Iron Tiger's SysUpdate Reappears, Adds Linux Targeting

trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html

March 1, 2023

APT & Targeted Attacks

We detail the update that advanced persistent threat (APT) group Iron Tiger made on the custom malware family SysUpdate. In this version, we also found components that enable the malware to compromise Linux systems.

By: Daniel Lunghi March 01, 2023 Read time: 11 min (3060 words)

Iron Tiger is an advanced persistent threat (APT) group that has been focused primarily on cyberespionage for more than a decade. In 2022, we noticed that they updated SysUpdate, one of their custom malware families, to include new features and add malware infection support for the Linux platform.

We found the oldest sample of this updated version in July 2022. At the time, we attributed the sample to Iron Tiger but had not yet identified the final payload. It was only after finding multiple similar payloads in late October 2022 that we looked further and found similarities with the SysUpdate malware family that had also been updated in 2021. As with the previous version, Iron Tiger had made the loading logic complex, probably in an attempt to evade security solutions.

This new version has similar features to the 2021 version, except that the C++ run-time type information (RTTI) classes we previously observed in 2021 had been removed, and that the code structure was changed to use the ASIO C++ asynchronous library. Both changes make reverse engineering the samples longer. We strongly advise organizations and users in the targeted industries to reinforce their security measures to defend their systems and stored information from this ongoing campaign.

Campaign development timeline

These are the key dates for understanding the chronology of Iron Tiger's operations:

- Apr. 2, 2022: Registration of the domain name linked to our oldest Windows sample of SysUpdate
- May 11, 2022: The command and control (C&C) infrastructure was set up.
- June 8, 2022: While this could have been tampered with, observed compilation date of our oldest Windows sample.
- July 20, 2022: Oldest Windows sample gets uploaded to Virus Total
- Oct. 24, 2022: Oldest Linux sample gets uploaded to Virus Total

We observed that the attacker registered the oldest domain name one month before starting the C&C configuration then waited one more month before compiling the malicious sample linked to that domain name. We think the gap between the two updates allows the attackers to plan their operations accordingly.

Loading process

We observed the loading process entailing the following steps:

- The attacker runs rc.exe, a legitimate "Microsoft Resource Compiler" signed file , which is vulnerable to a DLL side-loading vulnerability, and loads a file named rc.dll.
- The malicious rc.dll loads a file named rc.bin in memory.
- The rc.bin file is a Shikata Ga Nai encoded shellcode that decompresses and loads the first stage in memory. Depending on the number of command line parameters, different actions are performed:
    - Zero or two parameters: "Installs" the malware in the system, and calls Stage 1 again via process hollowing with four parameters
    - One parameter: Same as previous action but without the "installation"
    - Four parameters: Creates a memory section with the DES-encrypted malware configuration and a second Shikata Ga Nai shellcode decompressing and loading Stage 2. It then runs Stage 2 via process hollowing.

The "installation" step is considered simple wherein the malware moves the files to a hardcoded folder. Depending on the privileges of the process, the malware either creates a registry key or a service that launches the moved executable rc.exe with one parameter. This ensures that the malware will be launched during the next reboot, skipping the installation part.

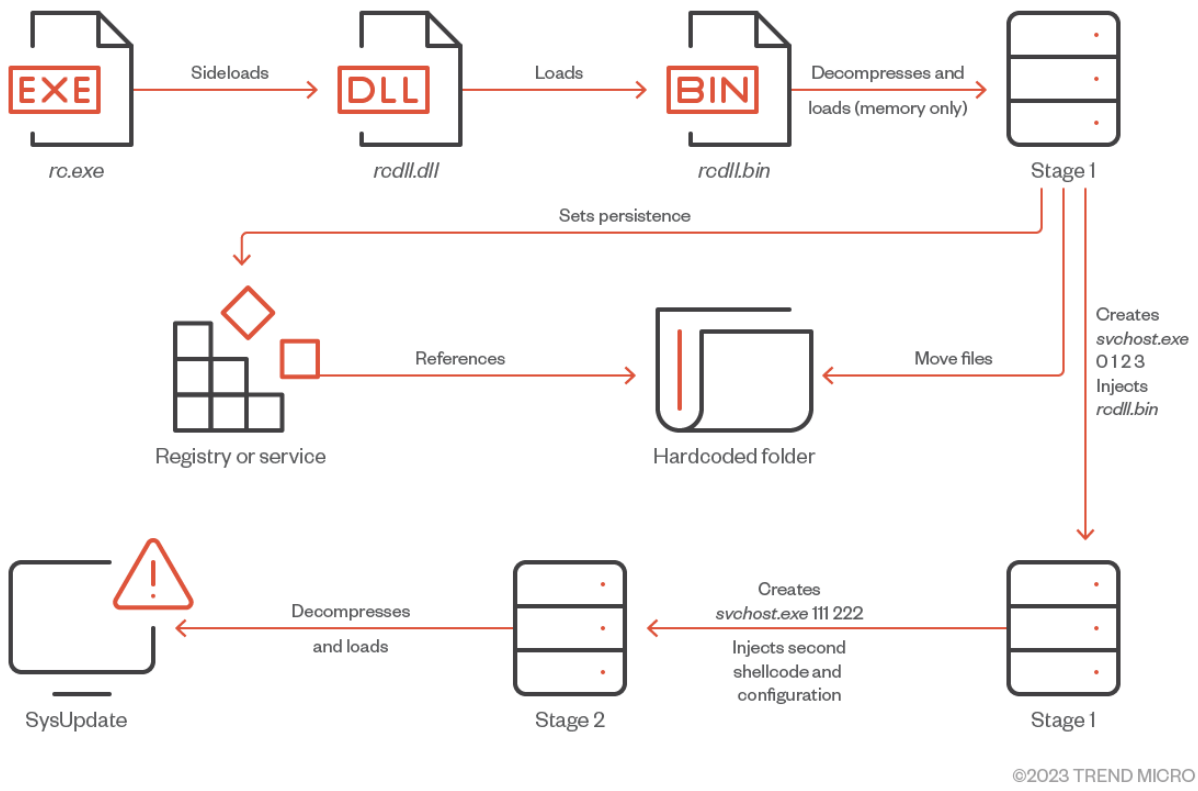


Figure 1. Updated SysUpdate loading process routine

We saw different legitimate executables being used, sideloading different DLL names, and multiple binary files names being loaded by those DLLs. We identified the executables and sideloaded files as follows:

Legitimate application name	Certificate signer	Side-loaded DLL name	Loaded binary file name
INISafeWebSSO.exe	Initech	inicore_v2.3.30.dll	inicore_v2.3.30.bin
rc.exe	Microsoft	rcdll.dll	rcdll.bin
dlpumgr32.exe	DESlock	DLPPREM32.dll	sv.bin
GDFInstall.exe	UBISOFT ENTERTAINMENT	GameuxInstallHelper.DLL	sysconfig.bin
route-null.exe	Wazuh	libwazuhshared.dll	wazuhext.bin
route-null.exe	Wazuh	libwazuhshared.dll	agent-config.bin
wazuh-agent.exe	Wazuh	libwinpthread-1.dll	wazuhext.bin

Table 1. SysUpdate's seemingly legitimate executables and their respective sideloaded files

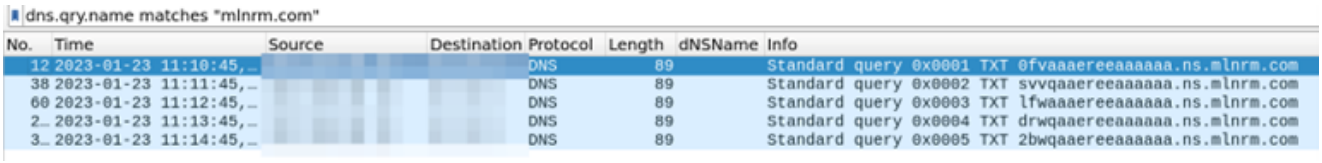
We want to highlight that this is the first time we observed a threat actor abusing a sideloading vulnerability in a Wazuh signed executable. Wazuh is a free and open source security platform, and we could confirm that one of the victims was using the legitimate Wazuh platform. It is highly likely that Iron Tiger specifically looked for this vulnerability to appear legitimate in the victim's environment. We have notified the affected victim of this intrusion but received no feedback.

Malware features

Looking at the features, several of the functions found in the latest update are similar to the previous SysUpdate version:

- Service manager (lists, starts, stops, and deletes services)
- Screenshot grab
- Process manager (browses and terminates processes)
- Drive information retrieval
- File manager (finds, deletes, renames, uploads, downloads a file, and browses a directory)
- Command execution

Iron Tiger also added a feature that had not been seen before in this malware family: C&C communication through DNS TXT requests. While DNS is not supposed to be a communication protocol, the attacker abuses this protocol to send and receive information.


dns.qry.name matches "mlnrm.com"

No.	Time	Source	Destination	Protocol	Length	dNSName	Info
12	2023-01-23 11:10:45,…			DNS	89		Standard query 0x0001 TXT 0fvaaaereeaaaaaa.ns.mlnrm.com
38	2023-01-23 11:11:45,…			DNS	89		Standard query 0x0002 TXT svvqaaereeaaaaaa.ns.mlnrm.com
60	2023-01-23 11:12:45,…			DNS	89		Standard query 0x0003 TXT lfwaaaereeaaaaaa.ns.mlnrm.com
2…	2023-01-23 11:13:45,…			DNS	89		Standard query 0x0004 TXT drwqaaereeaaaaaa.ns.mlnrm.com
3…	2023-01-23 11:14:45,…			DNS	89		Standard query 0x0005 TXT 2bwqaaereeaaaaaa.ns.mlnrm.com

Figure 2. C&C communication with DNS TXT records

First, the malware retrieves the configured DNS servers by calling the GetNetworkParams API function and parsing the DnsServerList linked list. If this method fails, the malware uses the DNS server operated by Google at IP address 8.8.8.8.

For the first request, the malware generates a random number of 32 bits and appends 0x2191 to it. This results in six bytes — four for the random number, two for 0x2191 — and encodes the result further with Base32 algorithm using the alphabet "abcdefghijklmnopqrstuvwxyz012345". Looking at Figure 2, the contacted domain name is after "TXT"; only the first four letters change as the rest of the encoded series is always the same. This is because the random number changes every time, but the end is the same "0x2191" result. This explains why the first DNS request always ends with "reeaaaaaa.<c&c domain>". If the C&C reply matches the format expected by the malware, it launches multiple threads that handle further commands and sends information about the infected machine.

Interestingly, the code related to this DNS C&C communication is only present in samples that use it, meaning that the builder is modular and that there might be samples in the wild with unreported features. We continue monitoring this group and malware family for updates on possible variations of C&C communication protocols being abused.

In all versions, the malware retrieves information on the infected machine and sends it to the C&C encrypted with DES. Collected machine information includes the following:

- Randomly generated GUID
- Hostname
- Domain name
- Username
- User privileges
- Processor architecture
- Current process ID
- Operating system version
- Current file path
- Local IP address and port used to send the network packet

The configuration is encrypted with a hardcoded DES key and is a few bytes long following the structure enumerated below:

Field content	Length (in bytes)	Comment	Example
Header	4	We only found one value	0x00000001
GUID	38	Follows the Microsoft format	{89D0E853-FA08-4f94-A5FE-A90E6869E074}
Size of the C&C section	4		0x00000018
Size of the next C&C domain name and port	4		0x00000014
C&C type	1	0x01 = regular C&C 0x05 = DNS tunneling 0x00 = regular C&C	0x01
C&C domain name	Variable		dev.gitlabs.me
Port number	4		0x00000050

Size of next section	4	Next section contains all the hardcoded names (folder, files, registry values)	0x00000034
Name of the hardcoded directory where files are copied	Variable	The folder is located either in %	gtdcfp
Name of the executable vulnerable to side loading	Variable		TextInputHost.exe
Name of the malicious side-loaded DLL	Variable		rc.dll
Name of the binary file containing the encoded Stage 1	Variable		rc.bin
Name of the service or registry key value used for persistence	Variable		gtdcfp

Table 2. Configuration structure

We noted that Stage 2 does not embed the configuration file, which is copied in memory by the previous stage. We only saw one case where there was only one stage being decrypted in memory and the configuration was hardcoded.

Interestingly, all the samples of this "new" version had a domain name as its C&C. In the previous version of SysUpdate, the group used hardcoded IP addresses as C&C. It is possible that this change is a consequence of the new DNS TXT records' communication feature as it requires a domain name.

SysUpdate samples for Linux

While investigating SysUpdate's infrastructure, we found some ELF files linked to some C&C servers. We analyzed them and concluded that the files were a SysUpdate version made for the Linux platform. The ELF samples were also written in C++, made use of the Asio library, shared common network encryption keys, and had many similar features. For example, the file handling functions are almost the same. It is possible that the developer made use of the Asio library because of its portability across multiple platforms.

Some parameters can be passed to the binary (note that "Boolean" refers to Boolean data that is sent to the C&C):

Parameter	**Effect**

-launch	Sets persistence, zeroes boolean, and exits
-run	Zeroes boolean and continues
-x	Daemonize the process, zeroes boolean, and continues
-i	Daemonize the process, zeroes boolean, sets persistence, and continues
-f <guid>	Sets the GUID to <guid> and continues

Table 3. Parameters passed to the binary as observed from Linux SysUpdate samples

The persistence is ensured by copying a script similarly named as the current filename to the */usr/lib/systemd/system/* directory, and creating a symlink to this file in the */etc/ystem/system/multi-user.target.wants/* directory. Thus, this method only works if the current process has root privileges. The content of the script is:

```
[Unit]
Description=xxx
[Service]
Type=forking
ExecStart=<path to current file> -x
ExecStop=/usr/bin/id
[Install]
WantedBy=multi-user.target
```

After running the code dependent on the parameters, if the operator has not chosen a GUID with the "-f" parameter, the malware generates a random GUID and writes it to a file similarly named as the current file, with a "d" appended to it. Then, the malware retrieves information on the compromised computer and sends it to the C&C.

The following information is sent to the C&C, encrypted with a hardcoded key and DES CBC algorithm:

- GUID
- Host name
- Username
- Local IP address and port used to send the request
- Current PID
- Kernel version and machine architecture
- Current file path
- Boolean (0 if it was launched with exactly one parameter, 1 otherwise)

For the DNS C&C communication version, the malware retrieves the configured DNS server by reading the content of the */etc/resolv.conf* file, or uses the DNS server operated by Google at IP address 8.8.8.8.

In 2022, we already noticed that this threat actor was interested in platforms other than Windows, with the rshell malware family running on Linux and Mac OS. For these reasons, we would not be surprised to see SysUpdate samples for the Mac OS platform in the future. Interestingly, most of the Linux samples we found used the new DNS tunneling feature we detailed in Figure 2, while only one of the Windows' samples used it.

Certificate compromise

Another interesting part of this campaign is the fact that some of the malicious files are signed with a certificate with the following signer: "Permyakov Ivan Yurievich IP". Looking for that name in search engines brings results from the official VMProtect website. The email address linked to the Authenticode certificate also links to that domain name. VMProtect is a commercial software intended to make analysis of code extremely difficult by implementing a custom virtual machine with non-standard architecture. The software has been used by multiple APT and cybercrime groups in the past to obfuscate their malware.

When searching on malware repositories for other files signed by the same certificate, we find multiple files named "VMProtectDemo.exe", "VMProtect.exe", or "VMProtect_Con.exe", which suggests that an official demo version of VMProtect is also signed by this certificate. It appears that the threat actor managed to retrieve the private key allowing him to sign malicious code. As of this writing, the certificate is now revoked.

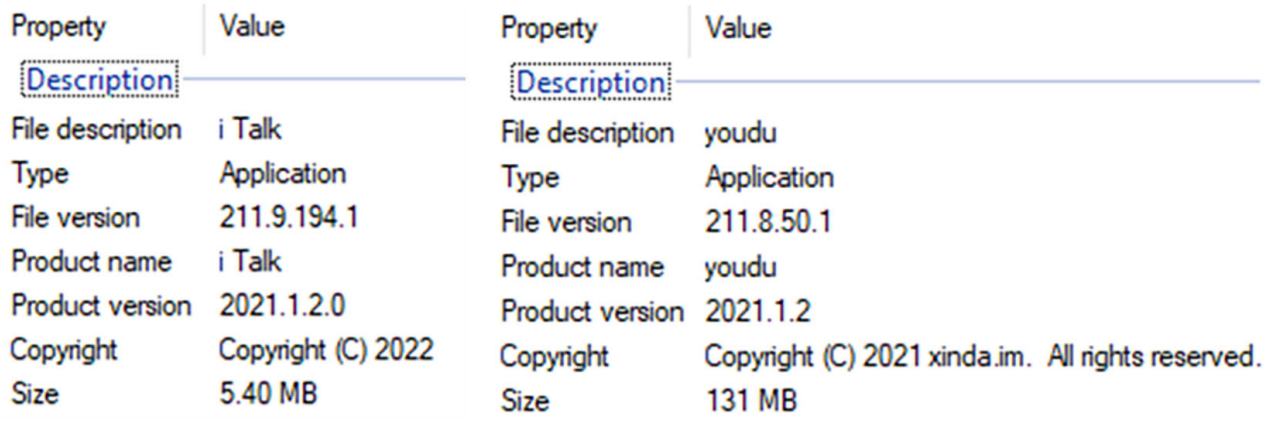
Using stolen certificates to sign malicious code is a common practice for this threat actor, as we already highlighted in 2015 and in all our recent investigations. Interestingly, the threat actor not only signed some of its malicious executables with the stolen certificate, but also used VMProtect to obfuscate one of them.

In late January 2023, a Redline stealer sample (detected by Trend Micro as TrojanSpy.Win32.REDLINE.YXDA1Z, SHA256: e24b29a1df287fe947018c33590a0b443d6967944b281b70fba7ea6556d00109) signed by the same certificate was uploaded. We do not believe that the stealer is linked to Iron Tiger, considering that the network infrastructure is different, and previous reports document the malware's goals to be centered on committing cybercrime than data theft. This could mean other users managed to extract the same private key from the VMProtect demo version, or it was sold in the underground to different groups, Iron Tiger among them.

Infection vector

We did not find an infection vector. However, we noticed that one of the executables packed with VMProtect and signed with the stolen certificate was named "youdu_client_211.9.194.exe". Youdu is the name of a Chinese instant messaging application aimed for use of enterprise customers. Its website mentions multiple customers in many industries, some of them in critical sectors such as government, energy, healthcare, or banking. But they also have other customers in industries such as gaming, IT, media, construction, and retail, apparently all located inside China.

The properties of the malicious file also match the usual Youdu version numbering. However, the legitimate files are signed with a "Xinda.im" certificate instead of the stolen VMProtect certificate.



Property	Value
Description	
File description	i Talk
Type	Application
File version	211.9.194.1
Product name	i Talk
Product version	2021.1.2.0
Copyright	Copyright (C) 2022
Size	5.40 MB

Property	Value
Description	
File description	youdu
Type	Application
File version	211.8.50.1
Product name	youdu
Product version	2021.1.2
Copyright	Copyright (C) 2021 xinda.im. All rights reserved.
Size	131 MB

Figure 3. Comparing the properties of the malicious file (left), and properties of the legitimate Youdu installer (right)

As seen in the product name identified in the malicious file's properties, we searched for possible products named "i Talk" but did not find any that could be related to this investigation. However, we found traces of files from the legitimate Youdu chat application signed by Xinda.im being copied to folders named "i Talk" on one victim's computer. This suggests that some chat application named "i Talk" might be repackaging components from the official Youdu client along with malicious executables. It appears that a chat application was used as a lure to entice the victim into opening the malicious file. This would be consistent with the tactics, techniques, and procedures (TTPs) of two previous Iron Tiger campaigns from 2020 and 2021: a documented compromise of a chat application widely used by the Mongolian government, and a supply chain attack on Mimi chat, a chat application used in parts of South East Asia.

Post-exploitation tools

We found a custom Chrome password and cookie grabber that appeared unfamiliar, and it was compiled and uploaded in September 2022. The file was also signed with the VMProtect certificate but it was not obfuscated. In general, the features were simple; the malware

decrypts the saved passwords to a file named “passwords.txt”, and the cookies to a file named “cookies.txt”.

Analyzing its details, the malware first parses the “Local State” file to retrieve the AES key used to encrypt the cookies and passwords. It then copies the “Login Data” file to a temporary file “chromedb_tmp”, issues an SQL query to extract the URL, login, and password fields from the file, and then decrypts them and appends the result to the “passwords.txt” file.

It proceeds to copy the “Cookies” file to a temporary file “chromedb_tmp”, extracts multiple fields from it using an SQL query, and then decrypts the content before copying the result to the “cookies.txt” file. Some specific cookies related to Google domain names are ignored, probably because they are mostly related to specific Google features or tracking that are considered useless by the threat actor.

We found two other samples from this stealer: One compilation date indicated an executable built in November 2020, and the other one in December 2021, although those dates could be tampered with. We found those samples were uploaded on November 2021 and August 2022, meaning this stealer existed since at least late 2021.

Targeting

We identified one gambling company in the Philippines as compromised by this campaign. Interestingly, the threat actor registered a domain name similar to the company name and used it as a C&C. This was not surprising as we have noticed this threat actor targeting this industry since 2019 during our Operation DRBControl investigation, and later in 2021 with an update of SysUpdate. We also attempted to notify the company of this incident through all their listed channels but have received no feedback.

As stated in the “Infection Vector” section, we noticed the Youdu chat application was probably used as a lure. It is worth mentioning that the customers mentioned in the Youdu official website are all located inside China, which could be an indicator of the threat actor’s interest in targets related to this country.

Conclusion

This investigation confirms that Iron Tiger regularly updates its tools to add new features and probably to ease their portability to other platforms, verifying the interest we found from this threat actor for Linux or Mac OS. It also corroborates this threat actor’s interest in the gambling industry and the South East Asia region, as we previously noted in 2020 and 2021.

This campaign also substantiates the regular usage of chat applications as infection vectors from Iron Tiger. We expect to find further updates of these tools in the future to accommodate other platforms and apps.

As an additional warning, we want to highlight that the targeting can be wider than the samples and targeting we have already observed. In 2022, we discussed a campaign targeting Taiwan and the Philippines that made use of HyperBro samples (detected by Trend Micro as Backdoor.Win32.HYPERBRO.ENC) signed with a stolen Cheetah certificate. The BfV, a German governmental entity, published a report in January 2022 mentioning attacks against German companies with HyperBro samples that were also signed with the same certificate. In October 2022, Intrinsec reported an incident in a French company also using HyperBro samples matching the structure we described in our 2021 investigation. This shows the threat actor is likely to reuse the tools mentioned here in future campaigns that might target different regions or industries in the short and long term. Considering the active campaign and regular developments made on this malware family, organizations are advised to enhance and broaden their current and established security measures, and heighten overall vigilance for possible infection vectors that can be abused by this threat group.

Indicators of Compromise (IOCs)

Download the full list of indicators here.