SentinelLABS

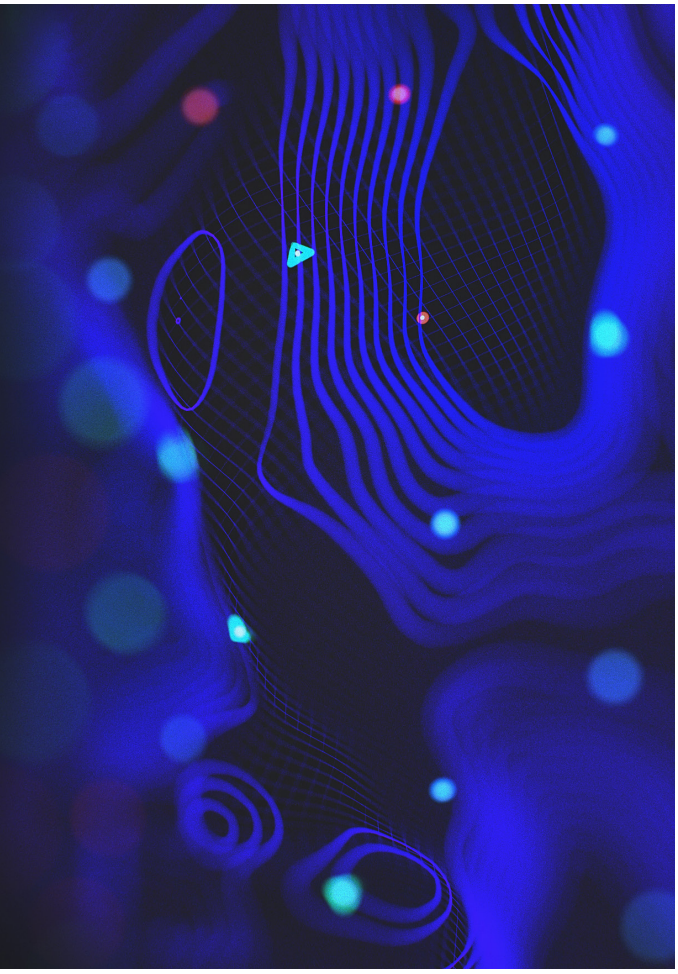
SHADOWPAD: A MASTERPIECE OF PRIVATELY SOLD MALWARE IN CHINESE ESPIONAGE

Authors: Yi-Jhen Hsieh, Joey Chen

August 2021

SentinelLABS Research Team

TABLE OF CONTENTS



EXECUTIVE SUMMARY

- ShadowPad is a privately sold modular malware platform –rather than an open attack framework– with plugins sold separately.
- ShadowPad is still regularly updated with more advanced anti-detection and persistence techniques.
- It's used by at least four clusters of espionage activity. ShadowPad was the primary backdoor for espionage operations in multiple campaigns, including the CCleaner, NetSarang, and ASUS supply-chain attacks.
- The adoption of ShadowPad significantly reduces the costs of development and maintenance for threat actors. We observed that some threat groups stopped developing their own backdoors after they gained access to ShadowPad.
- As a byproduct of that shared tooling, any claim on attribution needs to be reviewed in a cautious way when a shared backdoor like ShadowPad is involved.
- Instead of focusing on specific threat groups, we discuss local personas possibly involved in the development of ShadowPad as an iterative successor to PlugX.

SentinelLabs Team

OVERVIEW

ShadowPad emerged in 2015 as the successor to PlugX. However, it was not until several infamous supply-chain incidents occurred – CCleaner, NetSarang and ShadowHammer – that it started to receive widespread attention in the public domain. Unlike the publicly-sold PlugX, ShadowPad is privately shared among a limited set of users. Its plugin-based design and the capability of inserting plugins during runtime give it good extensibility on the functionalities for its users. Whilst collecting IoCs and connecting the dots, we asked ourselves: What threat actors are using ShadowPad in their operations? And ultimately, how does the emergence of ShadowPad impact the wider threat landscape from Chinese espionage actors?

To answer those questions, we conducted a comprehensive study on the origin, usage and ecosystem of ShadowPad. First, this report provides a detailed overview of ShadowPad, including the technical details and our assessment of its business model and ecosystem. Furthermore, in this whitepaper we introduce at least four activity clusters where ShadowPad has been used. Finally, we share how its emergence changes the attacking strategies of some China-based threat actors and how it affects the threat landscape of Chinese espionage attacks.

HISTORY

PlugX is a fully-featured and modular backdoor in shellcode format, first discovered in 2008[1]. It was named by the security community based on its plugin-based design. Although it is formed of various plugins, it does not allow the plugging and unplugging of those plugins during runtime. It was widely used by different threat groups after its emergence, and nowadays whilst still deployed in some espionage campaigns, it sees significantly less usage due to the popularity of the malware and therefore its detectability.

The relationship between PlugX and ShadowPad has been publicly discussed before[2]. However, SentinelOne discovered other evidence proving that ShadowPad is highly likely to be the successor to PlugX. The project name of a ShadowPad controller was “SC(1.1)” – embedded in the PDB string – while a project name of the PlugX controller was “SController (SC)” by its developer.

[1]https://blog.trendmicro.com/trendlabs-security-intelligence/plugx-new-tool-for-a-not-so-new-campaign/

[2]https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf

- PlugX Controller: D:\My2014\SController(5.6)(天道)(匙)\SC\
- ShadowPad Controller: X:\My2015\SC(1.1)\x64\Release\SoSvr.pdb

A report by AT&T assessed that the developer of PlugX was likely to be a known hacker, nicknamed "whg" - aka "无花果", based in China[3]. whg was an established programmer with a solid track record of developing backdoors and hacking tools, often selling "shared software" to others (as Fig 1 shows). whg is based in the Sichuan province of China, sharing deep connections with the actors behind what was previously known as 'Winnti' and evolved partly into APT41, one of the active ShadowPad users. Winnti was known to carry out several attacks with PlugX[4,5]. We discuss this further below.

Fig 1: The introduction on wgh's personal website. He stated that he had several years of experience in software development, and he also sold some "shared software" on this website.

TECHNICAL ANALYSIS

ShadowPad is a modular backdoor - each plugin contains specific functionality that can be 'plugged' or 'unplugged' during runtime - in shellcode format. It also allows dynamic loading of additional plugins which are not initially embedded in the sample from the C&C server.

In this section, we discuss the emergence of ShadowPad, describe some technical details of the backdoor, and give our assessment on how it is sold.

[3]https://cybersecurity.att.com/blogs/labs-research/tracking-down-the-author-of-the-plugx-rat
[4]https://securelist.com/winnti-more-than-just-a-game/37029/
[5]https://securelist.com/winnti-returns-with-plugx/66960/

Modular Design

ShadowPad is a modular backdoor in shellcode format. On execution, a layer of an obfuscated shellcode loader is responsible for decrypting and loading a Root plugin. While the sequence of operation in the Root plugin decrypts, it loads other plugins embedded in the shellcode into memory. The plugins are kept and referenced through a linked list:

```
struct plugin_node {
   plugin_node* previous_node;
   plugin_node* next_node;
   DWORD referenced_count;
   DWORD plugin_timestamp;
   DWORD plugin_id;
   DWORD field_0;
   DWORD field_1;
   DWORD field_2;
   DWORD field_3;
   DWORD plugin_size;
   LPVOID plugin_base_addr;
   LPVOID plugin_export_function_table_addr;
}
```

Along with the plugins embedded in the sample, additional plugins are allowed to be remotely uploaded from the C&C server, which allows users to dynamically add functionalities not included by default. The uploaded plugins will be kept in memory and added to the linked list of the plugin nodes, as shown in Fig 2.

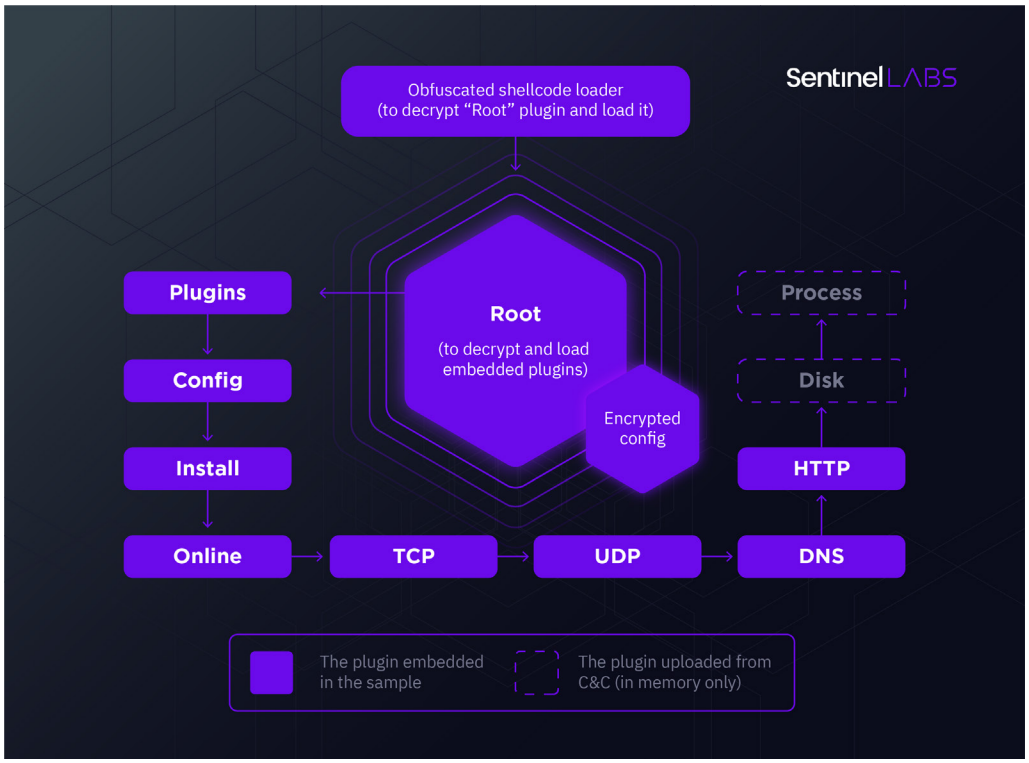


Fig 2: The architecture of ShadowPad backdoor

SentinelOne has collected 22 unique plugins from SentinelOne's internal sample set. These are listed fully in Appendix A.

Controller

As luck would have it, the ShadowPad controller (version 1.0, 2015) was accidentally discovered during private research. All of the stakeholders involved agreed to our releasing screenshots but not the details of the actual file, so we are unable to provide hashes for this component at present. Analysis of the controller allowed us to obtain a clear picture of how the builder generates the shellcodes, how the users manage the infected hosts, and the kinds of functions available on the controller.

Written in Delphi, it has the capability to both generate malware and control backdoor communications. The controller provides an interface to manage infected hosts, manage C&C server listeners and build new ShadowPad shellcode pieces (as shown in Fig 3). This is a relatively unique characteristic of malware used by Chinese espionage threat actors.

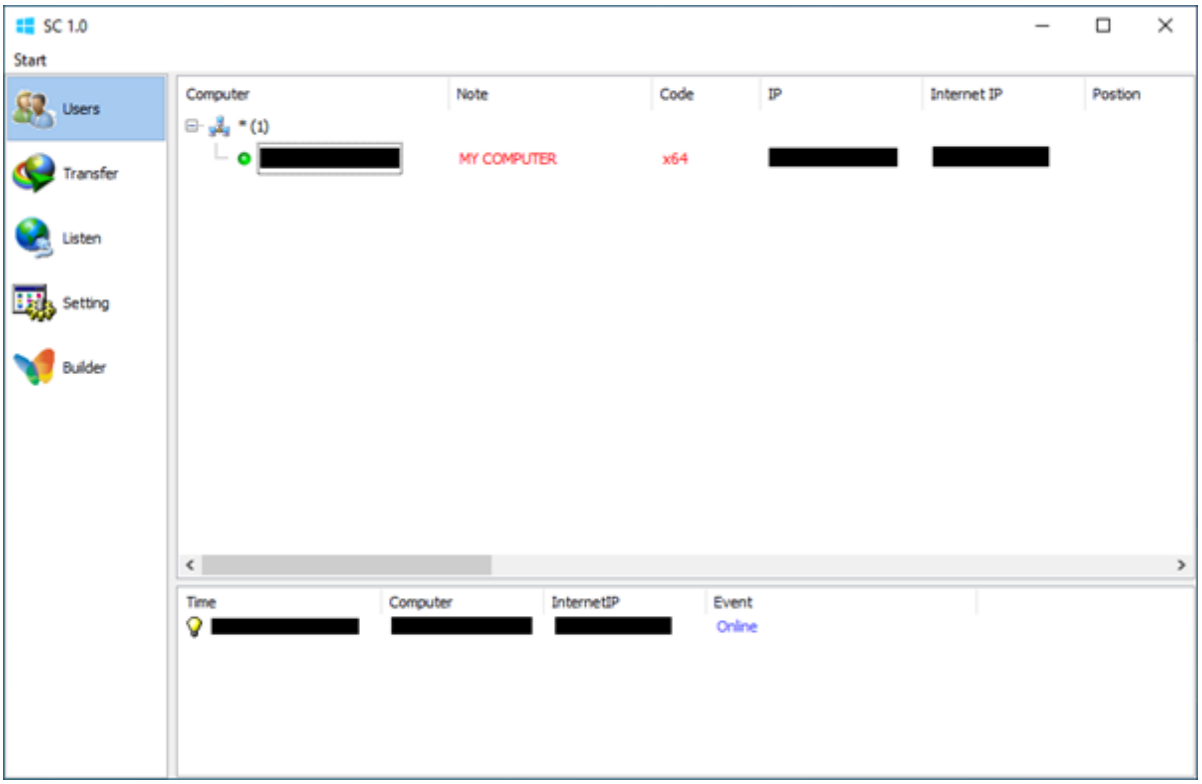


Fig 3: The main page of the controller

- **Users:** The list of infected hosts.
- **Transfer:** The transferring progress of files which are currently being transferred from and to the infected hosts.
- **Listen:** To control the C&C listeners and the protocols in use.
- **Setting:** Intended to be a setting panel, but there is no option on the list in this version.
- **Builder:** The ShadowPad shellcode builder.

The user can choose to enter the management console of a single infected computer (shown in Fig 4). The console allows the user to manage the plugin list and use the functions of each plugin. The plugins “Root” to “Http” are embedded in the samples by default. If the user wants to use the functions of other plugins, those plugins need to be uploaded to the infected computer (in Fig 5).

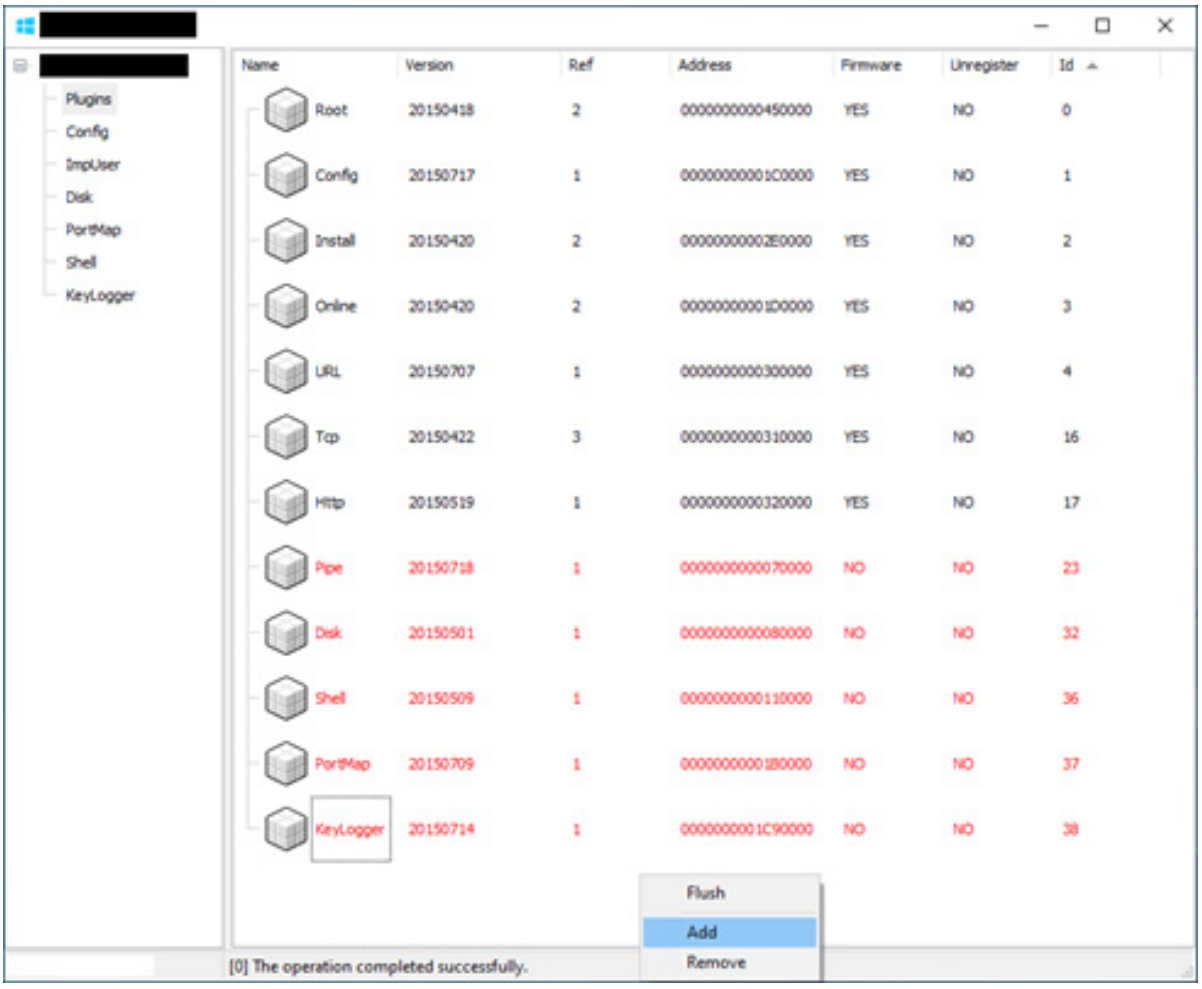


Fig 4: The plugin management page. The user can add or remove a plugin.

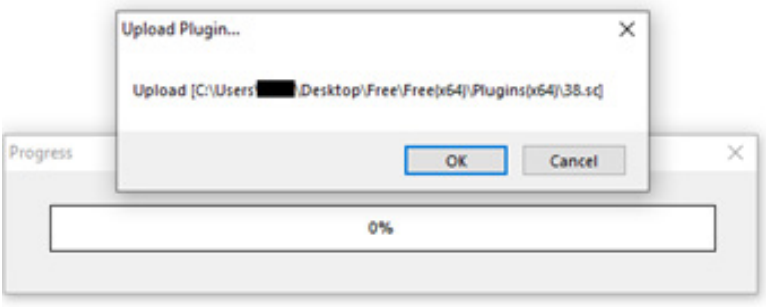


Fig 5: The popup message of asking the user to upload a plugin

The builder (in Fig 6) allows the user to modify the campaign code and notes, anti-debugger settings, installation settings (service and register), process injection settings, C&C servers and connection modes. It also contains configuration import and export functionalities.

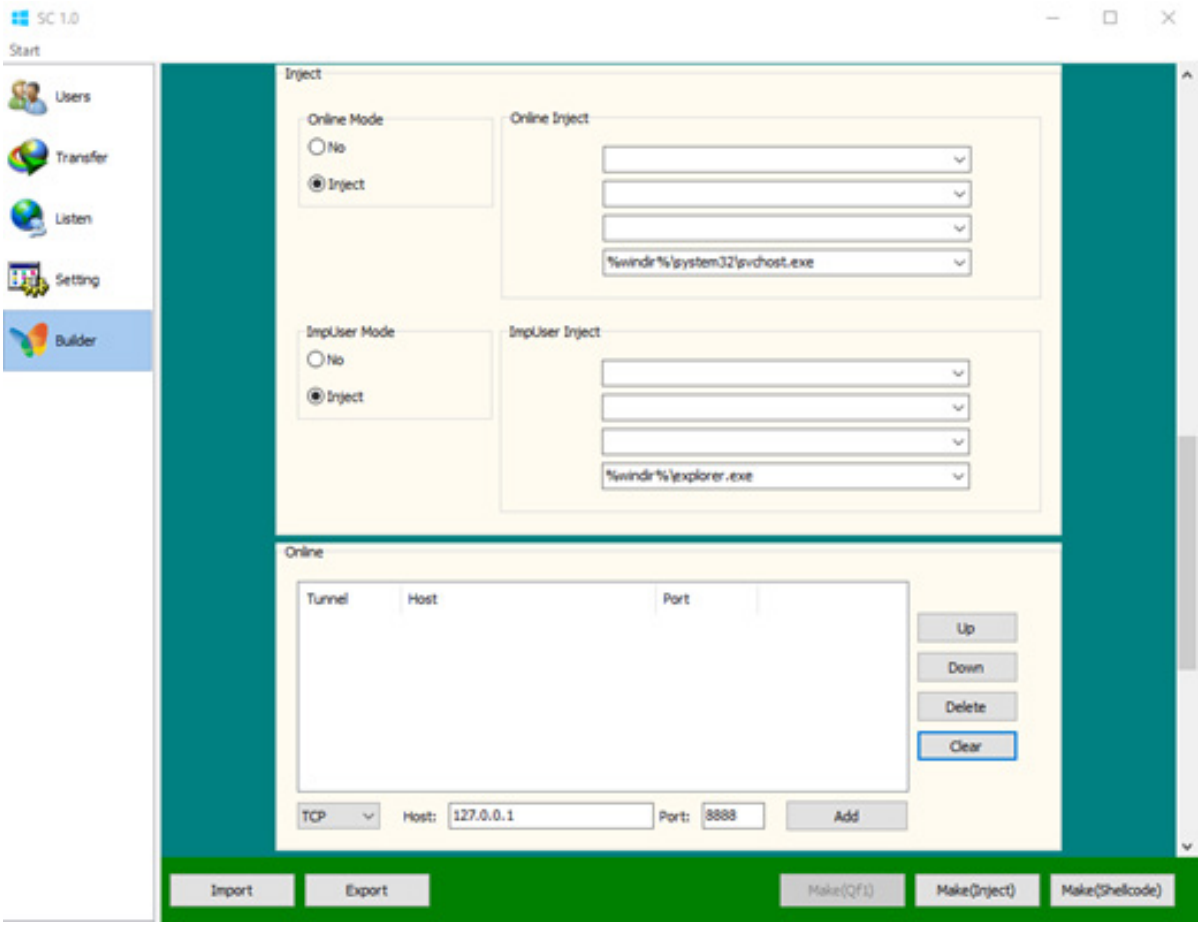


Fig 6: The builder in ShadowPad controller

PRIVATELY SHARED ATTACK FRAMEWORK OR PRIVATELY SOLD MODULAR MALWARE?

An intriguing question to address is whether ShadowPad is a privately shared attack framework or a privately developed modular malware platform for sale to specific groups. Its design allows the users to remotely deploy new plugins to a backdoor. In theory, anyone capable of producing a plugin that is encrypted and compressed in the correct format can add new functionalities to the backdoor freely. However, the control interfaces of the plugins are hardcoded in the “Manager” page of the ShadowPad controller (in Fig 7), and the controller itself does not include a feature to add a new control interface. In other words, it is unlikely that ShadowPad was created as a collaborative attacking framework. Only the plugins produced by the original developer could be included and used through the ShadowPad controller.

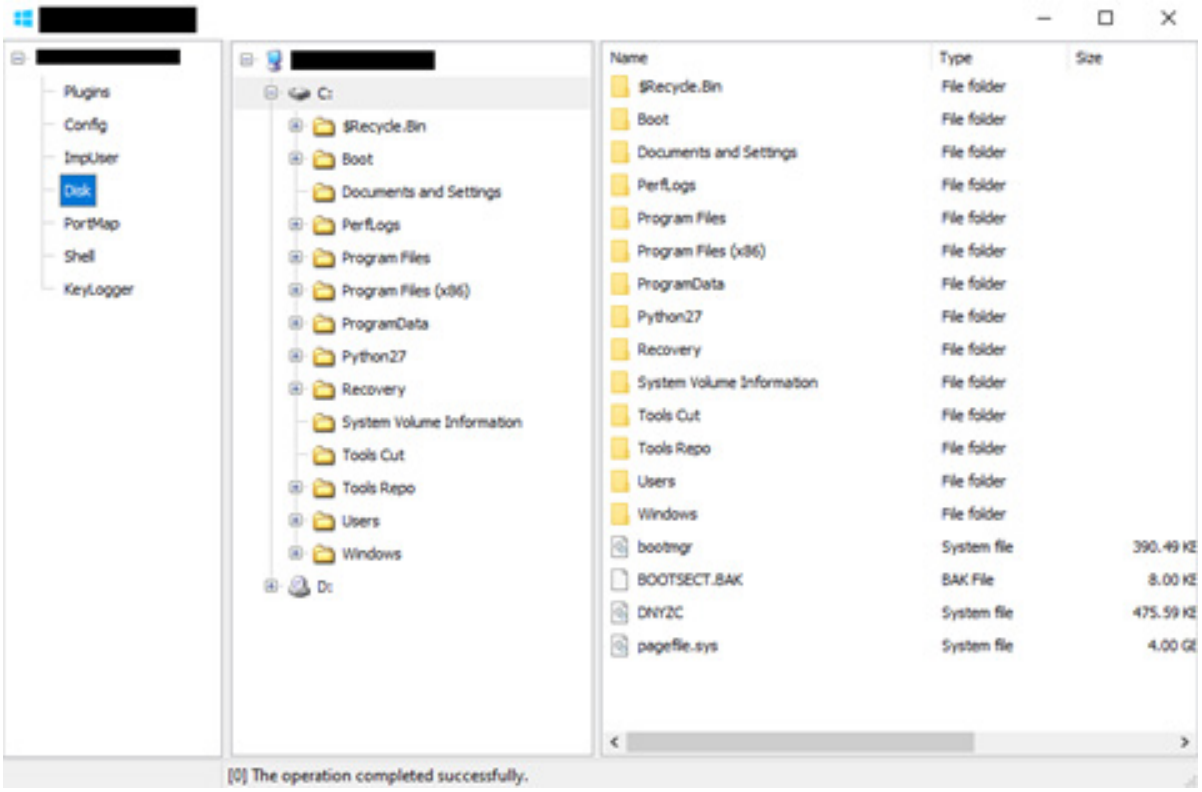
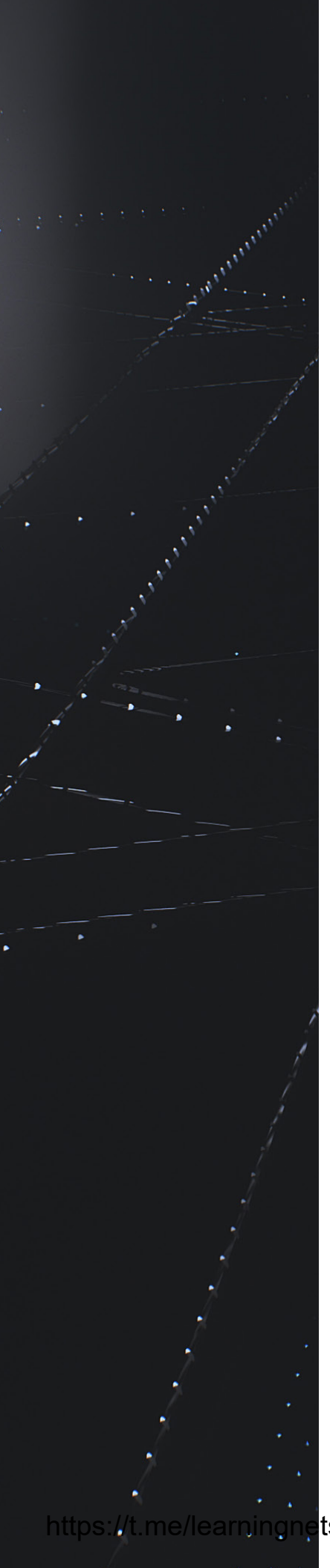


Fig 7: The interfaces to control the plugins are hardcoded and listed in the “Manager” page. The users can interact with the plugins only through the listed interface



On the other hand, even if the control interface of a plugin is listed in the menu, not every available plugin is embedded in the ShadowPad samples built by the controller by default. Once a plugin is not included in the compiled sample, the user needs to upload the corresponding plugin (encrypted and compressed in the correct format) and place it in the "Plugins" directory in the package during runtime on the client side. There is no configuration in the builder to allow the user to choose which plugins are compiled into the generated sample, so this setting can only be managed by the developer of the controller. Any functionality can be easily removed from the bundle by removing the corresponding plugin from the directory.

If ShadowPad was not originally designed as an open framework, the following question is whether it is freely shared with or sold to its users. The possible author 'whg' – and one of his close affiliates, Rose, who will be introduced in the following section – have been monetizing their malware development and hacking skills since the early 2000s. Both individuals sold self-developed malware, and Rose offered services such as software cracking, penetration testing and DDoS attacks[6]. If ShadowPad was developed by them or their close affiliates, it is more likely to be sold to – rather than freely shared with – other users under this context.

Selling the Plugins Separately Rather than Giving a Full Bundle by Default

As discussed, the available functionalities to ShadowPad users are highly controlled by the seller of ShadowPad. Looking deeply into the plugin numbers and the distribution of different plugins embedded in around a hundred samples, we assessed that the seller is likely selling each plugin separately instead of offering a full bundle with all of the currently available plugins. In other words, a buyer needs to pick how many plugins they need and acquire them from the seller. The seller does not provide all the functionality or capabilities by default.

[6]https://web.archive.org/web/20090925075518/http:/www.hackbase.com:80/news/2009-04-09/24948.html

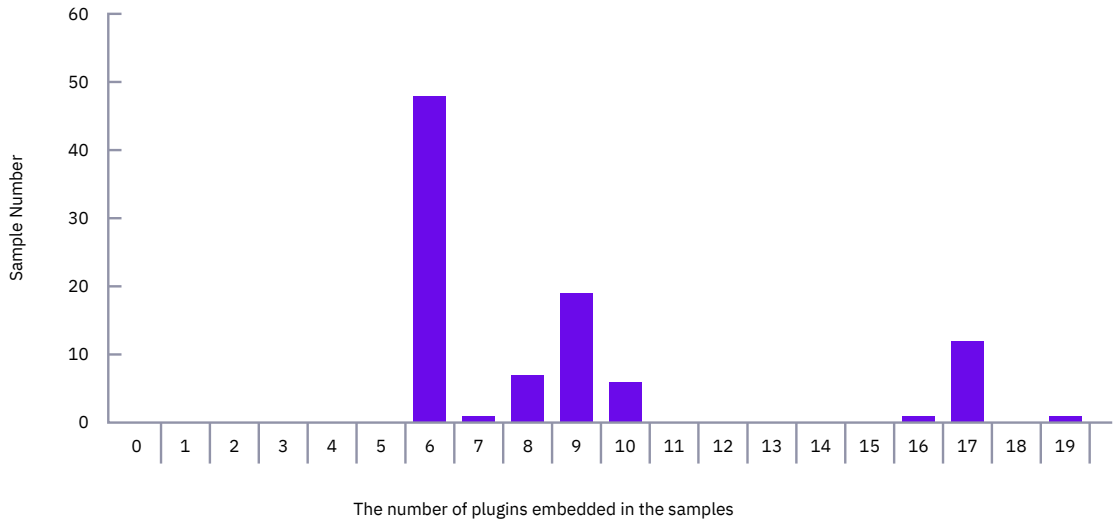


Fig 8: The number of samples grouped by the number of plugins in each sample

Fig 8 groups the samples by the number of the plugins embedded in them. As the figure shows, most of the samples contain less than nine plugins with the following plugins embedded: Root, Plugins, Config, Install, Online, TCP, HTTP, UDP and DNS. This set of plugins can only support the installation of backdoors and communications with C&C servers, without providing further functionality. Actors owning samples with more than 16 plugins, which are all packed by the same loader and are likely to be used by a single closed group, are likely to be offered as 'fully packaged' versions of ShadowPad with the specially configured builders that can build samples with a full set of plugins. In other cases, the actors can only compile ShadowPad backdoors with the basic set of plugins. They need to manually upload other plugins if they want to use other functionalities.

During our research, we found Tick - one of the threat groups with access to ShadowPad - developed a tool to extract the list of installed software information on an infected host while a plugin of ShadowPad with the same functionality – the plugin "Software" – was discovered in a sample used by another threat group in a similar time frame. This shows that not every customer of ShadowPad decides to (or is able to) obtain all of the available plugins. We assess that the plugins are likely to be provided separately.

WHAT THREAT ACTORS ARE USING SHADOWPAD?

Despite being the potential successor to PlugX, ShadowPad is sold privately to a limited set of customers. SentinelOne has identified at least 5 activity clusters of ShadowPad users since 2017.

APT41

APT41 is the accepted naming convention for the activities conducted by two spinoffs of what was once referred to as 'Winnti', sub-groups – BARIUM (Tan Dailin aka Rose and Zhang Haoran) and LEAD (Chengdu 404 Network Technology Co., Ltd)[7]. All of the individuals are based in Chengdu, Sichuan. Rose, Zhang Haoran, and Jiang Lizhi (AKA "BlackFox", one of the responsible persons of Chengdu 404) were coworkers between 2011 and 2017, while Rose and BlackFox already knew each other since at least 2006[8].

One of the actors, Rose - AKA "凋凌玫瑰" - started his active collaboration on malware development with whg, the author of PlugX, when he was a member of the hacking group NCPH back in 2005[9]. They developed "NCPH Remote Control Software" (as shown in Fig 9) together until 2007. The executable of the controller was freely shared on NCPH websites[10,11], but they also declared that the source code was for sale (see Fig 10). Aside from this, NCPH offered customized services of software cracking, malware development and penetration testing[12]. Both Rose and whg were monetizing their malware development skills back in the day.

[7]https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

[8]https://web.archive.org/web/20060906223841/http:/www.mghacker.com:80/blogview.asp?logID=127

[9]https://krebsonsecurity.com/wp-content/uploads/2012/11/WickedRose_andNCPH.pdf

[10]https://web.archive.org/web/20070519130046if_/http://www.ncph.net/newncph/news_view.asp?newsid=96

[11]https://www.51wendang.com/doc/02e6c3141d94fc4bd07015c0

[12]https://web.archive.org/web/20060614163159/http://www.ncph.net/yewul.htm

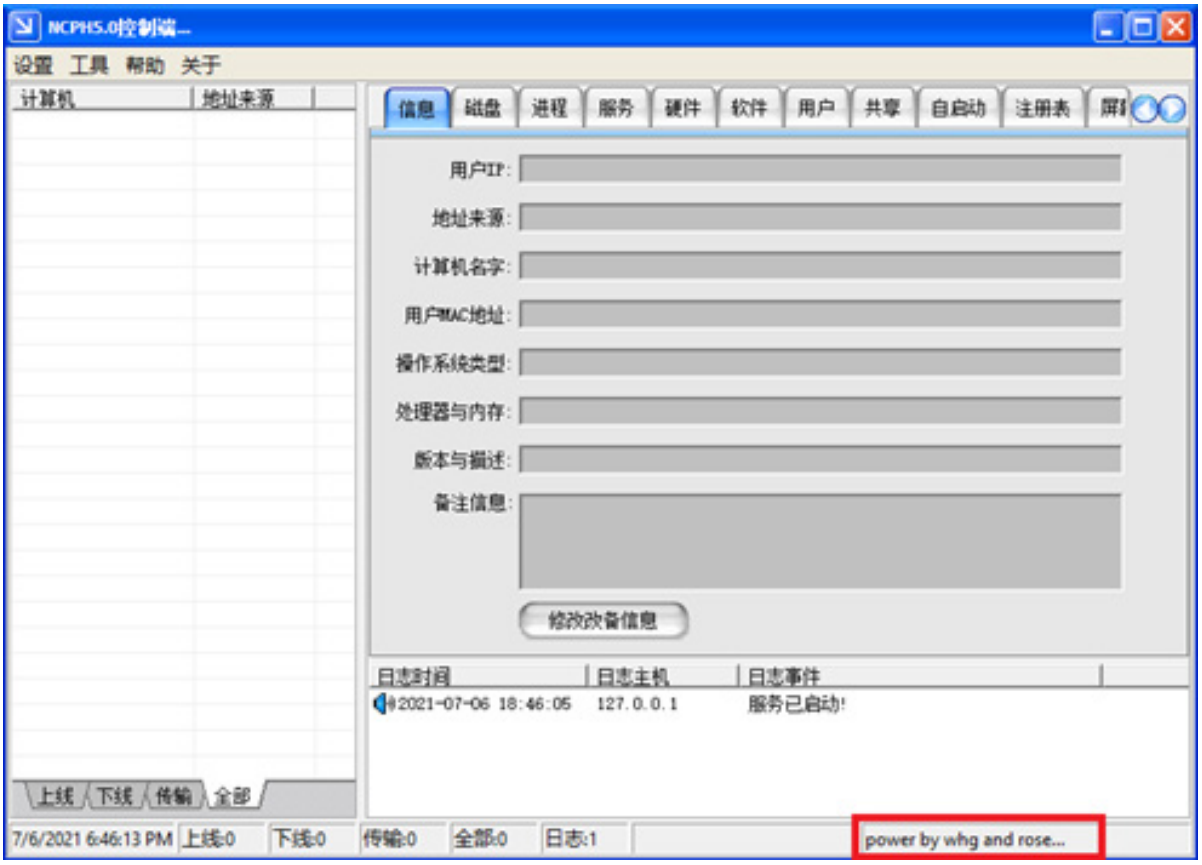
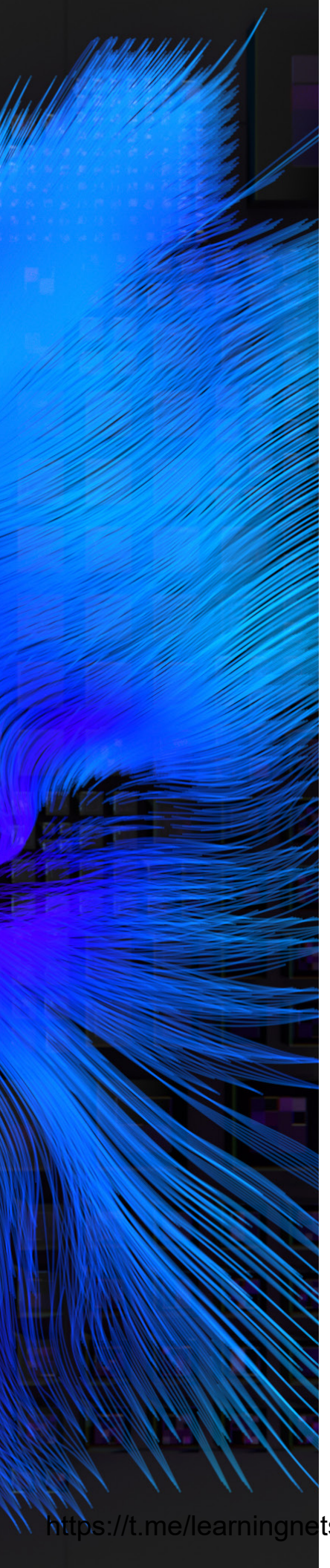


Fig 9: NCPH 5.0 Remote Control Software, developed back in 2005, was powered by whg and Rose.

Fig 10: Rose and his friends sold the source code of “NCPH remote control software” on NCPH forum.



BARIUM (Rose and Zhang Haoran) were one of the earliest threat groups with access to ShadowPad. Aside from some smaller-scale attacks against the gaming industry[13], they were accountable for several supply chain attacks from 2017 to 2018, some of their victims included NetSarang[14], ASUS[15], and allegedly, CCleaner[16,17]. In the aforementioned incidents, the actors used ShadowPad as the primary backdoor of the intrusion after the initial infection phases. During the supply chain attack against ASUS, the samples of ShadowPad were highly customized compared to other ShadowPad samples SentinelOne analyzed. Every layer of shellcode and plugin was packed with VMProtect, and the plugins had different plugin numbers. Another subgroup, LEAD, also used ShadowPad along with other backdoors to attack victims for both financial and espionage purposes. They were reported to attack electronic providers and consumers, universities, telecommunication, NGO and foreign governments.

Considering the long-term affiliation relationship between Rose and whg, we suspect that Rose likely had high privilege access to – or was a co-developer of – ShadowPad, and other close affiliates in Chengdu were likely sharing resources. This could also explain why BARIUM was able to utilize a special version of ShadowPad in some of their attacks.

TICK AND TONTO TEAM

Tick and Tonto Team (referred to as Tick in the following report) have been active users of ShadowPad since 2018. These two groups amalgamated into a new institution during the reorganization of the PLA, and soon thereafter SentinelOne identified significant resource sharing between them, such as the overlaps of C&C infrastructure and the utilities of similar toolsets. A noticeable change after the merge was that they started to use ShadowPad as their primary backdoor for conducting intrusion activities. In the past, they were known to develop their own backdoors for their operations.

---

[13]https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/
[14]https://securelist.com/shadowpad-in-corporate-networks/81432/
[15]https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
[16]https://content.fireeye.com/apt-41/rpt-apt41/
[17]https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities

The threat group conducted several operations with ShadowPad as the primary backdoor from 2018 onwards. Internally, they called ShadowPad "Casper", according to the PDB strings extracted from the customized loaders. Throughout 2019, Tick crafted and sent spear phishing emails to deliver ShadowPad in victims' networks for information exfiltration and long-term espionage[18]. In 2020, they exploited CVE-2019-9489[19] and CVE-2020-8468[20] in Trend Micro's security solutions that were exposed to the Internet, in order to deliver ShadowPad into internal networks for further exploitation[21]. Based on the sample sets we collected, Tick used at least five different versions of ShadowPad; however, all of the samples only contained the basic set of plugins.

Although they turned from self-developed backdoors to the acquired or leaked backdoors, they still developed some customized tools for intrusion, such as a modified mimikatz, a screen capture tool, a packet transmission tool, a tool to list the software installed on a computer, and a VBScript command execution tool. For instance, SentinelOne uncovered a VBScript command execution tool builder (as Fig 11 shows) which can generate a payload of VBScript with built-in evasion techniques to bypass TrendMicro products. The self-developed tool to list the software strongly suggests that Tick was unable to obtain all of the available plugins, since a plugin with the same functionality was available at that time.

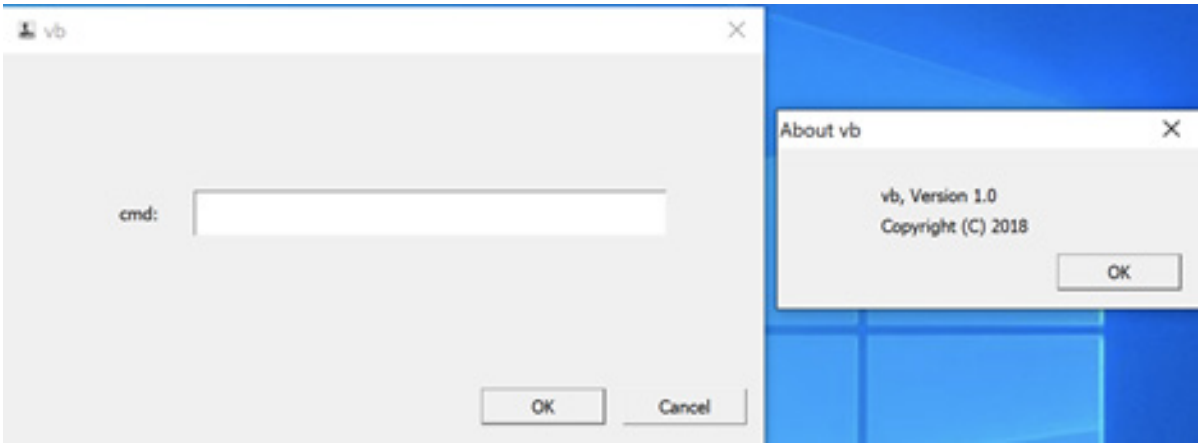


Fig 11: The builder of evasive VBScript developed by Tick. This is one of the self-developed hacking tools in Tick's arsenal.

[18]https://www.trendmicro.com/en_us/research/19/k/operation-endtrade-finding-multi-stage-backdoors-that-tick.html
[19]https://nvd.nist.gov/vuln/detail/CVE-2019-9489
[20]https://nvd.nist.gov/vuln/detail/CVE-2020-8468
[21]https://vb2020.vblocalhost.com/conference/presentations/tonto-team-exploring-the-ttps-of-an-advanced-threat-actor-operating-a-large-infrastructure/

OPERATION REDBONUS

SentinelOne caught a ShadowPad activity cluster that had no clear link to known threat groups. SentinelOne tracks the activities of this cluster under the moniker ‘Operation Redbonus’.

The first activity of ShadowPad SentinelOne discovered occurred at the end of 2019. All the samples we collected from Operation Redbonus were running the same version of ShadowPad. During our investigations, we also spotted other backdoors in use, such as Whitebird[22], IceFog and a customized instance of PCShare. The actors behind this cluster appear to show interest in Indian targets with several DDNS domains spoofing some Indian institutions.

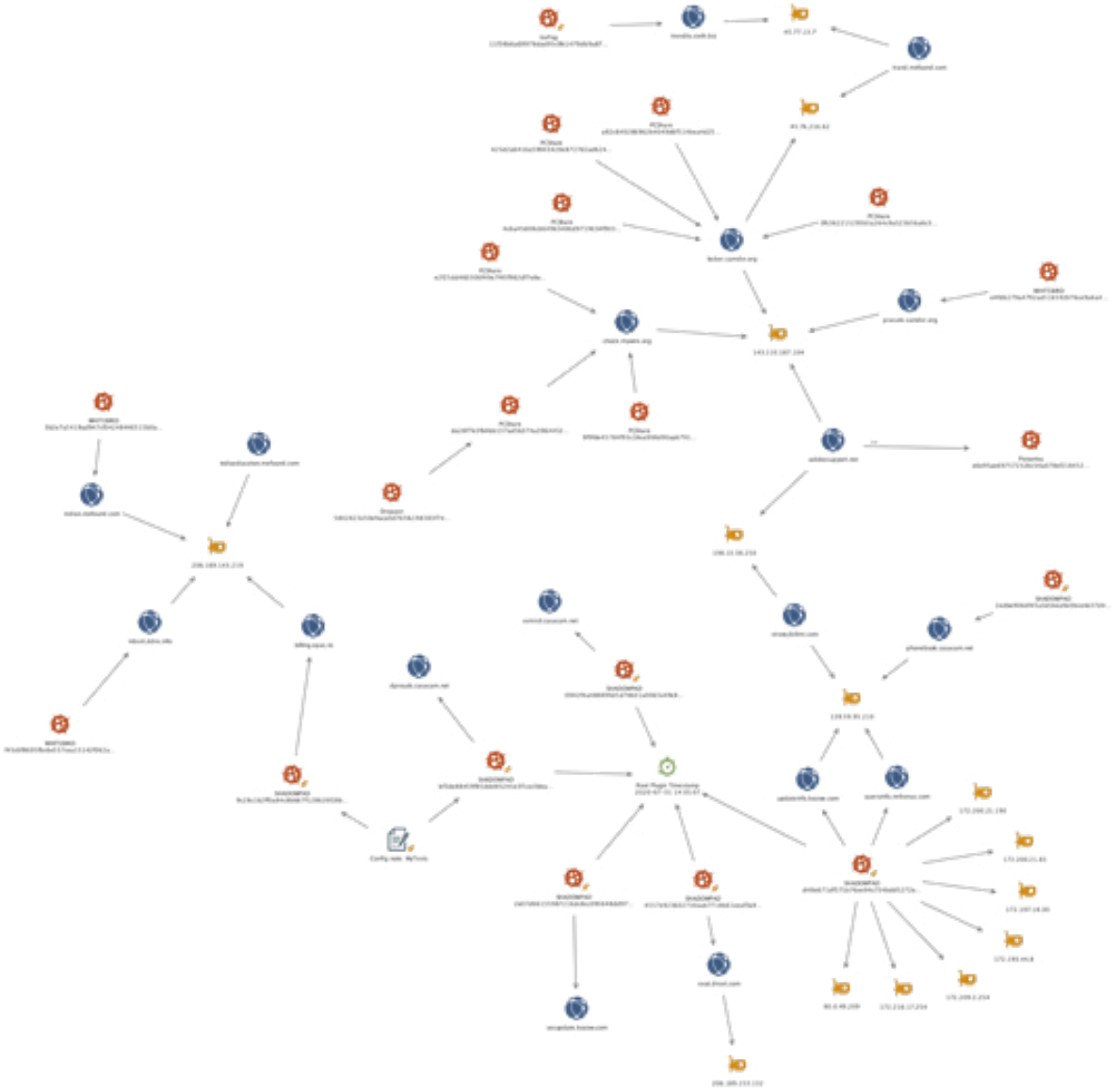


Fig 12: The artifacts of Operation Redbonus

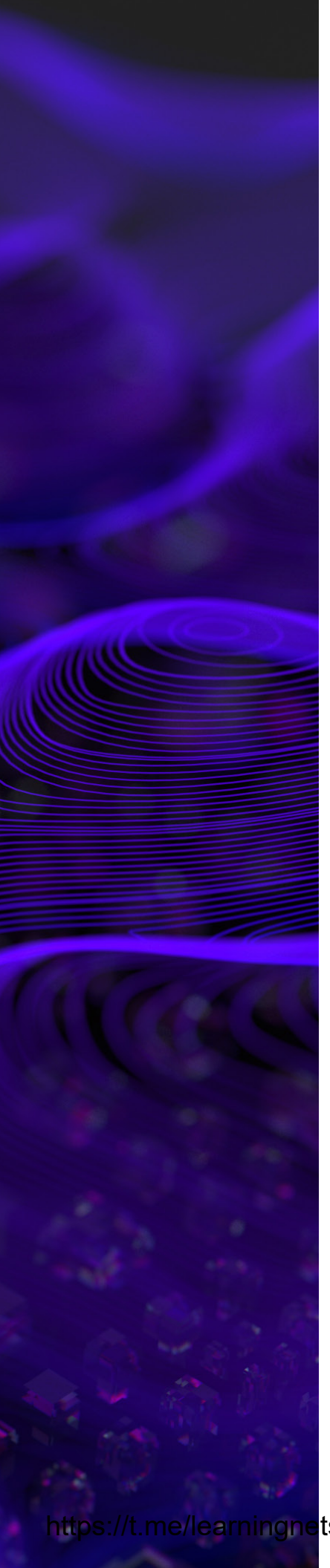
[22]https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf

OPERATION REDKANKU

There is another small set of ShadowPad samples without clear attributions in the public domain. All of the C&C servers extracted from the samples had a self-signed certificate b41948daacd4c081a58a14aa51c37af21738447b installed. Whilst further attribution or overlaps are not available at the time of writing, some related samples were documented to be a part of the ProxyLogon attacks according to a report by ESET[23].

Fig 13: The artifacts of Operation Redkanku

[23]https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/



FISHMONGER

Another activity cluster – tracked by SentinelOne as Fishmonger – has been active since at least 2018. The cluster is tracked based on the overlap of infrastructure and indicators, as well as some behavioral connections between different campaigns.

Back in 2019, the actors used a special version of ShadowPad which allowed them to generate samples with a handful of plugins embedded by default[24]. In 2020, they gained access to a new version of ShadowPad which had updates and more advanced obfuscation techniques. They are now using it and another backdoor called Spyder[25] as their primary backdoors for long-term monitoring[26], while they distribute other first-stage backdoors for initial infections including FunnySwitch, BIOPASS RAT[27], and Cobalt Strike. The victims include universities, governments, media sector companies, technology companies and health organizations conducting COVID-19 research in Hong Kong, Taiwan, India and the US.

[24]https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/

[25]https://st.drweb.com/static/new-www/news/2021/march/BackDoor.Spyder.1_en.pdf

[26]https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf

[27]https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html

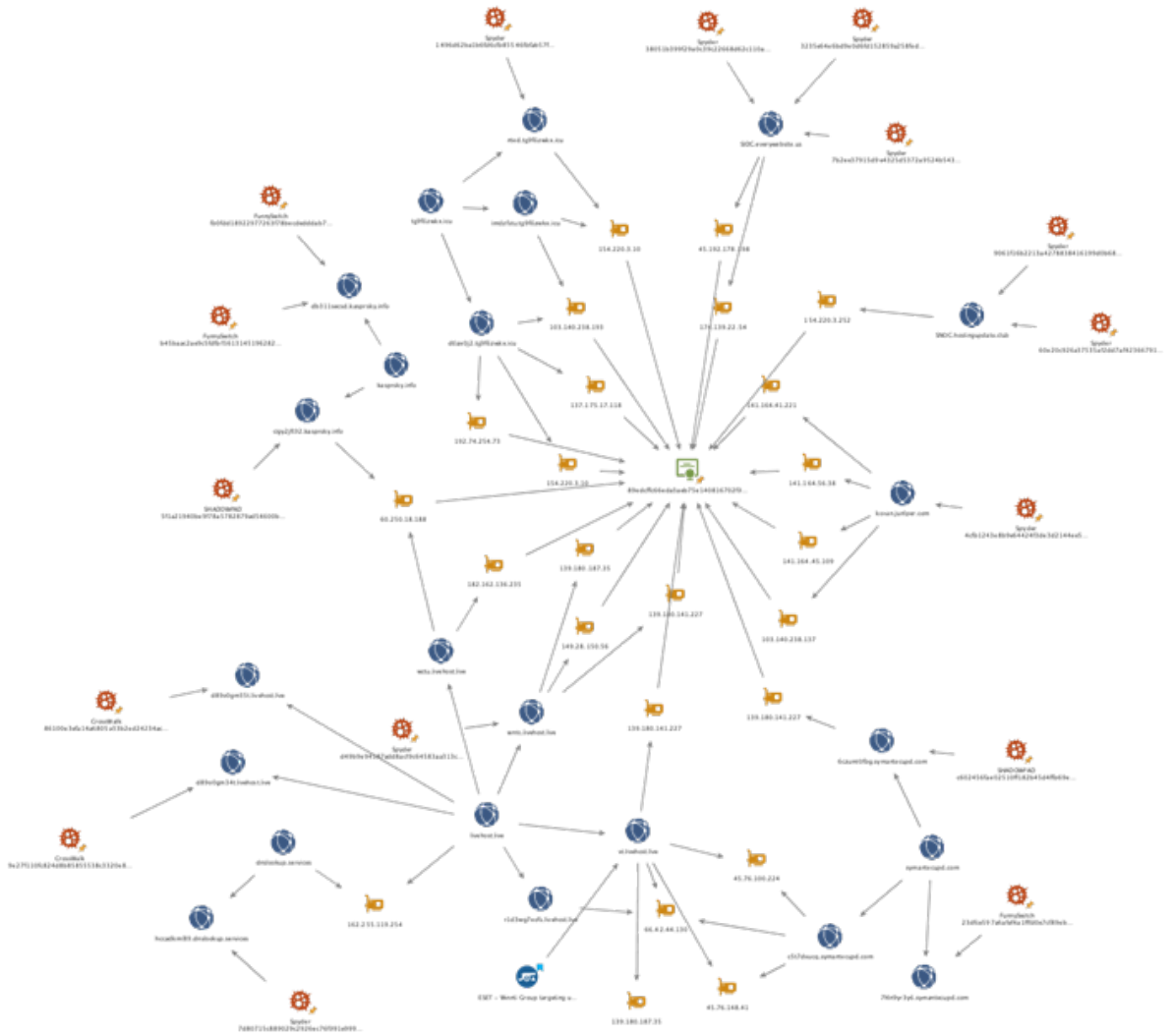


Fig 14: Part of the artifacts of Fishmonger

OTHERS

Some public reporting detail other possible users of ShadowPad, including LuckyMouse (ESET)[28] and Tropic Trooper (PwC)[29]. However, SentinelOne does not have visibility of this activity.

[28]https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

[29]https://www.youtube.com/watch?v=YCwyc6SctYs&t=1347s

ASSESSMENT

Apart from the threat groups and activity clusters detailed above, there are still some unattributed ShadowPad samples in the sample set SentinelOne collected and analyzed. The nature of privately sold backdoors requires more context to begin analytically-sound attribution. There might be other unidentified actors using this backdoor, and it requires a rigorous approach when attempting to attribute ShadowPad campaigns.

Since ShadowPad is a powerful backdoor with a complete set of functionalities, a number of its users (for instance, Tick and Fishmonger) deploy ShadowPad for the purpose of long-term espionage in victim environments. Threat actors using ShadowPad select systems with high privileges on networks to reduce the probability of detection, such as AD servers or domain controllers. Proactive scanning and periodical health checks on high-privilege hosts are essential to discover the footprints of attackers.

LANDSCAPE SHIFT: FROM DEVELOPING BACKDOORS TO ACQUIRING BACKDOORS

It is not a secret that a number of Chinese threat actors develop their own tool sets based on their needs during operations. However, established espionage threat actors also acquire tooling to add to their arsenals. Tick was one of the most active users of ShadowPad according to research. Prior to this, Tick was documented to be using self-developed backdoors including Darsef, xxmm and Datper[30]. A noticeable change SentinelOne discovered during the monitoring of the threat group was that the actors later stopped the use of other self-developed backdoors after actively using ShadowPad (which they called Casper).

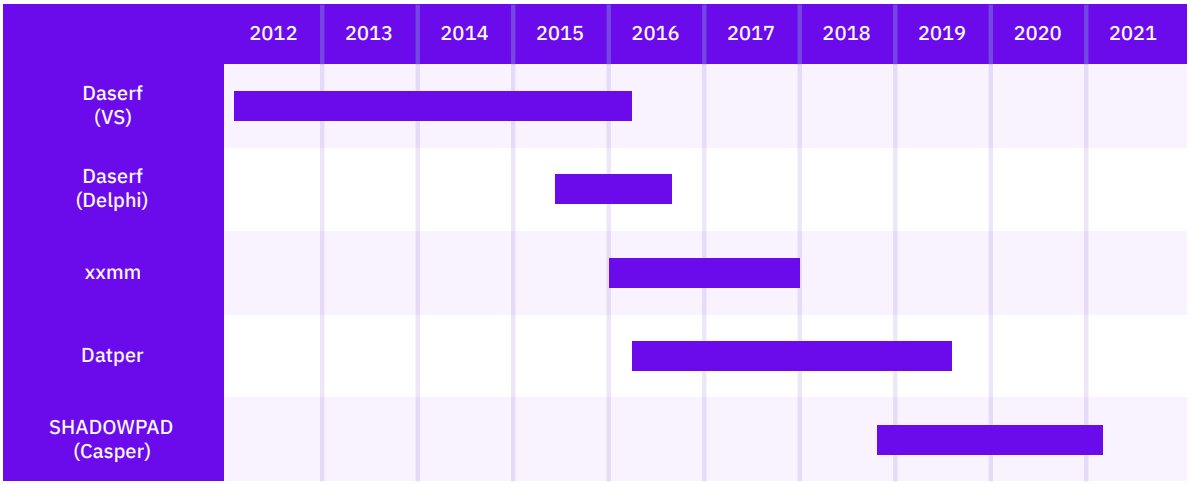


Fig 15: Timeline of backdoor used by Tick (picture)

[30]https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

This example of the shift from 'home-brewed' backdoors to acquired malware marks a noticeable change influenced by the privately sold malware platform ShadowPad. Acquiring a well-designed piece of malware significantly reduces the cost of operation and human resource needed to develop the malware in-house. The service provider also keeps enhancing the stability and usability of the backdoor with new features added, unlike much of the commodity malware found in cybercriminal circles or underground forums. Furthermore, the usage of shared malware provides espionage threat actors a layer of security in that it makes attribution much more difficult for defenders. The popularity of malware such as ShadowPad and Cobalt Strike among Chinese espionage groups makes campaign identification significantly harder.

CONCLUSION

The emergence of ShadowPad, a privately sold, well-developed and functional backdoor, offers threat actors a good opportunity to move away from self-developed backdoors. While it is well-designed – highly likely to be produced by an experienced malware developer – it is also under active maintenance on both its functionalities and its anti-forensics capabilities. For these threat actors, using ShadowPad as the primary backdoor significantly reduces the costs of development. They do not need to spend time developing new functionalities, adding new obfuscations to their samples or conducting testing on their backdoors before deployment. Besides, the nature of the "sold backdoor" reduces the chances of the actors being identified solely by the tool, allowing the actors to remain hidden and unidentified for longer.

For security researchers and analysts tracking China-based threat actors, the adoption of the "sold - or cracked - commercial backdoor" raises difficulties in ascertaining which threat actor they are investigating. More systematic ways – for instance, analysis on the relationship between indicators, long-term monitoring on the activities and campaigns – need to be developed in order to carry out analytically-sound attribution. Any claim made publicly on the attribution of ShadowPad users requires careful validation and strong evidentiary support so that it can help the community's effort in identifying Chinese espionage.

TECHNICAL INDICATORS

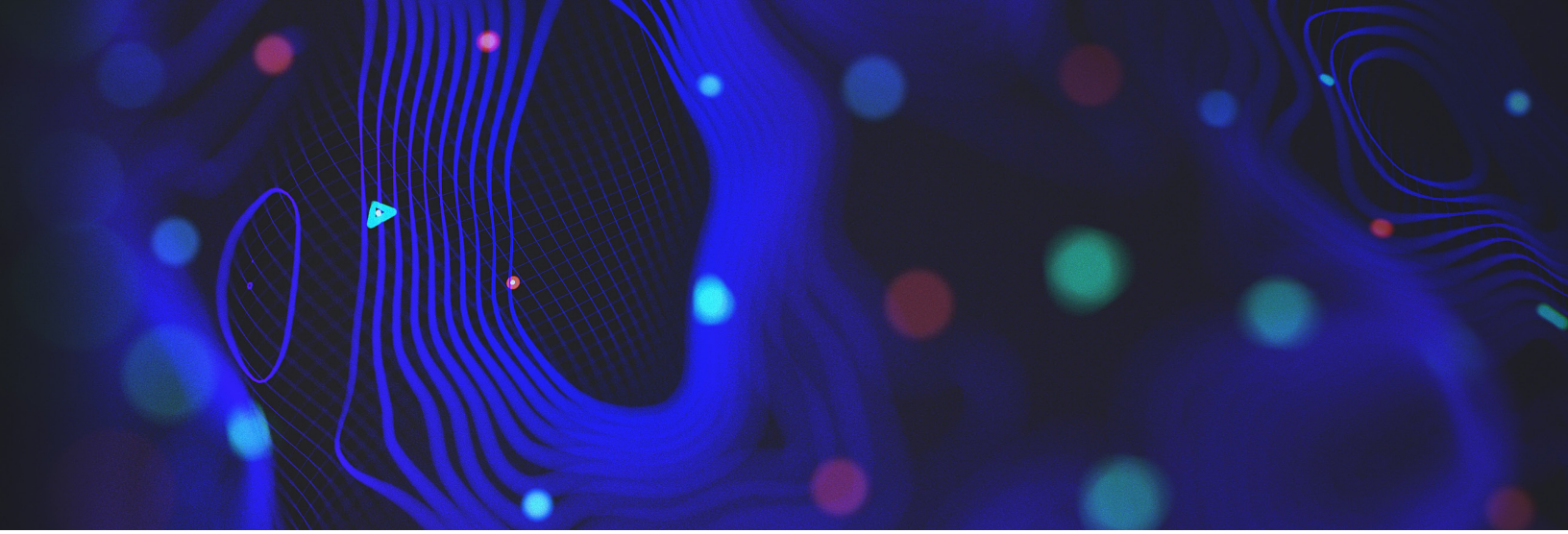
For a full list of hashes, C2 domains, and MITRE ATT&CK Indicators, see:
https://github.com/SentineLabs/Shadowpad

APPENDIX A

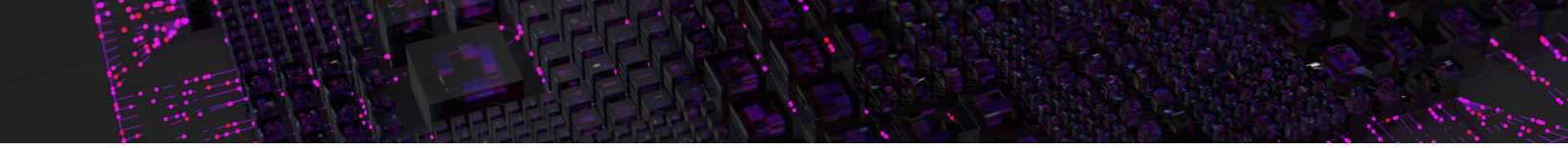
Plugins

SentinelOne has collected 22 unique plugins from SentinelOne's internal sample set.

ID	Plugin Name	Functionality	A sample with the plugin embedded in
0x64	Root	The main module	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x65	Plugins	Plugin manager: adding and removing plugins	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x66	Config	Configuration manager	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x67	Install	Malware installation for persistency	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x68	Online	Basic communication and command management with the C&C server	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x6A	ImpUser	User impersonation via token duplication	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0xC8	TCP	TCP C&C communication	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0xC9	HTTP	HTTP C&C communication	18d01a2742b1ffaea457b9a177d593a9acdacfc73 bbcf9d87cae90a254f559ed
0xCA	UDP	UDP C&C communication	2e6ef72d05b395224a03a73a50eaee1c9dc68297 6c99dde5317b76938cb669a4
0xCB	DNS	DNS C&C communication	9984d5b554b8dbfeffdb374e1c8eaf74af7109a0e 6b924b00ad5b878d0188895
0xCF	PIPE	Named pipe management	9f9d96e99cef99cbfe8d02899919a7f7220f2273b b36a084642f492dd3e473da



ID	Plugin Name	Functionality	A sample with the plugin embedded in
0x12C	Disk	File operation on the available disks	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x12D	Process	Process management	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x12E	Servcie	Service management	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x12F	Register	Registry management	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x130	Shell	Command line operation	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x131	PortMap	Port mapping	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x132	KeyLogger	Keylogger	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x133	Screen	Take screenshots and RDP simulation	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x137	Software	Get the information of all installed software	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x138	Hardware	Get the information of all hardware devices	9f9d96e99cef99cbfe8d02899919a7f7220f2273 bb36a084642f492dd3e473da
0x13D	RecentFiles	Retrieve the list of recently accessed files (.lnk)	fc117650688065deeb54e686f873359c2a56d2 3165567ab3f2a3b62498199fa9

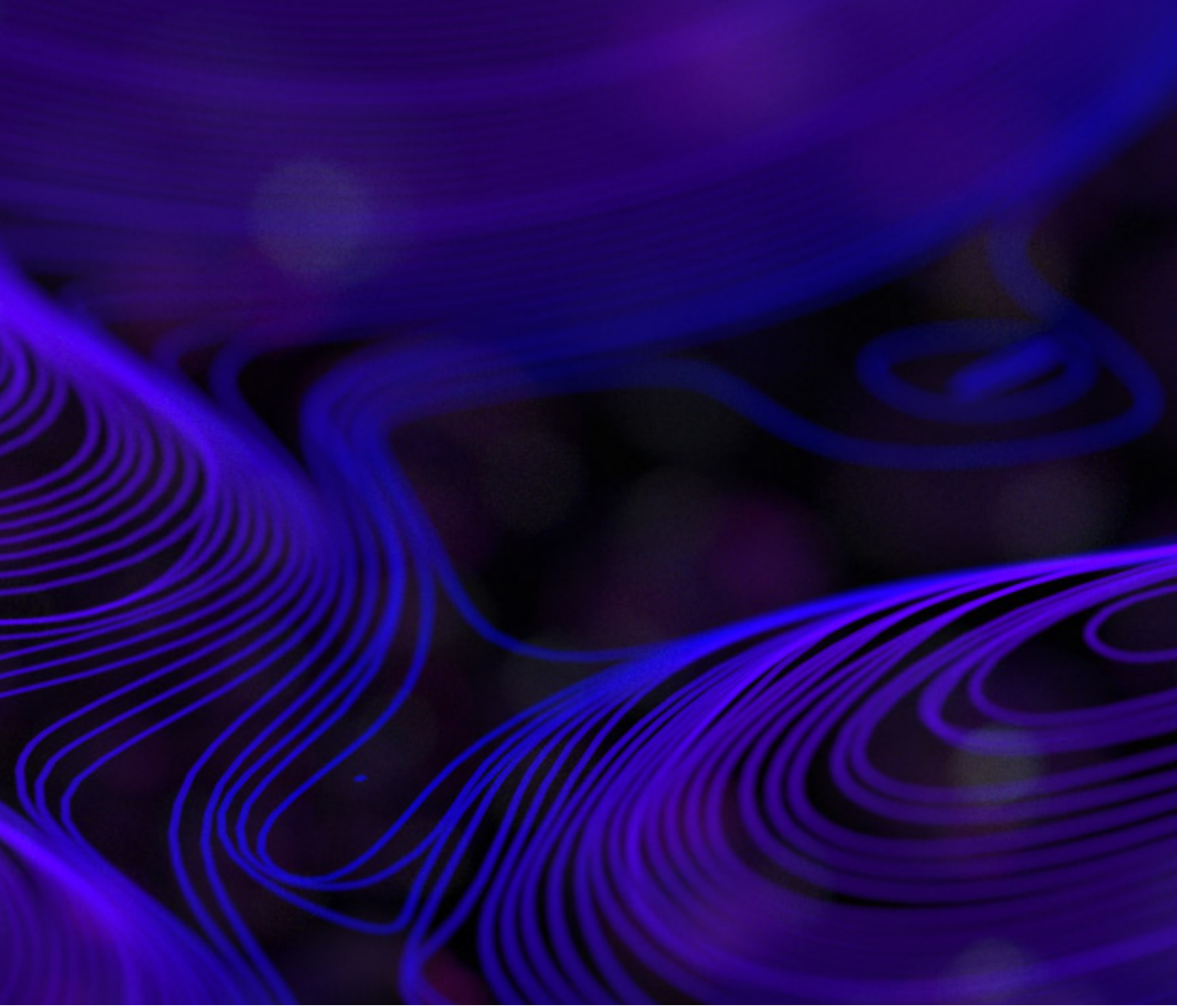


Configuration

The “Config” plugin decodes the configuration block and decrypts the encrypted strings embedded in the configuration block.

Offset	Data Type	Column
0x00	WORD	offset_product_key
0x02	WORD	offset_note
0x04	WORD	offset_binary_path
0x06	WORD	offset_service_name
0x08	WORD	offset_service_display_name
0x0A	WORD	offset_service_description
0x0C	WORD	offset_registry_key
0x0E	WORD	offset_registry_value
0x10 - 0x17	WORD	offset_process_spawn_and_inject 1-4
0x18 - 0x37	WORD	offset_c2 1-16
0x38 - 0x3F	WORD	offset_proxy_type 1-4
0x40 - 0x4F	DWORD	DNS 1-4
0x50	DWORD	timeout_multiplier

The constants of the string decryption algorithms and the starting offset of the encrypted string table differ between versions.



ABOUT SENTINELLABS

InfoSec works on a rapid iterative cycle where new discoveries occur daily and authoritative sources are easily drowned in the noise of partial information. SentinelLabs is an open venue for our threat researchers and vetted contributors to reliably share their latest findings with a wider community of defenders. No sales pitches, no nonsense. We are hunters, reversers, exploit developers, and tinkerers shedding light on the world of malware, exploits, APTs, and cybercrime across all platforms. SentinelLabs embodies our commitment to sharing openly –providing tools, context, and insights to strengthen our collective mission of a safer digital life for all. In addition to Microsoft operating systems, we also provide coverage and guidance on the evolving landscape that lives on Apple and macOS devices. https://labs.sentinelone.com/