Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware

trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

April 9, 2021

APT & Targeted Attacks

This blog details how Iron Tiger threat actors have updated their toolkit with an updated SysUpdate malware variant that now uses five files in its infection routine instead of the usual three.

By: Daniel Lunghi, Kenney Lu April 09, 2021 Read time: (words)

Update as of April 27, 2021, 7 A.M. E.T.: We've updated the "Rootkits From a Public Repository" section and the appendix to include a second sample.

More than a year after Operation DRBControl, a campaign by a cyberespionage group that targets gambling and betting companies in Southeast Asia, we found evidence that the Iron Tiger threat actor is still interested in the gambling industry.

This blog details how Iron Tiger threat actors have updated their toolkit with an updated SysUpdate malware variant that now uses five files in its infection routine instead of the usual three. We also provide details on Iron Tiger's possible connections to other threat actors based on similar tactics, techniques, and procedures (TTPs) we've observed. Finally, we describe some of the rootkits that Iron Tiger is using, one of which is used to hide files at the kernel level, and has not been previously reported as being used by this threat actor.

A Look at the Iron Tiger Threat Group

In 2019, Talent-Jump, Inc., a security service and system integration company, discovered several malware variants in a gambling company during an incident response operation and sought our help for further investigation and analysis.

In 2020 and 2021, Talent-Jump found new samples for malware families that are attributed to the Iron Tiger threat actor, which is also referred to as LuckyMouse, EmissaryPanda, and APT27.

While investigating Operation DRBControl in 2019, we found several connections to multiple threat actors:

- Iron Tiger, which uses the HyperBro trojan and some infrastructure links
- Winnti, which uses the same infrastructure and code-sharing links detailed in our paper
- Bronze President, a threat actor that targets non-governmental organizations (NGOs). Back in 2019, we named a malware family, which we believed was new, as "Type 2."

However, after the publication of our report, we learned that the Type 2 malware family described in our report was the same as the "RCSession" malware family that Dell Secureworks described in a blog that they published in December 2019.

After finding multiple tools belonging to the Iron Tiger threat actor (which we now track as Earth Smilodon), it is likely that the new malware families that we found during the Operation DRBControl investigation came from the same threat actor.

New Version of SysUpdate Malware

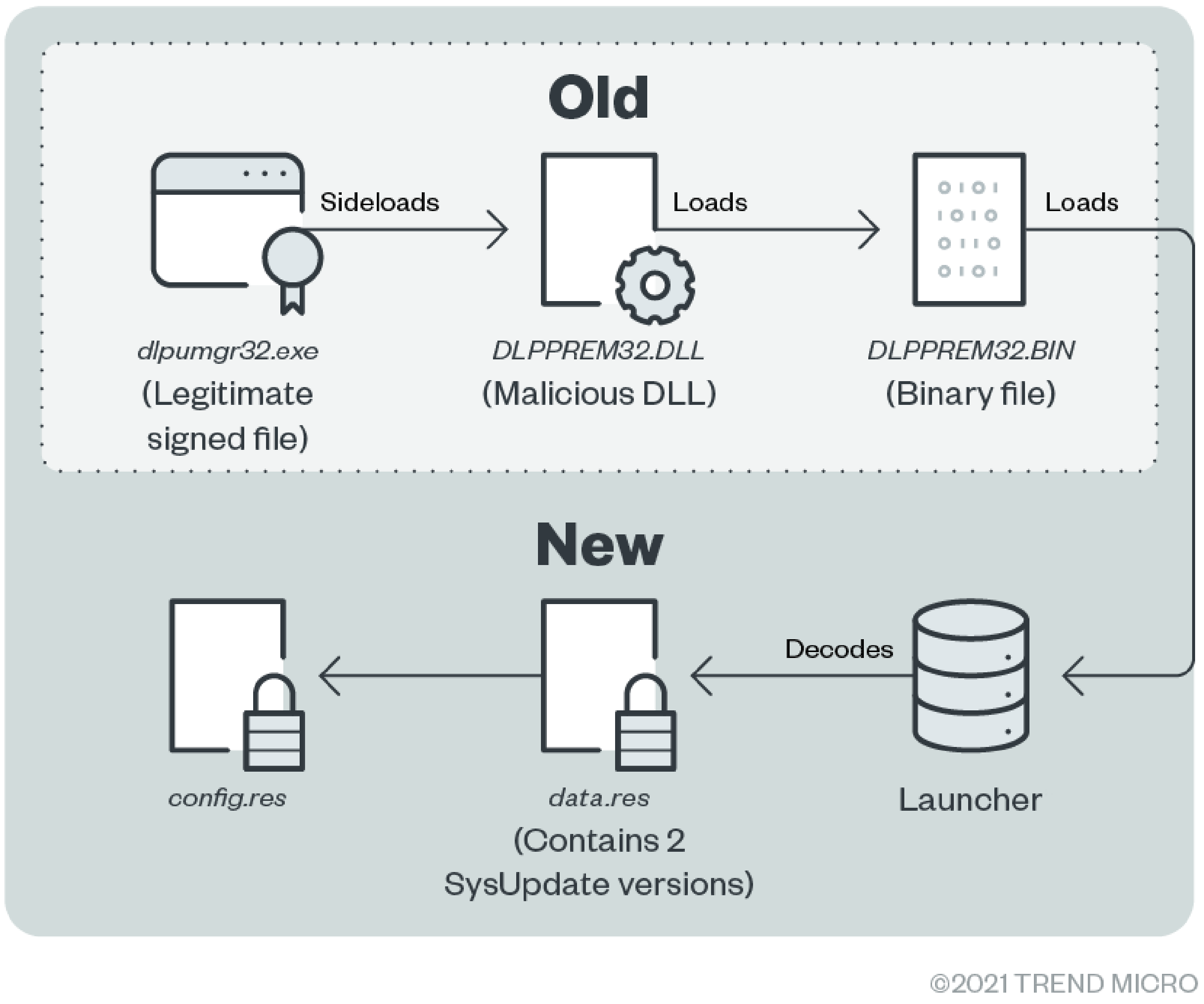


Figure 1. The old and new SysUpdate infection chains
In December 2020, we found a sample that we identified as one belonging to the SysUpdate malware family, also named Soldier, FOCUSFJORD, and HyperSSL. SysUpdate was first described by the NCC Group in 2018.

In the past, SysUpdate was loaded in memory by a known method involving three files:

- One legitimate executable, sometimes signed, and vulnerable to dynamic-link library (DLL) sideloading
- One malicious DLL loaded by the legitimate file
- One binary file usually containing obfuscated code, unpacked in memory by the malicious DLL

An additional executable that serves as a launcher is loaded in memory, which then loads the final SysUpdate payload. Based on our investigation, instead of the usual three files, the threat actor used five:

- *dlpumgr32.exe*, a legitimate signed file that belongs to the DESlock+ product

- *DLPPREM32.DLL*, a malicious DLL sideloaded by dlpumgr32.exe that loads and decodes *DLPPREM32.bin*
- *DLPPREM32.bin*, a shellcode that decompresses and loads a launcher in memory
- data.res, an encrypted file decoded by the launcher and contains two SysUpdate versions: one for a 32-bit architecture and another for a 64-bit architecture
- config.res, an encrypted file decoded by the launcher and contains the SysUpdate configuration, such as the command-and-control (C&C) address

Analysis of the Updated Tool: The Launcher

In summary, the launcher acts as an installer — it will copy the malware to a fixed place and ensure that it runs during the next boot of the infected host. In detail, this process involves multiple steps.

The launcher starts by instantiating the *CLoadInfo* object, which has the following structure:

Offset	Description	Hardcoded values in our sample
0	VTable of CLoadInfo class	
4	Directory to copy all files	%PROGRAMDATA%\Test\
8	Name of the legitimate executable	*dlpumgr32.exe*
12	Name of the sideloaded DLL	*DLPPREM32.DLL*
16	Name of the shellcode	*DLPPREM32.bin*
20	Name of the encrypted payload	*data.res*
24	MD5 of the encrypted payload	e43e40416520dab5b4c44ac8af907078
28	Name of the encrypted configuration	*config.res*
32	Name of the registry key value	*servTest*
36	Name of the service DisplayName	*Servdisplay*

Table 1. *CLoadInfo* object structure

The launcher's behavior changes depending on the number of arguments passed to the executable. It's important to highlight that the change of behavior only depends on the number of arguments, and not the content:

- **No argument**. If there is no argument, a hardcoded directory will be created wherein all the files will be copied. *The CreationTime, LastWriteTime,* and *LastAccessTime* will be updated according to the C:\Windows\system32\kernel32.dll file and their file attributes will be set to "hidden" and "system". Windows Management Instrumentation (WMI) will be used to run dlpumgr32.exe with arguments **"-up -run -x"** and it will exit the current process.
- **One argument**. It will skip the decoding of the configuration and persistence setup, and will perform the same behavior as one with three arguments.
- **Three arguments.**
    - The launcher first decrypts the config.res file with a hardcoded Data Encryption Standard (DES) key. It encodes it using another key and writes it to the registry key "**Software\Classes\scConfig**" (**HKEY_LOCAL_MACHINE** or **HKEY_CURRENT_USER** hive, depending on the privileges of the process).
    - After decrypting the configuration, the *config.res* file is deleted.
    - Depending on the privileges of the process, the malware will add a value to the "**Software\Microsoft\Windows\CurrentVersion\Run**" key, or it will create a service that runs the malware at boot time
    - The launcher decrypts the data.res file with a different hardcoded DES key. The result is a file with the following structure:

Size of the 32-bit shellcode
32-bit shellcode
Size of the 64-bit shellcode
64-bit shellcode

Table 2. Structure of decrypted data.res file

Lastly, the launcher starts a suspended process with the command line "**C:\Windows\system32\svchost.exe -k LocalServices,**"and injects the appropriate shellcode into it (either 32- or 64-bit). It will then resume the newly created process and exit the current process.

The following diagram summarizes the launch procedure:

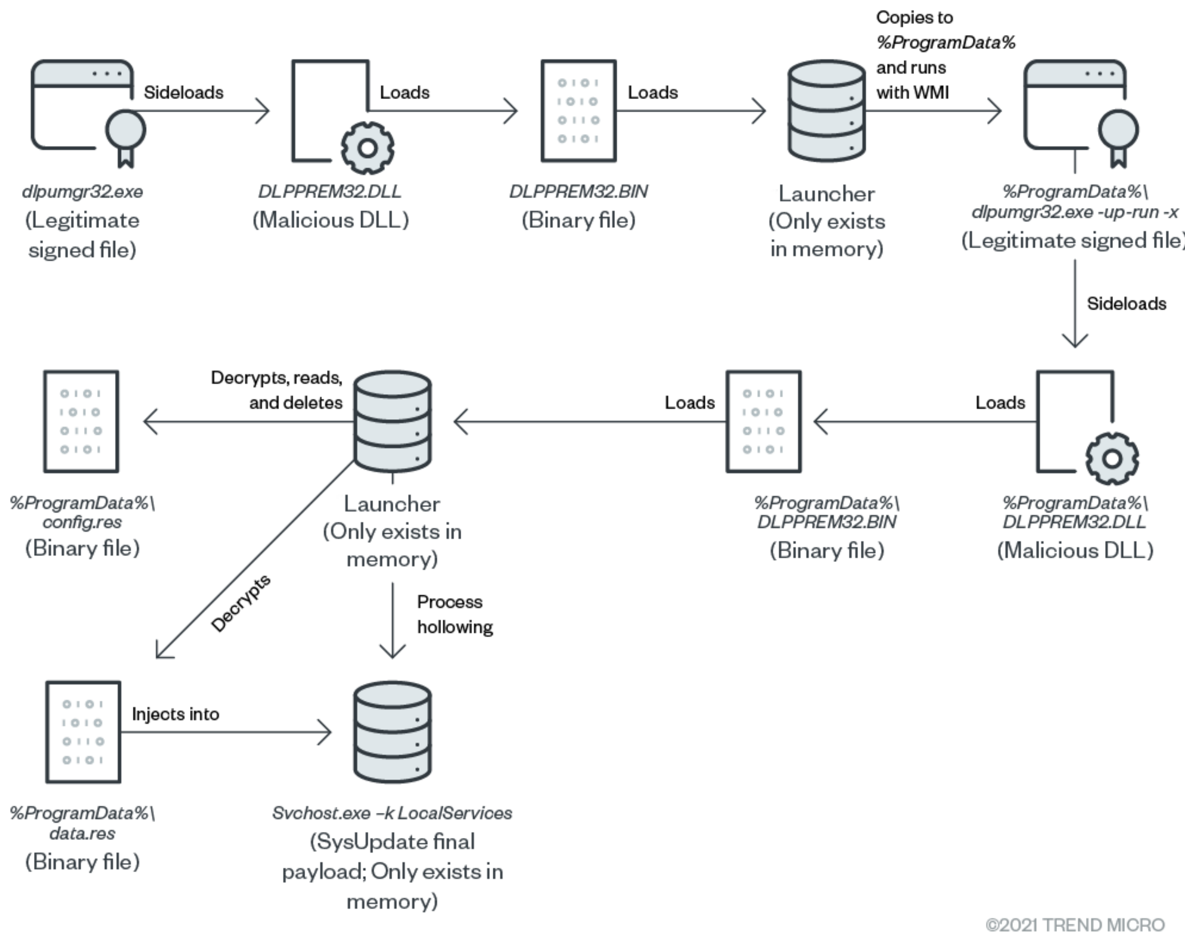

Sideloads
Loads
Loads
Copies to %ProgramData% and runs with WMI
dlpumgr32.exe (Legitimate signed file)
DLPPREM32.DLL (Malicious DLL)
DLPPREM32.BIN (Binary file)
Launcher (Only exists in memory)
%ProgramData%\ dlpumgr32.exe -up-run -x (Legitimate signed file)
Sideloads
Loads
Loads
Decrypts, reads, and deletes
%ProgramData%\ config.res (Binary file)
Launcher (Only exists in memory)
%ProgramData%\ DLPPREM32.BIN (Binary file)
%ProgramData%\ DLPPREM32.DLL (Malicious DLL)
Decrypts
Process hollowing
Injects into
%ProgramData%\ data.res (Binary file)
Svchost.exe –k LocalServices (SysUpdate final payload; Only exists in memory)
©2021 TREND MICRO

Figure 2. The launch procedure of the updated tool

The payload itself is a new version of SysUpdate.

Analysis of the Payload

The features of the updated SysUpdate payload look similar to its previous versions. We observed that the C++ code is structured around classes, many of which have self-explanatory names. Some of these classes, such as *CCompress, CIOStreamIF,* or *CTcpSocket,*have been present in the older versions of SysUpdate and compiled near the end of 2015.

Others have been in existence for many years, such as *TPacket, SCM Client, SystemInfo, CMD5, CIOStream,* and *CInfo***.** Some of them are newer and have been developed in 2020, such as *ConfigReg, CWorkQueue, WindowsEvent,* and *CEncoder* or *cudp.*

The sample we've analyzed contained many new and unique classes that featured a particular naming convention. The names of classes are mostly self-explanatory, and the manner in which the classes have been organized is probably the result of a framework developed by our threat actor.

Some of the classes' names start with "H" (*HControl, HSleep,* and *HTrans*), "I" (*IAgent, ITcpAgent,* and *IAgentListener*), "T" (*TCommon, TFileInfo, TFileRename, TFileUpload, TServicesInfo, TListUser,* and *TTransmit),* "C" (*CSSLAgent, CSocks5,* and *CTcpAgent*) or "CM" (*CMCapture, CMFile, CMPipeClient, CMPipeServer, CMProcess, CMServices,* and *CMShell).*

The communication is made via a named pipe (in our case, it's **"\\.\pipe\testPipe"**). Multiple features that are expected of an espionage backdoor are present in the sample. These include a screenshot feature, file management functions (such as search, delete, move, upload, and download), process and services management, and command execution.

It should be noted that we also found recent samples of the SysUpdate backdoor that do not implement these "new" classes. This suggests that different groups (or subgroups of Iron Tiger) are also using this malware family in their attacks.

Pandora Backdoor

On two occasions (in March and October 2020), we found a kernel rootkit that had been deployed. After analysis, it appears that this rootkit's behavior is very similar to that of the NDISProxy driver and remote access trojan (RAT). The version we found is slightly different — the driver isn't digitally signed but instead utilizes a known exploit to bypass Windows Driver Signature Enforcement (DSE) protection and load the driver directly into the system.

We chose to call it "Pandora" based on the program database (PDB) path of the unpacked stage 2, which is "**F:\Pandora\x\drv(32-64)\bin\src\drvx64.pdb.**"

The rootkit has multiple stages before getting to the actual payload:

Stage 1

- Grants system privileges via Windows services
- Uses DLL sideloading technique to evade security solutions
- Starts and injects code to a new *svchost* process to prevent tracking

Stage 2

- Utilizes a known vulnerability (CPU-Z CVE-2017-15303) that allows it to read and write into physical memory and read CPU control registers to turn the DSE off. This is done in conjunction with the Process Monitor driver (**procxp152.sys**), both of which are dropped upon loading the rootkit, even if they are not originally installed in the machine.
- Loads **"drvx64.sys,"** a crafted Windows Presentation Foundation (WPF) driver

Stage 2 - Driver

- Registers WPF callback and filters incoming traffic with a predefined token

- Injects final payload into "**lsass.exe**"

Stage 3 - Final Payload

- Installs itself as a Windows service
- Sets a specific keyword for communication
- Exchanges messages and commands with the kernel driver
- Performs backdoor functions

Each backdoor has a different token that is encrypted in the registry. If the incoming traffic contains a token and is in the HTTP format, the backdoor will intercept the traffic and process the command. In the version that we've analyzed, the installer writes the token in the registry key. We can't trigger the backdoor without a current token, which makes the backdoor more difficult to find and analyze.

Sample	Token	Mutex	Semaphore
Pandora 20200310	FHHqw@nF4Jo0vPAU180IP5h9umnd4KFi	ENDnetfilter	234netfilter
Pandora 20201010	Qp$zo&FgPBjGhm(.LGi_&j~tmhMO08)	ENDdsfsfs	xwwadsfsfs

Table 3. Pandora backdoor samples with different tokens

Based on our analysis, the Pandora backdoor contains more public code repositories compared with previous versions.

Feature	Name	Repository
Driver memory injection	Blackbone	https://github.com/DarthTon/Blackbone
NDIS network filtering driver	WFP Sample	"WDK\Windows Filtering Platform Stream Edit Sample/C++/sys/stream_callout.c"
Parse HTTP packets	HTTP Parser	https://github.com/nodejs/http-parser
Turn off DSE	StryKer	https://github.com/hfiref0x/Stryker

Encrypted Communication	D3DES	https://gitlab.gnome.org/GNOME/gtk-vnc/-/blob/v0.1.0/src/d3des.c
Compression	QuickLZ	https://github.com/robottwo/quicklz

Table 4. Pandora’s public code repositories

Rootkits From a Public Repository

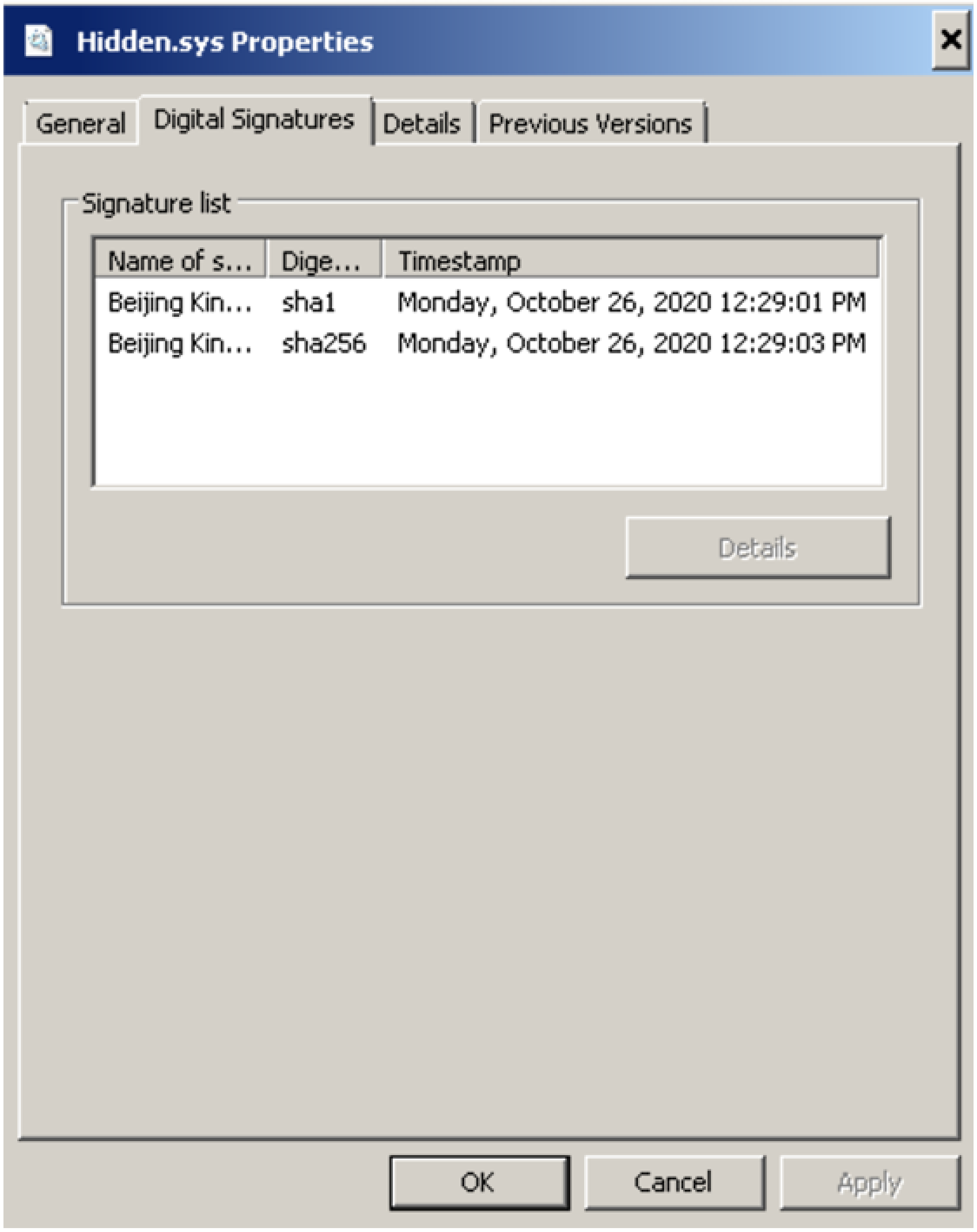
We found two different rootkits that are being used for hiding processes, files, and services.

Both of them were taken from a public Github repository whose authors are not associated with the threat actor.

Hidden.sys - https://github.com/JKornev/hidden/tree/master/

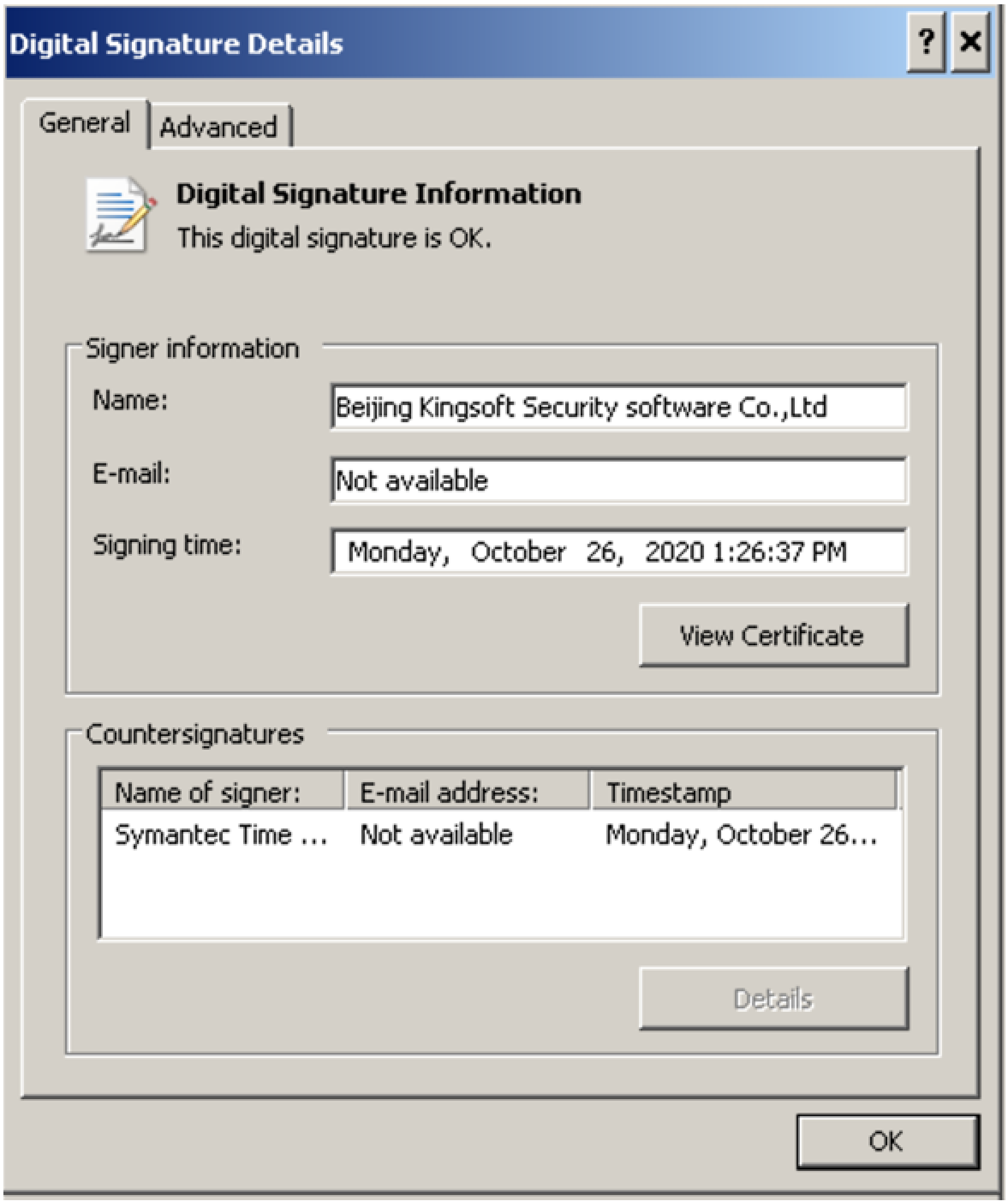
The first sample was found in April 2020. The driver was not signed and used the same DSE exploit that the Pandora backdoor uses for it to load.

The second sample was found in October 2020 and was signed by a legitimate certificate from Beijing Kingsoft Security Software Co., Ltd., a Chinese security software company. The certificate has been valid since February 2020. We have communicated with Kingsoft Corporation Limited regarding this issue and they have confirmed that as of writing, the certificate has already been voided.


Hidden.sys Properties

Signature list

Name of s…	Dige…	Timestamp
Beijing Kin…	sha1	Monday, October 26, 2020 12:29:01 PM
Beijing Kin…	sha256	Monday, October 26, 2020 12:29:03 PM


Digital Signature Details

General | Advanced

Digital Signature Information

This digital signature is OK.

Signer information

Name:	Beijing Kingsoft Security software Co.,Ltd
E-mail:	Not available
Signing time:	Monday, October 26, 2020 1:26:37 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	Monday, October 26...

Figure 3.

Hidden.sys properties and digital signature details

The tool is used to hide the threat actors' tools and services. The tool's configuration was added to registry run keys on a victim's computer.

Hidden Registry/Folder/File

Type	Value
REG	HKLM\SYSTEM\CurrentControlSet\services\HiddenService

REG	HKLM\SYSTEM\CurrentControlSet\services\servTest
REG	HKLM\SYSTEM\CurrentControlSet\services\TrkWkss
Folder	C:\programdata\vlc
File	C:\programdata\vlc\vlc.exe
Folder	C:\programdata\test
File	C:\programdata\test\dlpumgr32.exe
File	C:\windows\system32\drivers\Hidden.sys
File	C:\windows\system32\HiddenService.exe

Table 5. The tool's configuration

The references to "Hidden" are related to the rootkit itself. The "**dlpumgr32.exe**" and "servTest" lines are related to the new version of SysUpdate which we described earlier.

We do not know which malware variant is being sideloaded by **vlc.exe**. It is probably installed as a service named "**TrkWkss.**" We found a SysUpdate sample compiled in November 2020 that abuses a DLL sideloading vulnerability in VLC (see IOC list). This confirms that this threat actor is abusing this legitimate program to sideload its backdoors.

HyperBro Malware Family

The Iron Tiger APT group has used the HyperBro malware family since at least 2017. It is the evolved version of HttpBrowser, which the group has been using since at least 2015.

We found earlier versions of this malware that were sideloaded by malicious DLL files that unpacked and loaded a binary file named **"thumb.db"** in memory. All the requests were sent to the C&C server on port 443, with "**/ajax**" as the uniform resource identifier (URI).

While investigating Operation DRBControl, we found an updated version of this malware family that implements some new classes. We provided a detailed analysis of this new HyperBro version in our research.

We also discovered that the binary file that's being unpacked and loaded in memory by malicious DLL files is named "**thumb.dat.**" We also saw that all requests sent to the C&C server were sent to the URI "**/api/v2/ajax**" on port 443.

Since we analyzed that single sample, we found several new samples that matched the newer behavior, some of which have been deployed in our gambling target.

However, we continue seeing samples that feature the "older" behaviors, which suggests that different groups — or possibly subgroups of Iron Tiger — are using this malware family. Some of these samples match the target and behavior listed by ESET in their blog.

FRP Tool

We found the FRP tool being used on a Linux host, which is similar to Avast's findings in a report that they published on the Iron Tiger threat actor.

The FRP tool that we analyzed was a modified version, which was possibly copied off of Github.

Type 1 Malware Family

We found three new samples of the Type 1 malware family that abuses Dropbox as a secondary C&C channel, which we described in our Operation DRBControl whitepaper.

Apart from a modification in the malware sample's configuration (which happened after we published our paper), the differences with the versions that we analyzed in 2019 are minor. The version numbering was at 11.0, while the last sample we analyzed in August 2019 was at version number 9.0. This shows that the development is still active.

On the infrastructure side, we observed that the threat actor switched from using IP addresses hosted on the Google Cloud Platform (GCP) to IP addresses hosted on Microsoft Azure.

It should be noted that after our blog publication in February 2020, the threat actor compiled new Type 1 malware samples using a new configuration, which prevented us from closely monitoring their operations. We believe that this was a direct reaction to our research, suggesting that the threat actor read our investigation.

It's also important to note that the compilation timestamp of the sideloaded DLLs were set a few months in advance. For example, the binaries that we found in March and April 2020 had an August 26, 2020 compilation date. This is consistent with the behavior that we noticed during Operation DRBControl, wherein some binaries that have been found in mid-2019 had a compilation date of March 4, 2020. This shows that the threat actors intended to confuse forensics investigators with incorrect timestamps, which is why it's critical to analyze timestamps with caution during investigations.

Infection Vector

We could not confirm the primary infection vector. However, traces of the exploitation of the Microsoft Exchange vulnerability CVE-2020-0688 were found.

Multiple infection vectors have been attributed to this threat actor in the past:

- Watering holes
- Weaponized documents exploiting the Dynamic Data Exchange (DDE) method
- Weaponized documents exploiting the CVE-2018-0798 vulnerability in Equation Editor
- Exploitation of the CVE-2019-0604 vulnerability in Sharepoint
- Supply chain attack that compromises a chat software installer, Able Desktop
- Exploitation of recent vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) in Microsoft Exchange Server

During our investigation, we found some old samples that fit in these categories but have not been reported. They are unrelated to this campaign and can be found in our IOC list.

Targets

The closer look into Iron Tiger was prompted because of an incident response investigation involving a Philippine-based gambling company that the group targeted. True to form, the Iron Tiger threat actor has targeted the same company for 18 months.

Aside from targeting the same company, Iron Tiger also targeted other countries and industries. Over the past 18 months, we observed how the group targeted governments, banks, telecommunication providers, and even the energy sector in the Middle East and Southeast Asia.

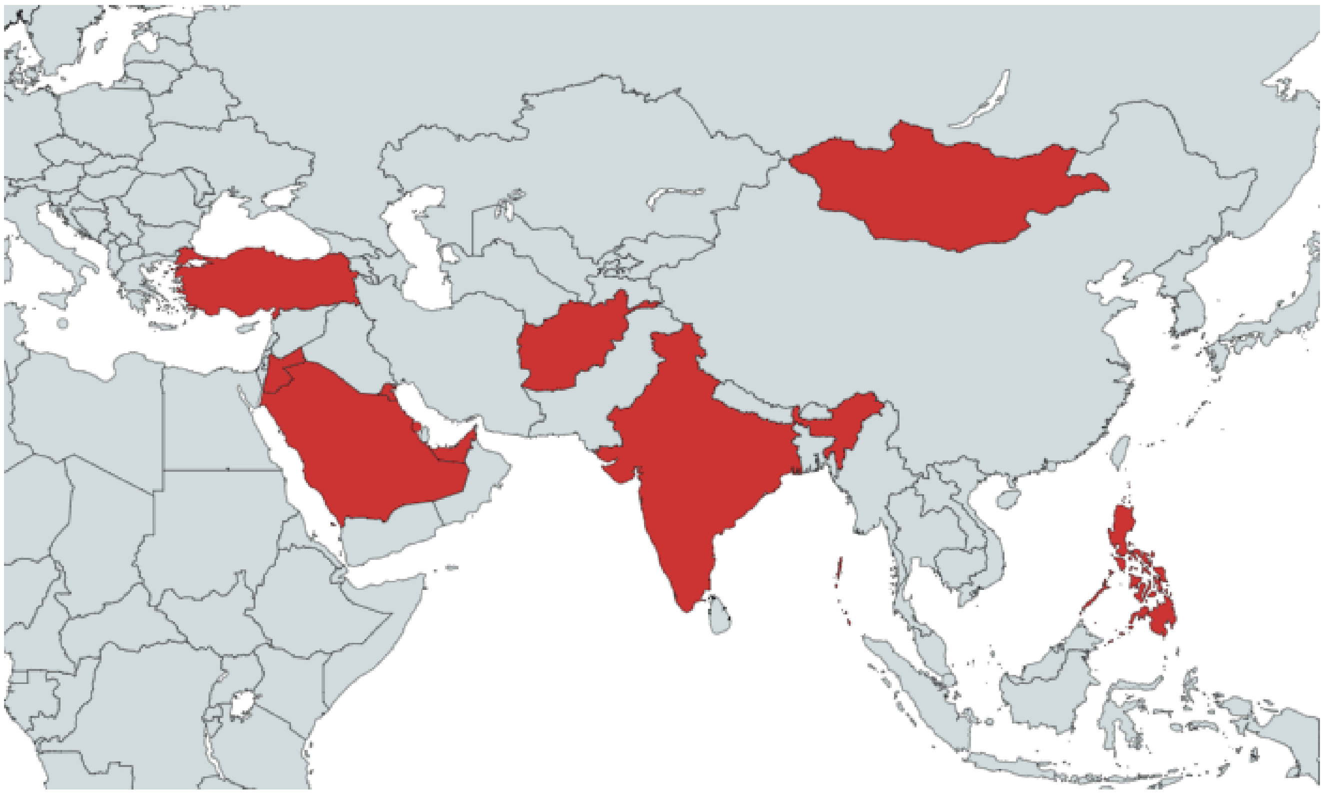


Figure 3. The countries that Iron Tiger has targeted in the past 18 months

Timeline

The following timeline shows different samples found in the same gambling company that Talent-Jump and Trend Micro investigated:

- July 2019: Operation DRBControl starts
- October 2019: One HyperBro malware sample found
- March 2020: New sample of Type 1 malware variant and a rootkit called Pandora found
- April 2020: One rootkit sample for hiding files processes, files, and services found
- October 2020: New HyperBro and Pandora samples found
- December 2020: One sample of the SysUpdate malware variant found
- January 2021: Fast Reverse Proxy (FRP) Linux tool found

Conclusion

This investigation provides more insight into the evolution of Iron Tiger's toolkit and shows the threat actor's persistence after targeting the same company for 18 months, as well as expanding its target base to include other companies and sectors in different countries in the Middle East and Southeast Asia.

We detailed how Iron Tiger threat actors have updated their tools, adding new features, and slightly changing their tactics, techniques, and procedures (TTPs), notably by using a rootkit to hide its backdoors. The different campaigns with different versions of the same tools concurrently being used suggest that there might be subgroups for this threat actor, or multiple groups with access to the builders of these tools.

We expect to see more cases involving four or five files instead of the usual “trident” in the future.

The indicators of compromise (IoCs) can be found in this appendix.