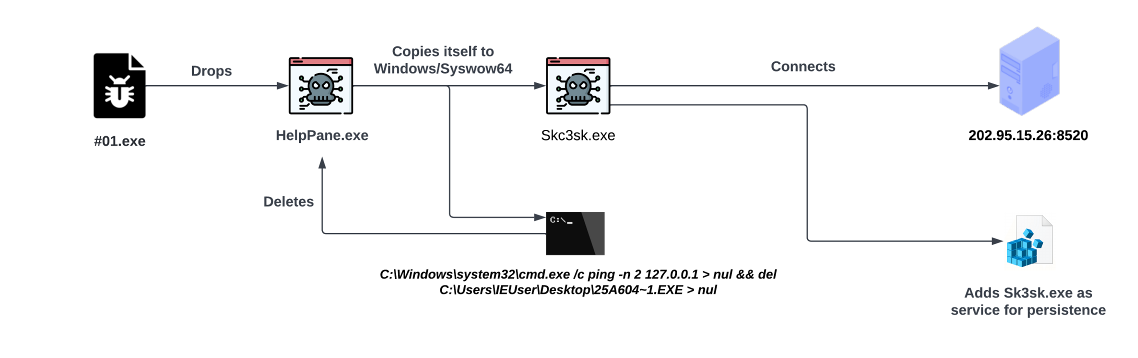
- Remote control of the victim’s computer
- Record key logs
- Take screenshots
- Download files from the victim’s computer
- Activating webcam and microphone
- List active processes
- Shutdown/Reboot the target computer

The file adds itself as a startup service to remain persistent. However, we did not find any indicators that are used especially to steal or copy private keys.

We deduced that this attack was linked to a possible Chinese APT group.

1.2 Execution Flow

- The first dropper puts the Gh0st RAT variant on disk and runs it.
- Dropped malware reads registry keys such as computer name and terminal service keys.
- The malware copies itself to the Windows SysWoW64 directory as Skc3sk.exe, and removes itself using cmd.
- Skc3sk.exe is added itself to Windows services for persistence.
- Skc3sk.exe connects to its C2 server.


#01.exe
Drops
HelpPane.exe
Copies itself to Windows/Syswow64
Skc3sk.exe
Connects
202.95.15.26:8520
Deletes
C:_
Adds Sk3sk.exe as service for persistence

```
C:\Windows\system32\cmd.exe /c ping -n 2 127.0.0.1 > nul && del
C:\Users\IEUser\Desktop\25A604~1.EXE > nul
```

Figure 1: Execution flow

1.3 Targets and Capabilities

All campaigns observed were directed at potential high-value targets. That APT does not focus on any particular businesses worldwide. They mostly target high-value targets where they can gather intelligence or make financial gain, this makes the crypto sector a preferred target and they expect to see more attacks against the crypto community in the near future.

In their operations, APT uses a modified version of Gh0st RAT, which maybe be Zergost. They took the risk of packing the malicious file and made minor edits in each attack, but kept the main malicious file the same.

STATIC ANALYSIS

2.1 Definition

Static analysis examines a malware file without actually running the program. Static analysis is used to detect whether a file is malicious, using technical indicators such as file names, hashes, strings including IP addresses and domain names, and file headers.

The process of static analysis of suspicious file is detailed below.

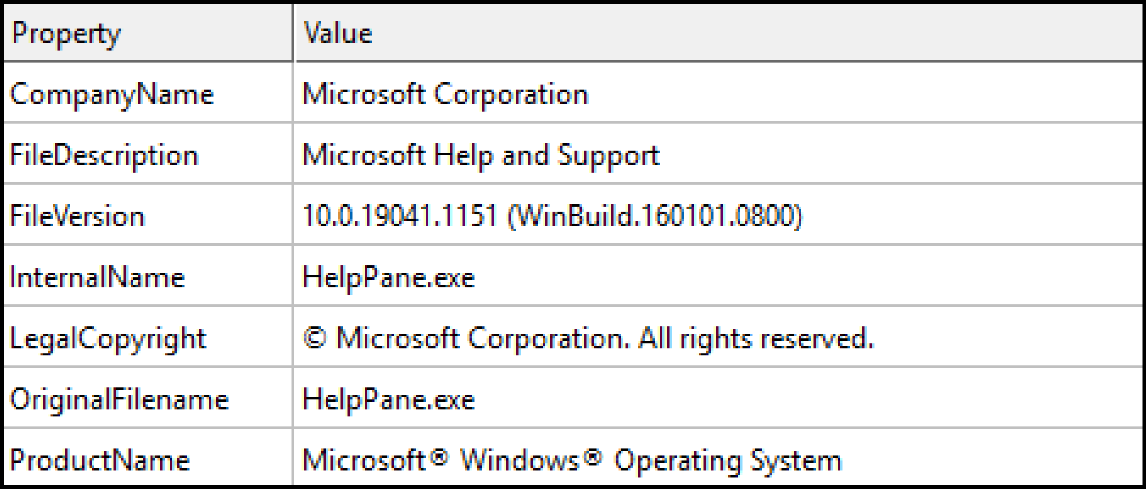
2.2 File Hashes

Dropper File	Drops the main malicious file
Filename	01.exe, nu0rj2ir1.dll, 3vfwzdzfm.dll
MD5	26f9be65373c00e14f21e90a53b23f36
SHA-1	3ec0a7cd02ed8a3575ea02fce967e6047015505b
SHA-256	40c7f0ef1fe74c46cb486b2fb026a547fafd93507ddf0cf0919fdd150c68929a

Dropped File	Main malicious file
Filename	Skc3sk.exe, HelpPane.exe, nld04kvf6.dll, m4kjijaiyjlgkj4ijlkgj.exe
MD5	4d104eed48acba38f9b6544820a00407
SHA-1	8abde557a32b022341153b52288cdcb7ef8c55e4
SHA-256	25a604e9ead508d18b50f379d26b3a2edfd7c395f8fc4298f8fddb4037b332e6

2.3 Version Information

That malware uses ‘HelpPane.exe’ as its internal name, and has file properties that imitate a Windows binary.



Property	Value
CompanyName	Microsoft Corporation
FileDescription	Microsoft Help and Support
FileVersion	10.0.19041.1151 (WinBuild.160101.0800)
InternalName	HelpPane.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	HelpPane.exe
ProductName	Microsoft® Windows® Operating System

Figure 2: File properties

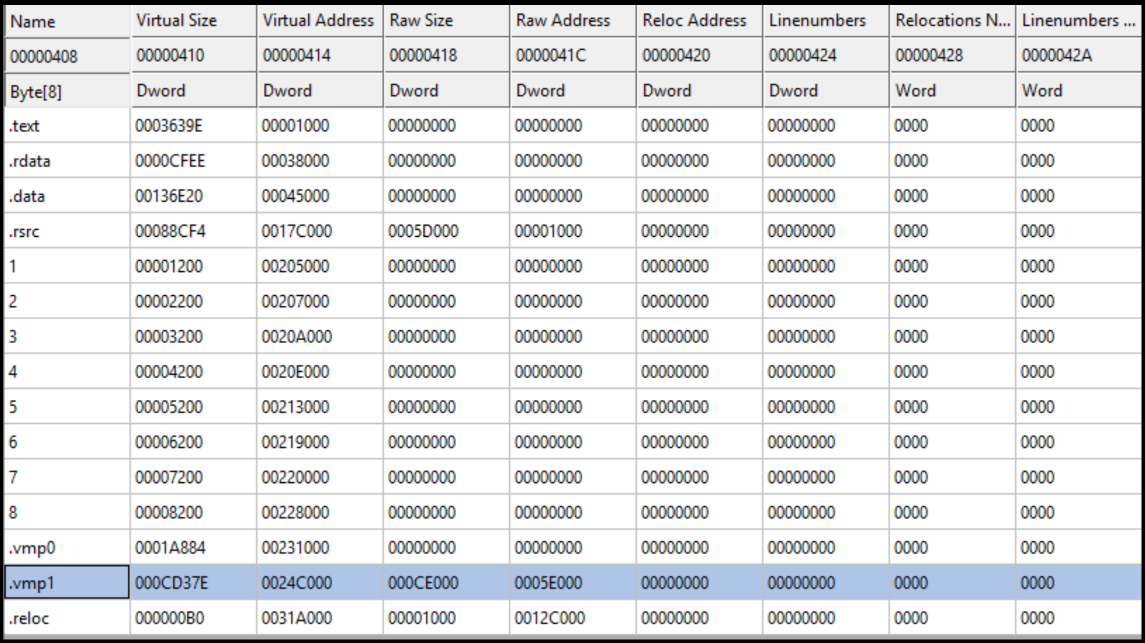
2.4 Section and Entropy Analysis

The PE file contains many zero-sized sections and has an unusual execution entry-point (vmp1).

When the .vmp1 section was compared to the other non-zero sections in terms of entropy, it was found to have a suspiciously high entropy, indicating that it is packed.

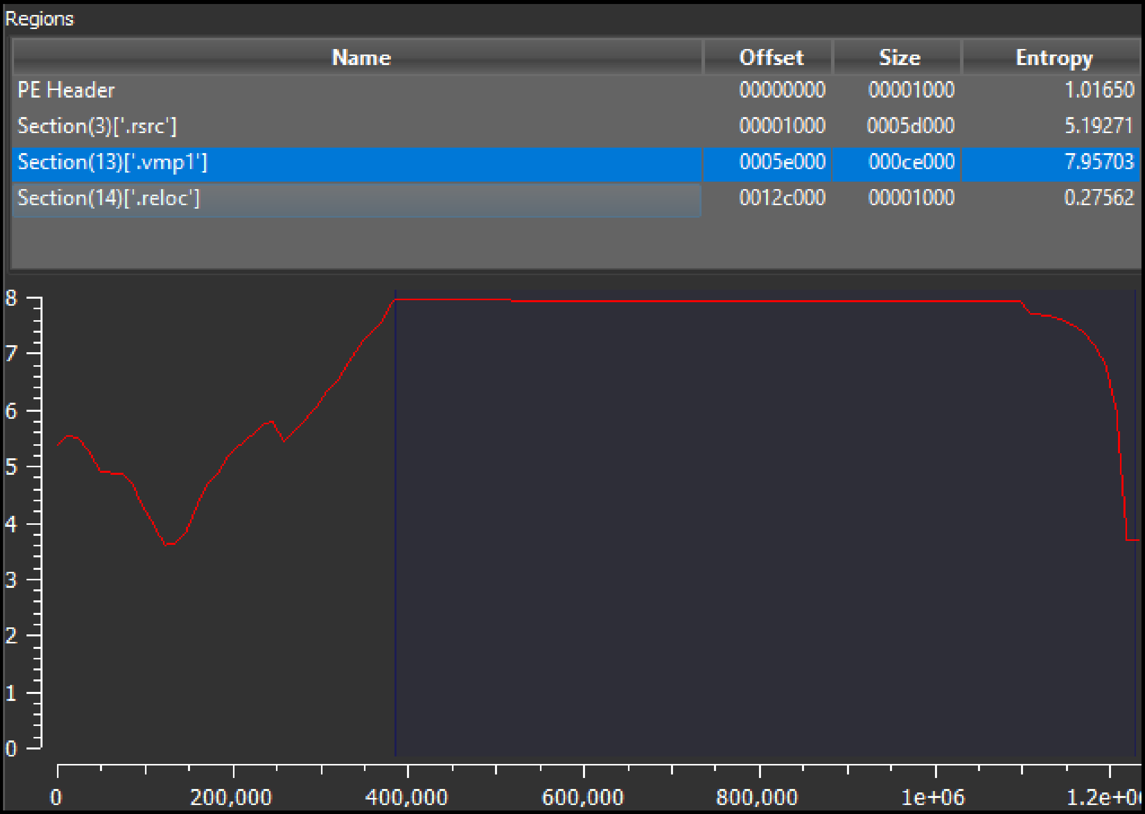
Further analysis has shown that the PE file was packed with VMProtect v1.70.4.

STATIC ANALYSIS



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...
00000408	00000410	00000414	00000418	0000041C	00000420	00000424	00000428	0000042A
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
.text	0003639E	00001000	00000000	00000000	00000000	00000000	0000	0000
.rdata	0000CFEE	00038000	00000000	00000000	00000000	00000000	0000	0000
.data	00136E20	00045000	00000000	00000000	00000000	00000000	0000	0000
.rsrc	00088CF4	0017C000	0005D000	00001000	00000000	00000000	0000	0000
1	00001200	00205000	00000000	00000000	00000000	00000000	0000	0000
2	00002200	00207000	00000000	00000000	00000000	00000000	0000	0000
3	00003200	0020A000	00000000	00000000	00000000	00000000	0000	0000
4	00004200	0020E000	00000000	00000000	00000000	00000000	0000	0000
5	00005200	00213000	00000000	00000000	00000000	00000000	0000	0000
6	00006200	00219000	00000000	00000000	00000000	00000000	0000	0000
7	00007200	00220000	00000000	00000000	00000000	00000000	0000	0000
8	00008200	00228000	00000000	00000000	00000000	00000000	0000	0000
.vmp0	0001A884	00231000	00000000	00000000	00000000	00000000	0000	0000
.vmp1	000CD37E	0024C000	000CE000	0005E000	00000000	00000000	0000	0000
.reloc	000000B0	0031A000	00001000	0012C000	00000000	00000000	0000	0000

Figure 3: Zero-sized file sections



Regions

Name	Offset	Size	Entropy
PE Header	00000000	00001000	1.01650
Section(3)['.rsrc']	00001000	0005d000	5.19271
Section(13)['.vmp1']	0005e000	000ce000	7.95703
Section(14)['.reloc']	0012c000	00001000	0.27562

Figure 4: Section entropies

2.5 Imports

When the file imports were analyzed, the following inferences were made.

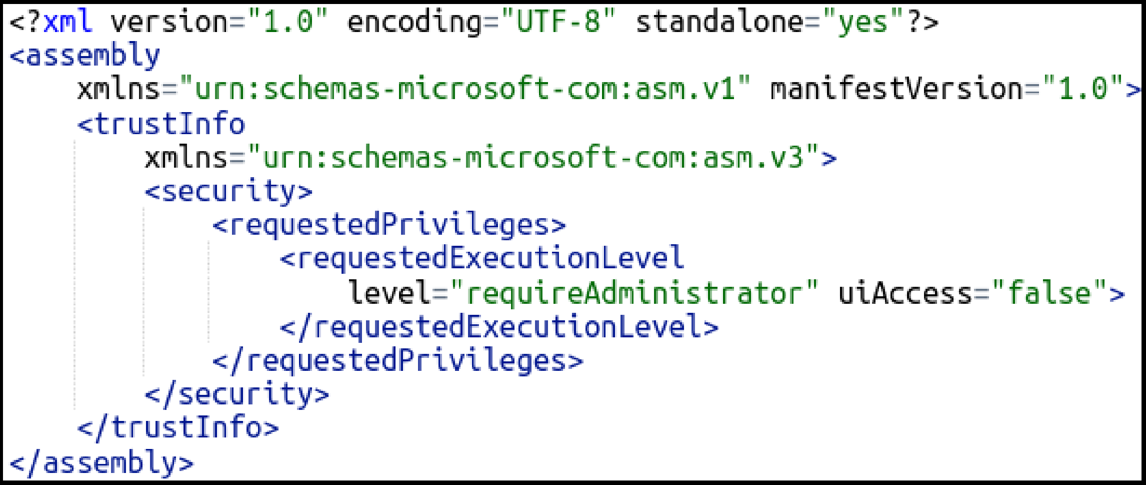
- The malicious file has command execution, and registry access capabilities (ShellExecuteA, RegCloseKey).
- Some imports were used by VmProtect to unpack the file. (GetModuleHandleA, LoadLibraryA, VirtualProtect, GetModuleFileNameA).
- Most of the imports were done dynamically at runtime (LoadLibraryA).
- Malware may have RAT capabilities (GetCursorPos).

SHELL32.dll	ShellExecuteA
USER32.dll	MessageBoxA, GetCursorPos
ADVAPI32.dll	RegCloseKey
KERNEL32.dll	GetModuleHandleA, LoadLibraryA
KERNEL32.dll	VirtualProtect, GetModuleFileNameA, ExitProcess
MFC42.dll	Ord(5875)
MSVCRT.dll	isdigit
GDI32.dll	ExtTextOutA
COMCTL32.dll	ImageListAdd
ole32.dll	CLSIDFromProgID

2.6 Strings

The malicious file has a manifest configuration to run the file as Administrator.

When a standard user starts such a process, the UAC dialog is displayed. That gives the user the opportunity to ask an administrator to provide their credentials.



```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly
    xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
    <trustInfo
        xmlns="urn:schemas-microsoft-com:asm.v3">
        <security>
            <requestedPrivileges>
                <requestedExecutionLevel
                    level="requireAdministrator" uiAccess="false">
                </requestedExecutionLevel>
            </requestedPrivileges>
        </security>
    </trustInfo>
</assembly>
```

Figure 5: File manifest trusted execution level

DYNAMIC ANALYSIS

3.1 Description

Dynamic analysis involves launching a suspicious file into a virtual machine, such as a malware analysis environment, and then examining it to determine what it does. Instead of relying on signatures to identify risk, the file is evaluated based on what it does when executed.

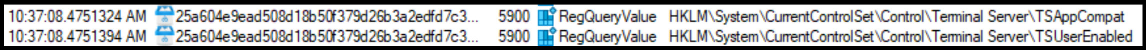
Generated network traffic, process memory, Sysmon logs, and API calls are analyzed during dynamic analysis.

The dynamic analysis process of the suspicious file is detailed below. Only important and useful events were presented.

3.2 Checks Terminal Service (RDP)

The malicious file reads keys related to the terminal service to determine if users can connect to it.

This indicates that adversaries can connect to infected systems using remote services.



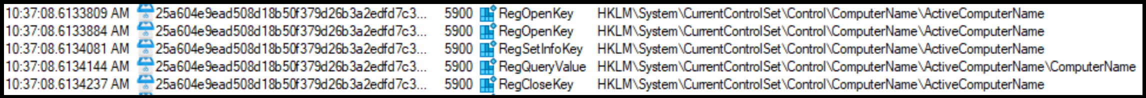
```
10:37:08.4751324 AM  25a604e9ead508d18b50f379d26b3a2edfd7c3...  5900  RegQueryValue  HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
10:37:08.4751394 AM  25a604e9ead508d18b50f379d26b3a2edfd7c3...  5900  RegQueryValue  HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled
```

Figure 6: Accessing terminal service-related keys

Key Definitions	
TSAppCompat	Indicates whether the system is running in application compatibility mode.
TSUserEnabled	Indicates whether users can log on to the terminal server.

3.3 Gathers Computer Name

The malicious file reads registry keys that contain the computer name.



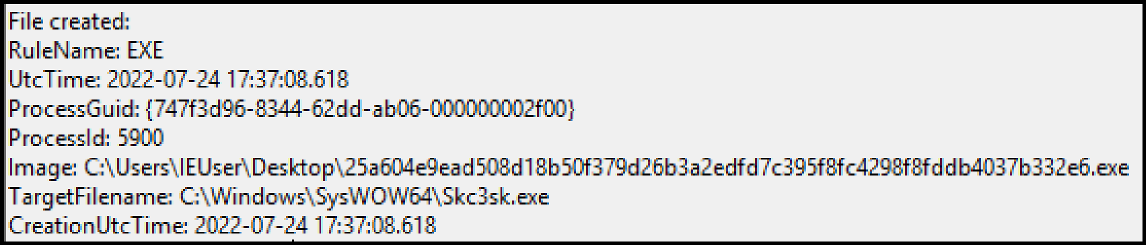
```
10:37:08.6133809 AM  25a604e9ead508d18b50f379d26b3a2edfd7c3...  5900  RegOpenKey     HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
10:37:08.6133884 AM  25a604e9ead508d18b50f379d26b3a2edfd7c3...  5900  RegOpenKey     HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
10:37:08.6134081 AM  25a604e9ead508d18b50f379d26b3a2edfd7c3...  5900  RegSetInfoKey  HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
10:37:08.6134144 AM  25a604e9ead508d18b50f379d26b3a2edfd7c3...  5900  RegQueryValue  HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName
10:37:08.6134237 AM  25a604e9ead508d18b50f379d26b3a2edfd7c3...  5900  RegCloseKey    HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
```

Figure 7: Accessing keys to read computer name

3.4 Copy File Under Windows Directory

The malicious file copies itself to C:\Windows\SysWOW64\Skc3sk.exe.

Further analysis found that this file will be used for persistence later on. The created file has the same hash value as the first executed file; therefore they are completely the same files.



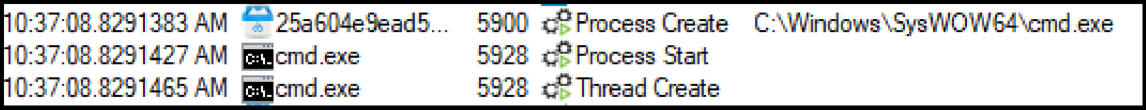
```
File created:
RuleName: EXE
UtcTime: 2022-07-24 17:37:08.618
ProcessGuid: {747f3d96-8344-62dd-ab06-000000002f00}
ProcessId: 5900
Image: C:\Users\IEUser\Desktop\25a604e9ead508d18b50f379d26b3a2edfd7c395f8fc4298f8fddb4037b332e6.exe
TargetFilename: C:\Windows\SysWOW64\Skc3sk.exe
CreationUtcTime: 2022-07-24 17:37:08.618
```

Figure 8: Accessing keys to read computer name

3.5 Spawning Command Shell and Self Deletion

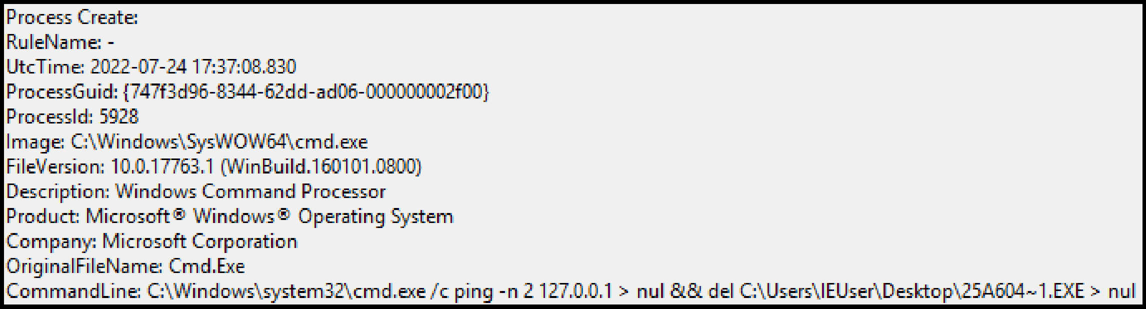
After copying itself, the first executed binary runs cmd.exe with C:\Windows\system32\cmd.exe /c ping -n 2 127.0.0.1 > nul && del C:\Users\IEUser\Desktop\25A604~1.EXE > nul command and deletes itself.

The following figures show the details of this execution.



```
10:37:08.8291383 AM  25a604e9ead5...  5900  Process Create  C:\Windows\SysWOW64\cmd.exe
10:37:08.8291427 AM  cmd.exe          5928  Process Start
10:37:08.8291465 AM  cmd.exe          5928  Thread Create
```

Figure 9: Spawning cmd and ping



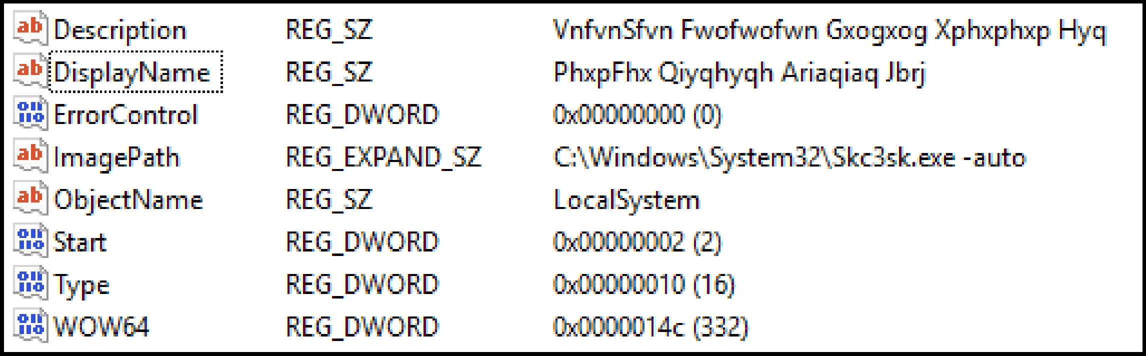
```
Process Create:
RuleName: -
UtcTime: 2022-07-24 17:37:08.830
ProcessGuid: {747f3d96-8344-62dd-ad06-000000002f00}
ProcessId: 5928
Image: C:\Windows\SysWOW64\cmd.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: C:\Windows\system32\cmd.exe /c ping -n 2 127.0.0.1 > nul && del C:\Users\IEUser\Desktop\25A604~1.EXE > nul
```

Figure 10: Executed cmd command

3.6 Persistence

Skc3sk.exe is added itself to the startup services for persistence with the service name SkGcskb Tlctl, but sets DisplayName as PhxpFhx Qiyqhyqh Ariaqiaq Jbrj.

These names were not generated dynamically, and were the same for each execution.

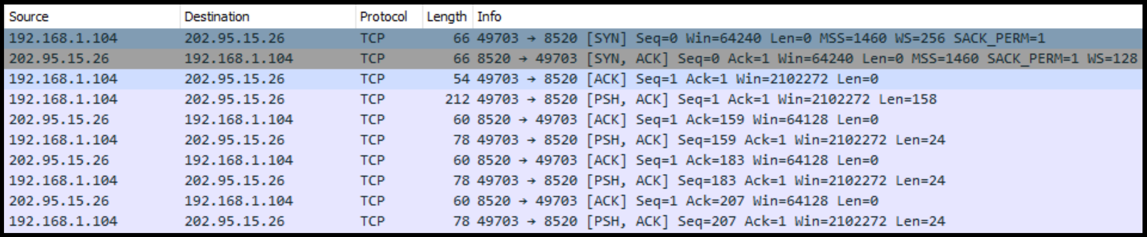


Description	REG_SZ	VnfvnSfvn Fwofwofwn Gxogxog Xphxphxp Hyq
DisplayName	REG_SZ	PhxpFhx Qiyqhyqh Ariaqiaq Jbrj
ErrorControl	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	C:\Windows\System32\Skc3sk.exe -auto
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)
WOW64	REG_DWORD	0x0000014c (332)

Figure 11: Adding service for persistence

3.7 Network Traffic

The process connects to 8520 port of 202.95.15.26. Since this IP was not online during the analysis, the outgoing traffic was redirected to a Netcat listener and obtained the outgoing traffic.



Source	Destination	Protocol	Length	Info
192.168.1.104	202.95.15.26	TCP	66	49703 → 8520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
202.95.15.26	192.168.1.104	TCP	66	8520 → 49703 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
192.168.1.104	202.95.15.26	TCP	54	49703 → 8520 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
192.168.1.104	202.95.15.26	TCP	212	49703 → 8520 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=158
202.95.15.26	192.168.1.104	TCP	60	8520 → 49703 [ACK] Seq=1 Ack=159 Win=64128 Len=0
192.168.1.104	202.95.15.26	TCP	78	49703 → 8520 [PSH, ACK] Seq=159 Ack=1 Win=2102272 Len=24
202.95.15.26	192.168.1.104	TCP	60	8520 → 49703 [ACK] Seq=1 Ack=183 Win=64128 Len=0
192.168.1.104	202.95.15.26	TCP	78	49703 → 8520 [PSH, ACK] Seq=183 Ack=1 Win=2102272 Len=24
202.95.15.26	192.168.1.104	TCP	60	8520 → 49703 [ACK] Seq=1 Ack=207 Win=64128 Len=0
192.168.1.104	202.95.15.26	TCP	78	49703 → 8520 [PSH, ACK] Seq=207 Ack=1 Win=2102272 Len=24

Figure 12: Network connection

MEMORY ANALYSIS

4.1 Description

Memory analysis is frequently used in malware analysis and digital forensics. Describes the process of examining a memory image that has been dumped from a targeted computer after the malware has been executed to retrieve a variety of artifacts, such as a list of processes and their related threads.

During memory analysis, many artifacts were found indicating that this malicious file is a variant of Gh0st RAT, there was also evidence showing that the malware downloads and uses Mimikatz.

4.2 Indicators of Zergost (Gh0st) Rat

The following strings were found within the process memory which strongly indicates that this malicious file is a variant Gh0st RAT. Reference.

- F:\hidden-master\x64\Debug\QAssist.pdb
- 6gkIBfkS+qY=
- c7b262cbb783f5efc855fb95ea73cdde
- <H1>403 Forbidden</H1>
- /jump?clientuin=%s&keyindex=9&pt_aid=715030901&daid=7

4.3 Indicators of Mimikatz

The following string was found within the process memory indicating the use of the mimikatz by the process.

- GetMP privilege::debug sekurlsa::logonpasswords exit

4.4 Malicious Dynamic Imports

There were many import names as a string within the process memory, these libraries can be dynamically imported during the execution process. These imports are other indicators that show this process has RAT capabilities.

CreateRemoteThread OpenFile GetKeyboardState SetCapture MessageBeep SetCursor LoadCursorW GetCursorPos GetKeyboardLayoutList

4.5 AV Names Inside Memory

The malicious process memory has many AV name strings, which shows that the malicious process is probably checking for AV solutions present on the computer.

This is also another indicator of Zegost RAT. Reference.

UnThreat.exe vsserv.exe knsdtray.exe avgwdsvc.exe Comodo K7TSecurity.exe remupd.exe NOD32 AYAgent.aye cfp.exe Ad-watch rtvscan.exe egui.exe V3Svc.exe mssecess.exe ad-watch.exe Avast Mcshield.exe Outpost QuickHeal PSafe ashDisp.exe avp.exe acs.exe QUHLPSVC.EXE PSafeSysTray.exe avcenter.exe F-Secure DR.WEB RavMonD.exe BitDefender TMBMSRV.exe f-secure.exe SPIDer.exe KvMonXP.exe baiduSafeTray.exe BaiduSd.exe HipsTray.exe QQPCRTP.exe KSafeTray.exe kxetray.exe 360sd.exe 360tray.exe.

THREAT ANALYSIS

5.1 APT Behavior

The Gh0st RAT variants are commonly used by Chinese APT groups. It is still unknown which APT group is behind these persistent attacks. The main goal is to infect high-value targets where they can obtain intelligence or make financial gain.

The analysis shows that malware with very similar traits began to spread in 2020, and continued to spread persistently until 2022.

You can find some samples below:

- 19-10-2020
- 17-11-2020
- 09-01-2021
- 22-02-2021
- 20-07-2022

All samples use a Gh0st RAT, possibly Zergost malware as their final payload, and all droppers have similar behavior by calling cmd.exe, copying the malicious one to the Windows folder, adding the malicious one to startup with administrator rights with similar parameters, and has Mimikatz signatures (which is not present in the open-source version of Gh0st RAT).

Almost all C2 IP addresses were using the same hosting provider.

In addition, the malware used is similar to that used by APT27 a.k.a. Iron Tiger in Operation PZChao. However, this does not mean that the threat group is APT27.

5.2 MITRE Mapping

Malicious uses the following MITRE TTP Values:

Execution:T1106	Functionality to dynamically determine API calls
Execution:T1569.002	Modify Windows services
Persistence:T1543.003	Persistence using Windows services
Defence Evasion:T1562.001	Changes security center settings
Defense Evasion:T1140	Uses string encryption-decryption
Defense Evasion:T1036	Copies itself to system directory
Discovery:T1012	Reads-Modifies Registry Keys
Discovery:T1518.001	Scans for AV solutions
Collection:T1056	Captures and logs keystrokes
Command and Control:T1573	Encrypted communication
Command and Control:T1571	Non-standart port

5.3 IOC Values

Registry:

- HKLM\System\CurrentControlSet\Services\SkGcskb Tlctl ImagePath = C:\Windows\SysWOW64\Skc3sk.exe -auto

Executed commands:

- C:\Windows\system32\cmd.exe /c ping -n 2 127.0.0.1 > nul && del C

Inside process memory:

- F:\hidden-master\x64\Debug\QAssist.pdb
- 6gkIBfkS+qY=
- c7b262cbb783f5efc855fb95ea73cdde
- /jump?clientuin=%s&keyindex=9&pt_aid=715030901&daid=7
- GetMP privilege::debug sekurlsa::logonpasswords exit

REFERENCES

REFERENCES

- gbhackers.com
- CyberMonitor
- etutorials.org
- safeguardcyber.com
- nccgroup.com
- g-soft.info
- joesandbox.com
- ctfiot.com
- joesandbox.com
- mitre.org
- securityaffairs.co
- cyware.com
- fortinet.com
- joesandbox.com

THANK YOU FOR CHOOSING

HALBORN