Updated Shadowpad Malware Leads to Ransomware Deployment

By By: Daniel Lunghi Feb 20, 2025 Read time: 10 min (2782 words)

Published: 2025-02-20 · Archived: 2026-04-02 11:09:39 UTC

Key Takeaways

- Two recent incident response cases in Europe involved Shadowpad, a malware family connected to various Chinese threat actors. Our research suggested that this malware family had targeted at least 21 companies across 15 countries in Europe, the Middle East, Asia, and South America.
- Unusually, in some of these incidents the threat actor deployed ransomware from an unreported family in these attacks.
- The threat actors gained access through remote network attacks, exploiting weak passwords and bypassing multi-factor authentication mechanisms.

In November 2024, we had two incident response cases in Europe with similar C&C servers and other TTPs, suggesting a single threat actor behind both operations. Both incidents involved Shadowpad, a malware family that has been used by multiple advanced Chinese threat actors to perform espionage.

Hunting for similar TTPs, we found a total of 21 companies being targeted with similar malware toolkit in the last 7 months. Nine of them in Europe, eight in Asia, three in the Middle East, and one in South America. We found eight different industries being affected, with more than half of the targets being in the Manufacturing industry. They are listed in the Victimology section.

In two cases, the threat actor deployed a ransomware of a previously unreported family. This is an uncommon move for threat actors using Shadowpad, although it has been reported that APT41 used Encryptor RaaSopen on a new tab. We don't know why our threat actor deployed the ransomware only for some of the targets we found.

Infection vector

In both incidents we investigated, the threat actor initially compromised the target via a remote network attack. They accessed the victim's network after connecting to the VPN using an administrative account with a weak password. In one case, the threat actor bypassed a certificate-based multi-factor authentication mechanism by unknown means, possibly by obtaining a valid certificate prior to the compromise. In the other case, there was no multi-factor authentication and there are traces of brute-force attacks, but we cannot confirm this is related to the successful connection of the threat actor.

After gaining access to the internal network, and armed with administrative privileges, the threat actor deployed the Shadowpad malware, sometimes in the domain controller.

Knowledge of the updating approaches and the targeting of actors of this caliber are critical for companies that may consider themselves of interest to such adversaries. Given the usage of ransomware, and likely interest in some level of intellectual property theft - we recommend that those in the Manufacturing industry in particular leverage their security platform providers to sweep for indicators of this campaign.

Victimology

We found 21 companies being targeted by this threat actor, in 15 different countries and 9 different industries.

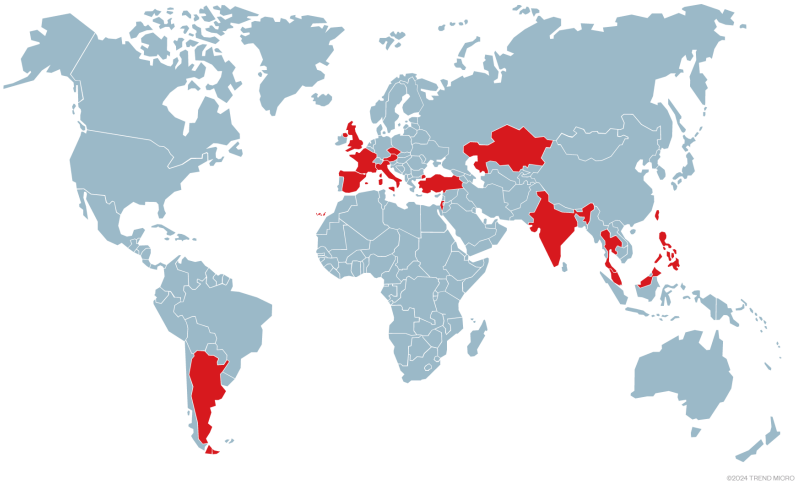

Figure 1. Map of targeted countries

Affected industry	Number of targets
Manufacturing	11
Transportation	2
Publishing	2
Energy	1
Pharmacy	1
Banking	1
Mining	1
Education	1
Entertainment	1

We don’t know the ultimate goal of the threat actor. However, it is possible that some of this targeting is related to intellectual property theft. Additionally, we are aware of some cases where the threat actor deployed a ransomware family. In both incidents, we observed the dumping of Active Directory information and the creation of RAR archives, which were later deleted.

Malware toolkit

Shadowpad

Shadowpad is a modular malware family discovered in 2017open on a new tab in a supply chain attack against the NetSarang software. It has been attributedopen on a new tab to the Chinese threat actor APT41, before being shared among multiple Chinese threat actors in 2019. We have monitored multiple groups related to APT41, such as Earth Baku, Earth Longzhi, Earth Freybug.

It has plugins for typical espionage features such as keylogging, screenshot grabbing, and file retrieval. The code is obfuscated by a custom algorithm and only decoded in memory. The obfuscation saw a major changeopen on a new tab in late 2020, with Earth Lusca being the first group that we saw using such a version. In February 2022, there was a slight update to the obfuscation of this second version. Mandiant has recently published a detailed blogpostopen on a new tab on such obfuscation and how to circumvent it.

The version in this case is similar to the February 2022 version, with some additional features that have been unreported until now:

- Simple and well-known anti-debugging techniques preventing the malware from being debugged normally (more details in a dedicated section below)
- Encryption of the Shadowpad payload in the registry by using the volume serial number, which is unique to the victim’s machine
- The format of the configuration and its parsing changed, but the content remains the same (see section below)
- Usage of DNS over HTTPS (DoH), which results in harder monitoring of the network connections. We no longer see the requests to resolve the C&C domain name, but only the connections to the IP address linked to such domain

While these features are not major enhancements of the malware itself, they show that the malware is in active development and that its developers are willing to make their malware nalysis harder. We do not know if this threat actor is the only group using this enhanced Shadowpad version. We encountered it for the first time in November 2023 targeting critical infrastructure in India, without being able to attribute the sample at the time.

Usually, Shadowpad is split into three different files:

- A legitimate signed executable file vulnerable to DLL side-loading
- A malicious DLL abusing the above vulnerability, with the purpose of decoding and loading the payload in memory
- A binary file containing the encoded Shadowpad payload

Once the DLL decodes and loads in memory the Shadowpad payload, it encodes it again in the registry using a key derived from the volume serial number, and it deletes the binary file from the filesystem. This prevents researchers that don't have access to the victim’s registry or RAM to retrieve the final payload, especially the configuration file containing the C&C.

During our investigation, we noticed the following legitimate files being abused: Note that most of these files are several years old as of this time:

SHA256	Legitimate filename	Side-loaded DLL	Signer
9df4624f815d9b04d31d9b156f7debfd450718336eb0b75100d02cb45d47bd9a	SentinelMemoryScanner.exe	SentinelAgentCore.dll	SentinelOn
28d78e52420906794e4059a603fa9f22d5d6e4479d91e9046a97318c83998679	Logger.exe	logexts.dll	Microsoft Corporatio
bdf019bc6cfb239f0beae4275246216cd8ae8116695657a324497ec96e538aac	nvAppBar.exe	nView64.dll	NVIDIA Corporatio
41128b82fa12379034b3c42bdecf8e3b435089f19a5d57726a2a784c25e9d91f	FmApp.exe	FmApp.dll	Fortemedia
c8268641aecad7bd32d20432da49bb8bfc9fe7391b92b5b06352e7f4c93bc19e	U3BoostSvr64.exe	<executable filename>LOC.dll	ASUSTeK Computer
e06710652fa3c8b45fd0fece3b59e7614ad59a9bc0c570f4721aee3293ecd2d1	syncappw.exe	syncapp.dll	Botkind, In
f4e8841a14aa38352692340729c3ed6909d7521dd777518f12b8bd2d15ea00c5	EPSDNLMW32.EXE	<executable filename>LOC.dll	SEIKO EP CORPORA
aa1233393dded792b74e334c50849c477c4b86838b32ef45d6ab0dc36b4511e3	RoboTaskBarIcon.exe	roboform-x64.dll	Siber Syste

Anti-debugging

The developers implemented multiple techniques to detect the debugging of the malware. While those techniques are well-known, the fact that the Shadowpad code is highly obfuscated makes them more difficult to find.

The techniques are the following:

- Checking the third byte from the Process Environment Block (PEB) (1 if the process if being debugged, otherwise 0)
- Checking the value of the NtGlobalFlag field from the PEB. If the process has been created by a debugger, its value will be 0x70, or zero otherwise
- Retrieving the number of CPU cycles at two different moments and compare the difference between both values. If the number of elapsed cycles is larger than a value fixed by the developer, the malware considers it is being debugged. This technique is performed by calling the RDTSC instruction twice and comparing the number of cycles to 10000000
- Retrieving the number of milliseconds that passed since the system was started by calling the GetTickCount Windows API on two different locations, and comparing the difference to a value fixed by the developer, in this case 3000
- Retrieving the context of the current thread through GetThreadContext Windows API and check if any debug register is set
- Checking the value of the ProcessDebugPort field by calling NtQueryInformationProcess Windows API, which equals to 0xffffffff when the process is debugged

If any of these checks result in the detection of the debugger, the malware terminates itself. Some of these techniques are implemented either in the DLL loader, the payload, or both.

Configuration

The structure of the configuration changed in comparison to the structure we discussed in July 2023.

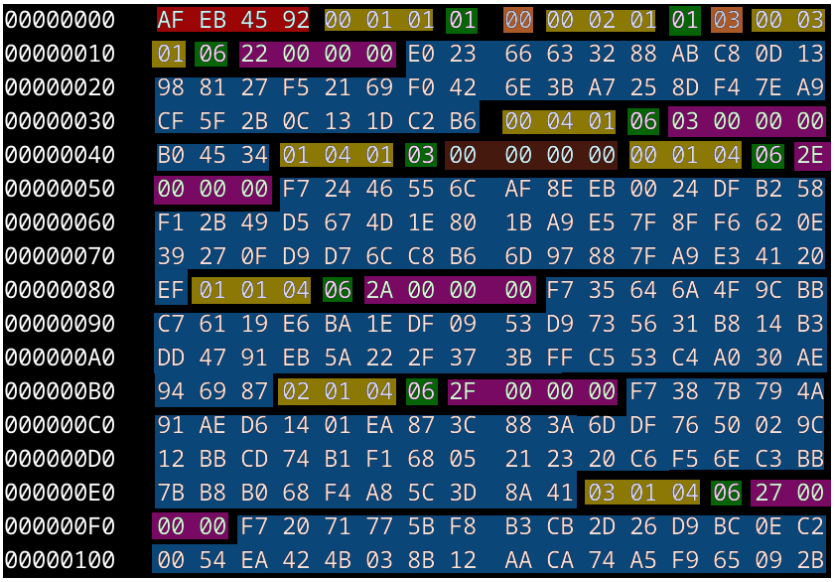

Figure 2. Structure of configuration file

There is still a 4-bytes configuration header at the beginning (highlighted in red).

Now, every item has a three-byte identifier (highlighted in yellow), and a one-byte type (highlighted in green)

We identified the following types:

Item type	Description
0x1	One-byte value
0x2	Two-bytes value
0x3	Four-bytes value
0x5	Encrypted bitstream
0x6	Encrypted string

In the case of an encrypted string or bitstream, the item is followed by a 4-bytes length (highlighted in pink), and the encrypted data itself (highlighted in blue).

There are also items that contain a value, either one-byte (highlighted in orange), 2 bytes, 4 bytes (highlighted in brown).

We identified the following IDs:

ID	Description
0x10300	Mutex name
0x10400	“campaign note”
0x30100	Service name
0x30200	Service display name
0x30300	Service description
0x30400	Registry key used for persistence
0x30500	Value of the registry key used for persistence
0x40100 to 0x40103	path to the process run at boot time
0x40200	side-loaded DLL name
0x40300 to 0x40303	path to the process where the code is injected
0x40500 to 0x40503	C&C
0x40700 to 0x40701	DNS servers

0x40800 to 0x40806	HTTP headers for C&C communication

Ransomware

We found an unreported ransomware family that we believe is related to this threat actor. Although it has been reportedopen on a new tab that APT41 deployed Encryptor RaaS ransomware in the past, it was described as uncommon, and we have not seen any other threat actor using an advanced malware such as Shadowpad deploying a ransomware.

Similarly to Shadowpad, the loading mechanism involves three files:

- Legitimate usysdiag.exe file signed by Beijing Huorong Network Technology Co., Ltd.
- Malicious sensapi.dll side-loaded by usysdiag.exe
- Encoded payload named usysdiag.dat

Once loaded in memory, the malware encrypts all files on the affected system, with the following exceptions:

- Files with the following extensions: .EXE, .DLL, and .SYS
- Files in the following folders: Windows, Program Files, Program files (x86), ProgramData, AppData, and Application Data

For each encrypted file, the ransomware generates a random 32 bytes AES key that is used to encrypt the file. The key is then XORed with 0x3F and encrypted with a public RSA key hardcoded in the sample. The resulting encrypted blob is appended to the encrypted file, meaning that the person with the private RSA key can decrypt the blob to retrieve the AES encryption key and decrypt the file.

Every encrypted file is renamed with the .locked extension.

Then an HTML file with one of the following names is dropped into every directory containing encrypted files:

- locked.html
- unlock_please_view_this_file.html
- unlock_please_view_this_file_unlock_please_view_this_file_unlock_please_view_this_file_unlock_please_view_this_file_unlock_please_view_t

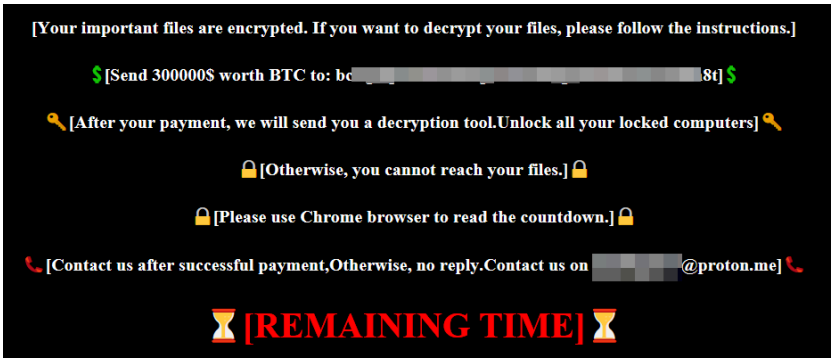

Figure 3. Contents of ransom note

The HTML file contains a reference to a website selling the Kodex Evil Extractor tool, which contains a ransomware feature that has been reportedopen on a new tab in the past. The ransom note looks the same as the one displayed in the Evil Extractor documentation.

However, the description of the algorithm from Evil Extractor documentation does not match at all what we have observed.

> **The "Remastered" version of Kodex Ransomware uses base64 to encrypt files. In simple terms, it distorts the base64 code of the file according to its own algorithm, and only its algorithm can revert the file to its original state. This is a fairly simple but very difficult-to-crack method. Alongside this algorithm, keys are protected using AES encryption method, consisting of a total of 4 primary keys and 1 decryption key. If any of these keys are missing, decryption cannot be performed in any way.**

Figure 4. Text from Evil Extractor documentation

We also found two different Evil Extractor samples in VirusTotal, verified that they were dropping an HTML file with the same appearance, and confirmed that the behavior was totally different from our malware. It actually matched what the Kodex documentation described.

Therefore, we believe the threat actor copied the Kodex ransomware HTML file structure to mislead the analysts into believing this is the Kodex ransomware, while the ransomware family we have analyzed is totally different.

Whatever the intents of the attackers, this part of the attack was not profitable: we have noted no transactions into any of the cryptocurrency addresses we found in these ransom notes. This indicates no victim actually paid the ransom.

Post-exploitation tool

CQHashDumpv2

In two cases we saw Shadowpad running a file named cq.exe with the --samdump argument. We found this file was part of the CQToolsopen on a new tab, a penetration testing toolkit presented at BlackHat in 2019 by CQureopen on a new tab.

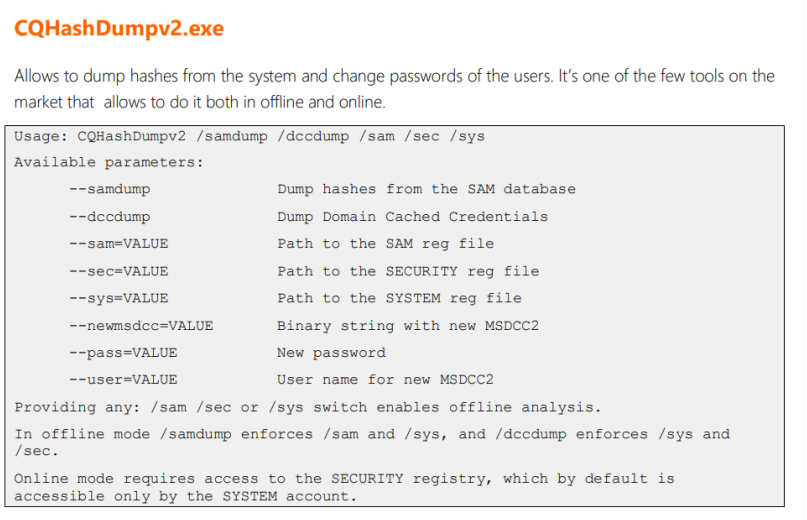

Figure 5. Documentation of CQHashDumpv2.exe from BlackHat paper

Impacket

Impacket is a collection of Python classes for working with network protocols. We noticed the usage of WmiExec from the Impacket toolkit to connect to remote hosts.

Dumping Active Directory databases

While we have no evidence of which tool was used (probably NTDSUtil), the threat actor created files named aaaa.dit likely containing the Active Directory database content that could then be used for offline password cracking.

Infrastructure

We have only one domain name that has been used by Shadowpad as a C&C server in both incident response investigations we conducted. For all other Shadowpad loaders we found, we were unable to retrieve the related encoded payload and, consequently, the associated C&C information.

This domain is updata.dsqurey[.]com. By pivoting on the infrastructure, we were able to identify further IP addresses. We found 3 additional domain names, up to 10 if we count the subdomains.

Some of these domain names were linked to other Shadowpad samples, and to a blogpostopen on a new tab that mentioned similar TTPs to what we observed, enforcing our belief they are linked to this threat actor.

Those domains are listed in the IOC section.

Attribution

We did not find evidence strong enough to link this activity to older operations or to a known threat actor. We found two low confidence links pointing towards the Teleboyi threat actor, which we will explain below.

PlugX code overlap

PlugX is a malware family existing since at least 2008, used in multiple targeted attacks usually by Chinese threat actors, although over time its usage expanded to wider type of attacks. It is believed that Shadowpad is the successor of PlugX.

We found in Virus Total a PlugX sampleopen on a new tab connecting to the bcs[.]dsqurey[.]com domain name. One of the Shadowpad's samples linked to this case connected to updata[.]dsqurey[.]com.

The PlugX sample uses a custom algorithm for string decryption.

In their JSAC presentation (slide 27), TeamT5 describe TeleBoyi custom PlugX loader as using a similar algorithm for decryption of strings. TeamT5 also lists "Operation Harvestopen on a new tab" as being related to Teleboyi. The McUtil.dll

PlugX loader (SHA-256: f50de0fae860a5fd780d953a8af07450661458646293bfd0fed81a1ff9eb4498) listed in Operation Harvest blogpost displays a similar string decryption algorithm. Another similarity is the PE icon of the PlugX sample, which is part of the icons listed by TeamT5. Based on all these findings, we assess with high confidence that this PlugX sample belongs to Teleboyi.

However, we found out that the dsqurey[.]com domain name was initially registered on 2018-03-27, expired in late March 2022, and was registered again on 2022-06-23. We don't know if the same threat actor got his domain back, or if it was registered by a different threat actor. We consider this link to Teleboyi as weak.

Infrastructure overlap

In January 2024, 108.61.163[.]91 resolved to dscriy.chtq[.]net, a domain we link to this threat actor.

In May 2022, it resolved to sery.brushupdata[.]com, a domain name listed in Operation Harvest.

We consider this link to Teleboyi weak since there is one year and a half between both resolutions.

Acknowledgments

Thanks to our European incident response and APT-OPS teams as well as Fernando Mercês for their help in this investigation.

Thanks to the Orange Cyberdefense CERTopen on a new tab for their information on the ransomware family.

Trend Vision One™

Trend Vision One™one-platform is an enterprise cybersecurity platform that simplifies security and helps enterprises detect and stop threats faster by consolidating multiple security capabilities, enabling greater command of the enterprise's attack surface, and providing complete visibility into its cyber risk posture. The cloud-based platform leverages AI and threat intelligence from 250 million sensors and 16 threat research centers around the globe to provide comprehensive risk insights, earlier threat detection, and automated risk and threat response options in a single solution.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One customers can access a range of Intelligence Reports and Threat Insights within Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

- Updated Shadowpad Malware Leads to Ransomware Deployment
-
- Emerging Threats: Updated Shadowpad Malware Leads to Ransomware Deployment
-
- Hunting Queries

Trend Vision One Search App

Trend Vision One Customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Monitor for connections to Shadowpad C&C domains

eventSubId:(203 OR 204 OR 301 OR 602 OR 603) AND (\"updata.dsqurey.com\")

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabledproducts.

Indicators Of Compromise

The indicators of compromise for this entry can be found here.

Tags