Secureworks®

REQUEST DEMO

THREAT ANALYSIS

SHADOWPAD MALWARE ANALYSIS

Sw **Counter Threat Unit Research Team**
February 15, 2022

SUMMARY

The ShadowPad advanced modular remote access trojan (RAT) has been deployed by the Chinese government-sponsored BRONZE ATLAS threat group since at least 2017. A growing list of other Chinese threat groups have deployed it globally since 2019 in attacks against organizations in various industry verticals. Secureworks® Counter Threat Unit™ (CTU) analysis of ShadowPad samples revealed clusters of activity linked to threat groups affiliated with the Chinese Ministry of State Security (MSS) civilian intelligence agency and the People's Liberation Army (PLA).

Some clusters that target China's 'near abroad' appear to be linked to PLA theater commands. These theater commands were introduced in the PLA reforms announced in 2015. Evidence of infrastructure and malware crossover among threat groups likely operating within the same theater command suggests that PLA reforms could be facilitating collaboration among these groups.

ShadowPad is decrypted in memory using a custom decryption algorithm. CTU™ researchers have identified multiple ShadowPad versions based on these distinct algorithms. ShadowPad extracts information about the host, executes commands, interacts with the file system and registry, and deploys new modules to extend functionality. CTU researchers discovered that ShadowPad payloads are deployed to a host either encrypted within a DLL loader or within a separate file alongside a DLL loader. These DLL loaders decrypt and execute ShadowPad in memory after being sideloaded by a legitimate executable vulnerable to DLL search order hijacking.

SHADOWPAD DLL LOADER EXECUTION

The majority of ShadowPad samples analyzed by CTU researchers were two-file execution chains: an encrypted ShadowPad payload embedded in a DLL loader. ShadowPad DLL loaders are sideloaded by a legitimate executable vulnerable to DLL search order hijacking. The DLL loader then decrypts and executes the embedded ShadowPad payload in memory using a custom decryption algorithm specific to the malware version. Table 1 lists legitimate executable and malicious DLL pairs that CTU researchers observed in analyzed samples.

Legitimate executable	Vendor	ShadowPad DLL loader filename	
AppLaunch.exe	Microsoft	mscoree.dll	
hpqhvind.exe	Hewlett Packard	hpqhvsei.dll	
consent.exe	Microsoft	secur32.dll	
TosBtKbd.exe	Toshiba	tosbtkbd.dll	
BDReinit.exe	BitDefender	log.dll	
Oleview.exe	Microsoft	iviewers.dll	

Table 1. Legitimate executable and DLL loader filenames used to load ShadowPad.

CTU researchers identified ShadowPad execution chains involving a third file that contains the encrypted ShadowPad payload. These chains execute the legitimate executable (usually renamed), sideload the ShadowPad DLL loader, and load and decrypt the third file. CTU researchers observed threat actors using BDReinit.exe or Oleview.exe as initial files in the three-file ShadowPad execution chain. The third file in the BDReinit.exe execution chain is log.dll.dat; in the Oleview.exe execution chain, it is iviewers.dll.dat. CTU researchers have attributed campaigns using these execution chains to the Chinese [BRONZE UNIVERSITY](#) threat group, which has targeted transportation, natural resource, energy, and non-governmental organizations. Third-party researchers have also [identified](#) three-file ShadowPad execution chains that begin with consent.exe (followed by secur32.dll and secur32.dll.dat) and AppLaunch.exe (followed by mscoree.dll and mscoree.dll.dat). Additionally, CTU analysis revealed a sample that used AppLaunch.exe followed by mscoree.dll and mscoree.dll.mui.

Other ShadowPad samples from 2018 also deviated from the typical two-file execution chain. Those samples, which used the filename TSVIPSrv.DLL, are placed in the Windows System32 directory and are loaded by the Windows SessionEnv Service, which is vulnerable to DLL hijacking. CTU researchers observed BRONZE ATLAS using this technique in 2021 to load other payloads via this filename, including Cobalt Strike.

CTU researchers discovered ShadowPad samples sharing behavioral similarities such as injecting the decrypted ShadowPad payload into a newly launched target process and establishing persistence on a compromised host specified in the configuration settings. Figure 1 lists configuration information for a ShadowPad sample that reveals command and control (C2) details, the process injection target, and persistence via creation of a service and a registry Run key.

ShadowPadV2 Config	
Type	ShadowPadV2 Config
ID	MyTest-af0228
Name	Manager
Binary Path	%ALLUSERSPROFILE%\Test\Test.exe
Service Name	Manager
Service Display Name	Manager
Service Description	Manager
Persistence Reg Key	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Reg Value Name	Manager
Injection Target	%windir%\system32\svchost.exe
address	• HTTP://ttareyice.jkub.com:443 • HTTP://ttareyice.jkub.com:80

Figure 1. ShadowPad sample configuration information. (Source: Secureworks)

As part of the execution chain, ShadowPad copies the legitimate binary and sideloaded DLL to a subdirectory specific to each sample. Most analyzed samples were copied to a subdirectory under C:\ProgramData, C:\Users*<username>*\Roaming, or C:\Program Files. In three-file execution chains, the third file (e.g., log.dll.dat, iviewers.dll.dat) is typically deleted and the ShadowPad DLL loader is padded to over 50MB, likely to evade antivirus software. As part of this process, an encrypted payload is usually saved to a registry key under HKLM\SOFTWARE\Classes\CLSID\{GUID}*<eight-character hexadecimal string>* (see Figure 2).
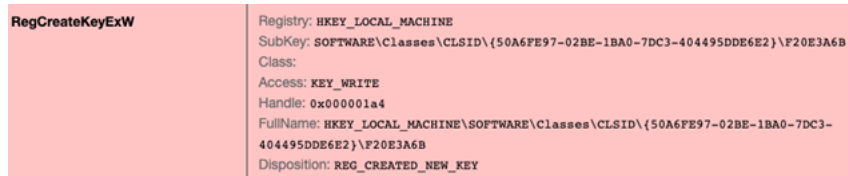
Figure 2. Sample ShadowPad encrypted payload location. (Source: Secureworks)

After the initial setup the legitimate executable is launched as a Windows service. This service initiates the ShadowPad execution chain. The ShadowPad payload is injected into a child process of the service process that is specified in the ShadowPad configuration information. Figure 3 shows the timeline of a ShadowPad execution chain (i.e., log.exe -> log.dll -> log.dll.dat), followed by the service creation and execution of the copied files (log.exe renamed to reg.exe), and the payload injection.
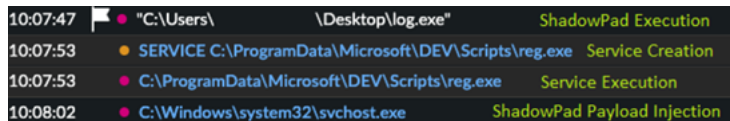

Figure 3. Observed timeline of ShadowPad execution, service creation, and payload injection on a compromised network. (Source: Secureworks)

CTU researchers observed threat actors interacting with ShadowPad malware on compromised hosts. In one incident, multiple cmd.exe child processes were launched via hands-on-keyboard activity (see Figure 4).
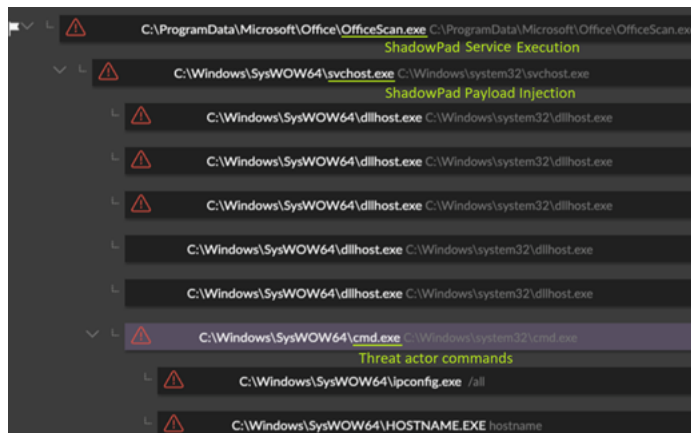

Figure 4. Threat actor interaction with ShadowPad malware. (Source: Secureworks)

Identifying characteristics

The following file structures and behaviors can indicate a ShadowPad compromise:

- A subdirectory within C:\ProgramData, C:\Users*<username>*\Roaming, or C:\Program Files that contains a legitimate executable (likely renamed) and one of the known ShadowPad DLL loader filenames from Table 1 (see Figure 5)
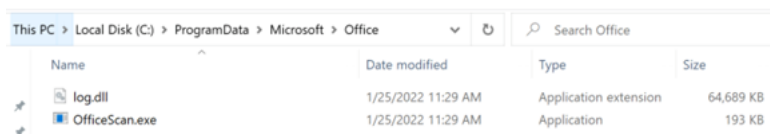

Figure 5. Example legitimate executable and ShadowPad DLL loader in C:\ProgramData subdirectory. (Source: Secureworks)

- A Windows service that launches the legitimate executable from that subdirectory (see Figure 6)

Figure 6. Example of installed Windows service for ShadowPad persistence. (Source: Secureworks)

- Process telemetry showing the Windows service creating an unusual child process (e.g., svchost.exe), which in turn creates multiple dllhost.exe and cmd.exe child processes

THE BRONZE ATLAS/CHENGDU 404 NEXUS

ShadowPad gained notoriety in 2017 after it was deployed in software supply chain attacks involving CCleaner, NetSarang, and ASUS Live Update utility. These campaigns were attributed to the BRONZE ATLAS threat group.

A 2017 Microsoft complaint and U.S. Department of Justice (DOJ) indictments unsealed in 2020 provide additional information on ShadowPad's connection to BRONZE ATLAS. The Microsoft complaint alleges that BRONZE ATLAS (also known as Barium) deployed ShadowPad in 2017 to steal intellectual property and personally identifiable information (PII). At the time, the malware was used only by BRONZE ATLAS. The DOJ indictments allege that Chinese nationals working for the Chengdu 404 network security company deployed ShadowPad in a global campaign attributed to BRONZE ATLAS.

A related DOJ indictment revealed that these Chinese nationals collaborated with another Chinese national known by the handle 'Rose' (sometimes known as Withered Rose and Wicked Rose), using similar tactics, techniques, and procedures (TTPs) and sharing malware. The indictment describes this individual as a sophisticated threat actor who committed computer intrusion offenses targeting high-technology organizations globally. Campaigns linked to Rose were tracked as Barium.

A third-party report claimed that Rose likely co-developed malware with an associate named 'whg,' who has been linked to the development of the PlugX malware. PlugX is used by multiple Chinese threat groups. Third-party researchers also identified string and code overlap between PlugX and ShadowPad. This overlap suggests close links between the ShadowPad and PlugX developers. ShadowPad may have been developed by an individual or group affiliated with BRONZE ATLAS. One possibility is that Chengdu 404 originally developed ShadowPad, as the individuals named in the DOJ indictments were allegedly involved with developing malware used in their campaigns.

It is likely that only BRONZE ATLAS used ShadowPad until approximately 2019. Most of the ShadowPad DLL loader samples can be clustered based on compile timestamps, C2 infrastructure, payload versions, DLL loader code overlap, and likely victimology. CTU researchers identified multiple ShadowPad clusters used in campaigns since 2019 and attributed these clusters to distinct threat groups. These groups include BRONZE ATLAS and BRONZE UNIVERSITY, whose targeting suggests affiliation with the MSS. A third-party report suggests that BRONZE UNIVERSITY (referred to in the report as Earth Lusca) may be operating near to Chengdu in China after operational security mistakes revealed China-based infrastructure. Other ShadowPad clusters appear to reflect targeting aligned with PLA theater command areas of responsibility.

PLA REFORMS

In late 2015, PRC leader Xi Jinping announced widespread reforms to the PLA that included the establishment of the Strategic Support Force (PLASSF or SSF). This new branch focuses on modernizing the PLA's capabilities in strategic frontiers of space, cyberspace, and the electromagnetic domain. The impact on the PLA's cyberespionage mission has been extensive. Many organizations responsible for cyberespionage and signals intelligence (SIGINT) associated with the Third Department of the PLA's General Staff Department (commonly known as 3PLA) have been absorbed into the SSF Network Systems Department (NSD). The SSF NSD is also believed to be responsible for a broad range of information warfare capabilities beyond cyberespionage, coordinating electronic countermeasures as well as offensive and defensive cyber projects. Figure 7 shows the likely SSF organizational structure.
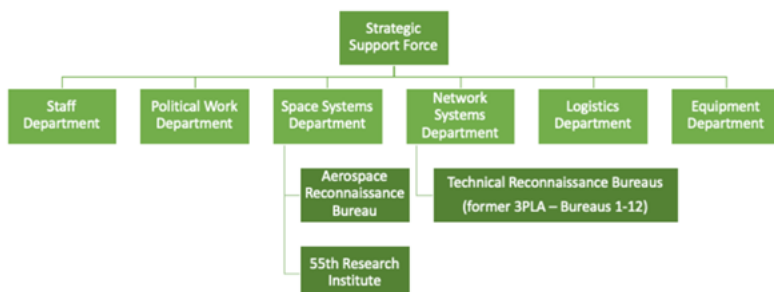

Figure 7. PLA SSF likely organizational structure. (Source: Institute for National Strategic Studies)

As part of the modernization, the PLA replaced its seven military regions with five theater commands: Eastern, Southern, Western, Northern, and Central (see Figure 8). These theater commands orchestrate ground, naval, air, and conventional missile forces for military operations in their geographic area of responsibility. While the exact area of responsibility for each theater command is ambiguous, they are broadly responsible for specific threats within their respective regions:

- Eastern Theater Command: Taiwan strait and East China sea

- Southern Theater Command: South China sea

- Northern Theater Command: Russia and the Korean peninsula

- Western Theater Command: Central Asia and the Sino-Indian border

- Central Theater Command: defends the capital and possibly provides support to other theater commands

Figure 8. PLA theater command structure. (Source: The Jamestown Foundation)

Prior to the PLA reforms, each military region maintained at least one Technical Reconnaissance Bureau (TRB) to handle SIGINT and cyberespionage activities focused on the military region's area of responsibility. The TRBs were distinct from the former 3PLA units that were located across China, but they may have been tasked by the 3PLA.

The relationship between the TRBs and the theater commands is unclear. The TRBs may have been consolidated under the SSF NSD alongside former 3PLA units. It is also possible that they continue to target countries in their area of responsibility but under the command and control of the SSF NSD.

CONNECTIONS TO PLA-LINKED THREAT GROUPS

CTU researchers grouped distinct ShadowPad activity clusters by targeted geographic regions. Clusters align with the documented area of responsibility for three of the theater commands: Northern, Southern, and Western. CTU researchers attribute some of the ShadowPad activity to Chinese threat groups that have been publicly linked to specific PLA units located in the corresponding theater commands:

- **Northern Theater Command:** CTU researchers linked ShadowPad activity to BRONZE HUNTLEY and BRONZE BUTLER, which are reportedly located in the Northern Theater Command. These threat groups deployed ShadowPad against targets in South Korea, Russia, Japan, and Mongolia. These regions align with the Northern Theater Command's focus. In 2021, CTU researchers observed malware and infrastructure overlap between the two threat groups, suggesting close collaboration.

- **Western Theater Command:** Some ShadowPad activity primarily targeted countries neighboring China's western border, such as India and Afghanistan. CTU researchers clustered this activity based on attacker-controlled infrastructure, ShadowPad DLL loader variants such as ICEKILLER, and contextual information from third-party sources. Third-party researchers linked some of these campaigns to an individual working on behalf of the Western Theater Command. CTU analysis did not reveal sufficient evidence to corroborate these claims, but the locations and victimology are consistent with threat actors operating on behalf of the Western Theater Command.

- **Southern Theater Command:** CTU researchers identified activity that used a specific ShadowPad version to target organizations in the South China Sea region. BRONZE GENEVA is likely responsible for part of this activity based on overlap between the C2 infrastructure for the Nebulae malware family associated with BRONZE GENEVA and a ShadowPad sample analyzed by CTU researchers.

This attribution of ShadowPad campaigns to theater commands is based on the submitter's location for ShadowPad malware samples uploaded to the VirusTotal analysis service (potentially indicating the victim's country), the C2 domain names that appear to reference specific regions (e.g., cloudvn. info suggests Vietnam targeting), contextual information regarding the activity and victimology, and the absence of evidence that ShadowPad samples with the same attributes were deployed in other regions.

CONCLUSION

Evidence available as of this publication suggests that ShadowPad has been deployed by MSS-affiliated threat groups, as well as PLA-affiliated threat groups that operate on behalf of the regional theater commands. The malware was likely developed by threat actors affiliated with BRONZE ATLAS and then shared with MSS and PLA threat groups around 2019. Given the range of groups leveraging ShadowPad, all organizations that are likely targets for Chinese threat groups should monitor for TTPs associated with this malware. Organizations with operations in or connections to geographic regions covered by the regional theater commands should specifically monitor for known TTPs associated with threat groups likely affiliated with the relevant theater command.

THREAT INDICATORS

The threat indicators in Table 2 can be used to detect activity related to this threat. Note that IP addresses can be reallocated. The IP addresses and domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
billing.epac.to	Domain	ShadowPad C2 server
9d686ceed21877821ab6170a348cc073	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
3ebeb4e08c82b220365b1e7dd0cc199b765eed91	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
9c28c1b2ff0a84c8b667f128626f28b173feb07481192e214b5a29b98964a7f9	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
172.197.18.30	IP address	ShadowPad C2 server
172.200.21.190	IP address	ShadowPad C2 server
27d889c351ac2f48d31b91d06061ec8d	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
f5b7ea5e705655a1bc08030b601443088a5af4dd	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
d48e671df571b76ee94c734bdd5272e12fcd1362f1d75138ff547bc2bc0c31ef	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
vsmrcil.casacam.net	Domain	ShadowPad C2 server
17e812958704f4ced297731ce47de020	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
57b5ca13d7b2dd9287bdda548ccf7b21c1201464	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
0942f4a488899d5d78b31a0065e49c8689ccda88efc28186e29ee76861ba99da	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
exat.dnset.com	Domain	ShadowPad C2 server
fac0b4fe5372d76607c36ccb51e6b7bb	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
952614358b37d2a519d66ee7759c70e31218ed36	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
4557e923602730aab7718b61eeaf3a93edd0339a3c89c8f7061b9818c2df5203	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
dprouds.casacam.net	Domain	ShadowPad C2 server
17268032c7562fa9473bb85018cb1c2c	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
3d1ae0779b304a8d54df142933158417440ca3ff	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)

bf3de88459f85ddd85245e3f1ce3bba6568919bbe46a808ad5d94d5415014926	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
secupdate.kozow.com	Domain	ShadowPad C2 server
41ff21ea773b73812d91f91b68280ed3	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
8d0be3bca6c93b1ab396ec4a93a33371c82b6567	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
2e07d66155987216dc8cc095b48dd971415f0da261b5b26c58a0e3d34f446038	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
goest.mrbonus.com	Domain	ShadowPad C2 server
1480d2856e4d57d0c8394ade835493db	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
3dfa0fc7da98d0efbd6dbc4b47e01f669e54ea07	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
69eb1aa0021c9b6905b8f0a354884a67f18d20aa045db20b5b5d59f41c7f201f	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
phiinoc.dnsdyn.net	Domain	ShadowPad C2 server
40e7f1a18735819d6cf5f5cff0fb72f4	MD5 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
0b75c1507d6849b303fb496ab8afa60c6c3e8624	SHA1 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
bc0c31be0d4784a6f8ad6333767580e61e7bbe500139fe0d111c39475470a312	SHA256 hash	ShadowPad DLL loader ICEKILLER variant (mscoree.dll)
stratorpriv.lubni23.com	Domain name	BRONZE HUNTLEY ShadowPad C2 server
59961f8c3d8d6cfb7a378f58ff5c5f30	MD5 hash	BRONZE HUNTLEY ShadowPad DLL loader (secur32.dll)
56ff0a3f5d8f67468f1771d38cc6d017a0cd6462	SHA1 hash	BRONZE HUNTLEY ShadowPad DLL loader (secur32.dll)
0dfd91a0dd5d1143697413ebd50efde2411d07b4113d7d282ca0ec3c9d77d5ed	SHA256 hash	BRONZE HUNTLEY ShadowPad DLL loader (secur32.dll)
rolesnews.com	Domain name	BRONZE HUNTLEY ShadowPad C2 server
dfd3b637fc35e850138b33758934f3f7	MD5 hash	BRONZE HUNTLEY ShadowPad DLL loader (secur32.dll)
0d0c5e63a9daf3c322667310e1c06c8b896f7b4c	SHA1 hash	BRONZE HUNTLEY ShadowPad DLL loader (secur32.dll)
ec6852c341aff9d770debc1ef72fb5795c4d71c1327d57d79d65136cc2a670a4	SHA256 hash	BRONZE HUNTLEY ShadowPad DLL loader (secur32.dll)
www.cloudvn.info	Domain name	ShadowPad C2 server linked to targeting of Vietnamese organizations
0ddd78208c16e9f8174868bdf92eac9b	MD5 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
fa639e82ae481a70dffff2c50745ada660c93aa8	SHA1 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
244e22147cc1e37543159a95cf4674a61f290af305c1c1e37b69c45b444f9097	SHA256 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
103.255.179.186	IP address	ShadowPad C2 server linked to targeting of Vietnamese organizations
f977be4ebb0d06c9a19b37d8bbb37178	MD5 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
92c091453295536aef0bac93aa24a294624266da	SHA1 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
2e6ef72d05b395224a03a73a50eaee1c9dc682976c99dde5317b76938cb669a4	SHA256 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
154.202.198.246	IP address	ShadowPad C2 server
b40dec21d0c3061bef422bb946366cba	MD5 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
78f59be833fe8a504a0def218d72aef62823bdaf	SHA1 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)

73bb7e7d0743d40a1d967497a5fbb79c0 7132eb15a546fa25bbecaf43993a1d2	SHA256 hash	ShadowPad DLL loader linked to targeting of Vietnamese organizations (hpqhvsei.dll)
3520e591065d3174999cc254e6f3dbf5	MD5 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
47cdaf6c5c3fffeeff1f2c9e6c7649f99 ab54932	SHA1 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
dbb32cb933b6bb25e499185d6db71386a 4b5709500d2da92d377171b7ff43294	SHA256 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
bda94af893973fe675c35e5699d90521	MD5 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
41b78af0a34f2d1da8d52d895ee50da26 f2a5ab4	SHA1 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
18c4a15e587b223a3fb4d27eedeb16b81 e5c75409d9ffbbe8aeeb7c4c2bd5041	SHA256 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
47.56.228.89	IP address	BRONZE UNIVERSITY ShadowPad C2 server
c3292a51c1b92d7dd08518095bb851f8	MD5 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
ea60a4100d7a893079c29a6027d604759 f62c63b	SHA1 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
d8f695730fcf2cb5a894107740be0a0fa 9bbae6851b83d396976a678236dec30	SHA256 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
b1a9afc937a6e7e0d09e5ccd8b2198f5	MD5 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
5f751bab830f5470fcbac04b1c165bc0b 6e6ecff	SHA1 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
1402ed922a7efc05a6d9482136598fdb5 2afd95cb4e40190ea44a3ba087a58ab	SHA256 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
3e372906248b215ea0ee853cb4e29dd8	MD5 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
c62b977c93979effb48a1614956c2a788 abb22fe	SHA1 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
8d1a5381492fe175c3c8263b6b81fd99a ace9e2506881903d502336a55352fef	SHA256 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
ffbadead054d1eac270f1a24d02e8a1f	MD5 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
c73329dfbe99de4abb93b4fda6310a0c5 eedd8f9	SHA1 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
0371fc2a7cc73665971335fc23f38df2c 82558961ad9fc2e984648c9415d8c4e	SHA256 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
ti0wddsnv.wikimedia.vip	Domain name	BRONZE UNIVERSITY ShadowPad C2 server
06539163f71f8bd496db75ccb41db820	MD5 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
880fa69a6efd8de68771d3df2f9683107 fb484c0	SHA1 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
a8e5a1b15d42c4da97e23f5eb4a0adfd2 9674844ce906a86fa3554fc7e58d553	SHA256 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
373eacf3ffd1b5722f9d3c1595092b4c	MD5 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
363e32fafd2732b3cfb53dfd39bef56da 1affd7f	SHA1 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
8065da4300e12e95b45e64ff8493d9401 db1ea61be85e74f74a73b366283f27e	SHA256 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
207.148.98.61	IP address	BRONZE UNIVERSITY ShadowPad C2 server
ea6be331b5fa349a2fa464b062043b0e	MD5 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
9605ad1bf0432ffb148d422099e23eaa2 6bed4c8	SHA1 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
04089c1f71d62d50cbd8009dfd557aa1e 6db1492a9fa2b35902182c07a0ed1c1	SHA256 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
yjij4bpade.nslookup.club	Domain name	BRONZE UNIVERSITY ShadowPad C2 server
5fe99a8f8cbfe46832478aa9c9634ed6	MD5 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
b224ae9ffd8119d773dedb1863d46725c 29143f8	SHA1 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)

c602456fae02510ff182b45d4ffb69ee6aae11667460001241685807db2e29c3	SHA256 hash	BRONZE UNIVERSITY ShadowPad payload (log.dll.dat)
6czumi0fbg.symantecupd.com	Domain name	BRONZE UNIVERSITY ShadowPad C2 server
Live.musicweb.xyz	Domain name	BRONZE UNIVERSITY ShadowPad C2 server
Obo.videocenter.org	Domain name	BRONZE UNIVERSITY ShadowPad C2 server
5.188.33.106	IP address	BRONZE UNIVERSITY ShadowPad C2 server
299980c914250bac7522de849f6df24f	MD5 hash	BRONZE UNIVERSITY ShadowPad DLL loader (iviewers.dll)
9a035477c1ef725309ae4afac50ffc18d8194a90	SHA1 hash	BRONZE UNIVERSITY ShadowPad DLL loader (iviewers.dll)
9981b9d2024665b7312b673926be96df34be2dc9779956ff49690968e0265d2d	SHA256 hash	BRONZE UNIVERSITY ShadowPad DLL loader (iviewers.dll)
6538263d35b9bb438a9648e904ed7394	MD5 hash	BRONZE UNIVERSITY ShadowPad encrypted payload (iviewers.dll.dat)
680bcd1b172a3658954931131f8248bf66dbc5b1	SHA1 hash	BRONZE UNIVERSITY ShadowPad encrypted payload (iviewers.dll.dat)
253f474aa0147fdcf88beaae40f3a23bdadfc98b8dd36ae2d81c387ced2db4f1	SHA256 hash	BRONZE UNIVERSITY ShadowPad encrypted payload (iviewers.dll.dat)
139.180.141.16	IP address	BRONZE UNIVERSITY ShadowPad C2 server
Teamview.Microsoft.msglocalmicro.com	Domain name	BRONZE UNIVERSITY ShadowPad C2 server
Ts.ekaldhfl.club	Domain name	BRONZE UNIVERSITY ShadowPad C2 server
246d233f4fcda6f4c1ec1177dbad31b4	MD5 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
e76049ee244e74729a20f666328d5eeff8d6488f	SHA1 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)
136848cfbd59af5dcba0fcfb3257bb714184129f94d1a67def618f39dde7c17d	SHA256 hash	BRONZE UNIVERSITY ShadowPad DLL loader (log.dll)

Table 2. Indicators for this threat.

REFERENCES

Threat Intelligence Team. "New investigations into the CCleaner incident point to a possible third stage that had keylogger capacities." Avast. March 8, 2018. https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities

Dr Web. "Study of the ShadowPad APT backdoor and its relation to PlugX." October 26, 2020. https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf

Fraser, Nalani and Vanderlee, Kelli. "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Mission Levels." FireEye. October 10, 2019. https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

Headquarters, Department of the Army (U.S.). "Chinese Tactics." August 9, 2021. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33195-ATP_7-100.3-000-WEB-1.pdf

Hsieh, Yi-Jhen and Chen, Joey. "ShadowPad: A Masterpiece of Privately Sold Malware in Chinese Espionage." Sentinel Labs. August 19, 2020. https://assets.sentinelone.com/c/Shadowpad?x=P42eqA

Insikt Group. "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries." Recorded Future. June 16, 2021. https://www.recordedfuture.com/redfoxtrot-china-pla-targets-bordering-asian-countries/

Kaspersky. "ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World." August 15, 2017. https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world

Ni, Adam and Gill, Bates. "The People's Liberation Army Strategic Support Force: Update 2019." The Jamestown Foundation. May 29, 2019. https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019

Prescott, Adam. "Chasing Shadows: A deep dive into the latest obfuscation method being used by ShadowPad." PwC. December 8, 2021. https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html

Recorded Future. "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries." June 16, 2021. https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf

Stokes, Mark A.; Lin Jenny; and Hsiao, L.C. Russell. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute. November 11, 2011. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

United States Department of Justice. "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." September 16, 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

United States District Court for the District of Columbia. "United States of America v. Zhang Haoran, Tan Dailin, Defendants." May 7, 2019. https://www.justice.gov/opa/press-release/file/1317216/download

United States District Court for the Eastern District of Virginia. "Civil Action No: 1:17-cv-01224." October 26, 2017. https://www.noticeofpleadings.net/barium/files/COMPLAINT_AND_SUMMONS/Complaint.pdf

Wuthnow, Joel and Saunders, Phillip C. "Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications." Institute for National Strategic Studies. March 2017. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-10.pdf

Zetter, Kim. "Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers." Vice. March 25, 2019. https://www.vice.com/en/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

TAGS: Threat Analysis   Threat Intelligence   Research

ABOUT THE AUTHOR

Sw   **COUNTER THREAT UNIT RESEARCH TEAM**   →

The Secureworks Counter Threat Unit™ (CTU) is a dedicated threat research team that analyzes threat data across our global customer base and actively monitors the threat landscape.

← **BACK TO MORE THREAT ANALYSES AND ADVISORIES**

NOW TRENDING...

→ 2024 Global State of the Threat Report

→ Modernize Your Security Operation Center with XDR

→ MDR Done Right
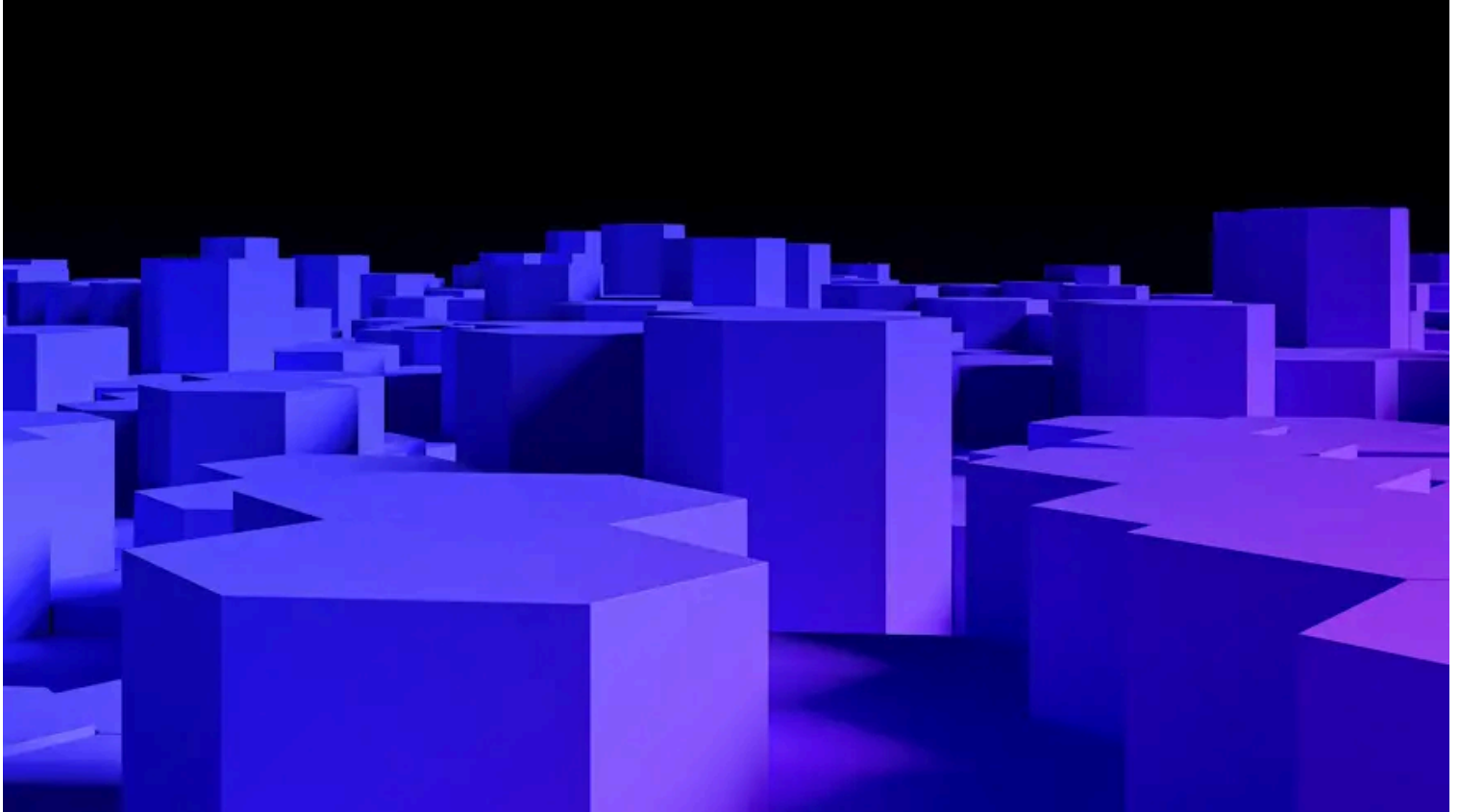
VIRTUAL EVENT

GLOBAL THREAT INTELLIGENCE SUMMIT 2024

WATCH NOW →

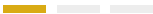## GET THE LATEST SECURITY UPDATES

TALK WITH AN EXPERT

ADDITIONAL RESOURCES

BLOG

THREE CYBERSECURITY PLATFORM PREDICTIONS FOR 2024

READ NOW →

Get the latest updates and news from Secureworks.

SUBSCRIBE NOW →

PLATFORM

Detection & Response

XDR

Log Management

MITRE ATT&CK Coverage

Network Security

NDR

Endpoint Security

EDR

NGAV

Identity Security

IDR

OT Security

Operational Technology

Vulnerability Management

Vulnerability Risk Prioritization

WHY SECUREWORKS

Why Secureworks

Customer Trust

Compare Secureworks

At Your Side

ROI Calculator

Artifical Intelligence

Corporate Responsibility

Corporate Overview

Counter Threat Unit

Careers

Investor Relations

SERVICES

Managed Detection & Response

MDR Overview

Threat Hunting

MDR for OT