SentinelOne

ShadowPad: the Masterpiece of Privately Sold Malware in Chinese Espionage

Yi-Jhen Hsieh, Joey Chen

Yi-Jhen Hsieh

Threat Intelligence Researcher @SentinelOne

Joey Chen

Threat Intelligence Researcher @SentinelOne

SentinelOne

Outline

- From PlugX to ShadowPad: the history
- Technical overview
- The business model of ShadowPad
- Which threat actors are using ShadowPad?
- Landscape shift: from developing backdoors to acquiring backdoors
- Mitigation advice

SentinelOne

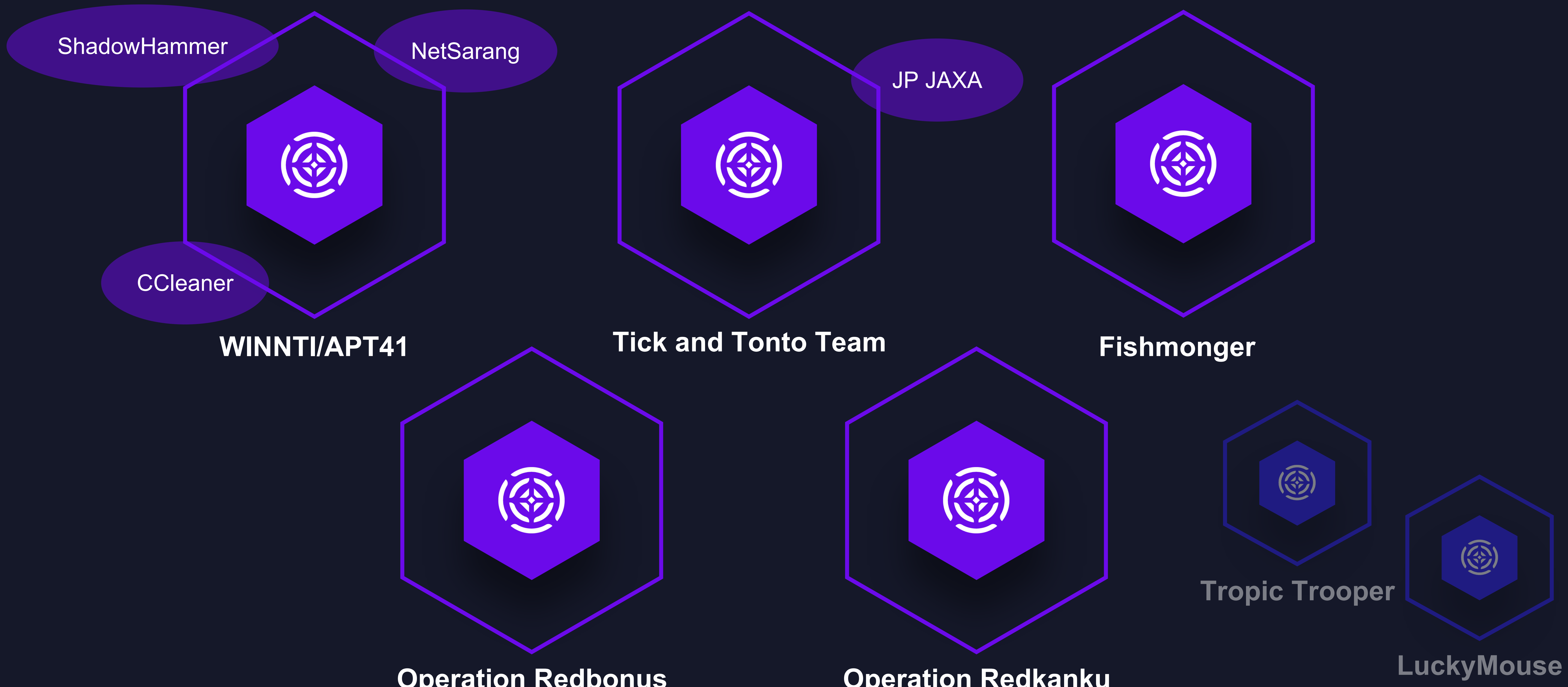
From PlugX to ShadowPad: the history

What is ShadowPad?

- A modular backdoor in shellcode format.
- The plugins can be plugged or unplugged remotely during runtime.

- It is used in several well-known campaigns as the primary backdoor for intrusion.

Which threat actors are using ShadowPad?



ShadowPad: A successor to PlugX?

	ShadowPad	PlugX
Shellcode	Yes	Yes
Plugin-based	Yes	Yes
Remote plugin management	Yes	No
Distribution	Privately shared	Widely used

SentinelOne

ShadowPad: A successor to PlugX? (cont.)

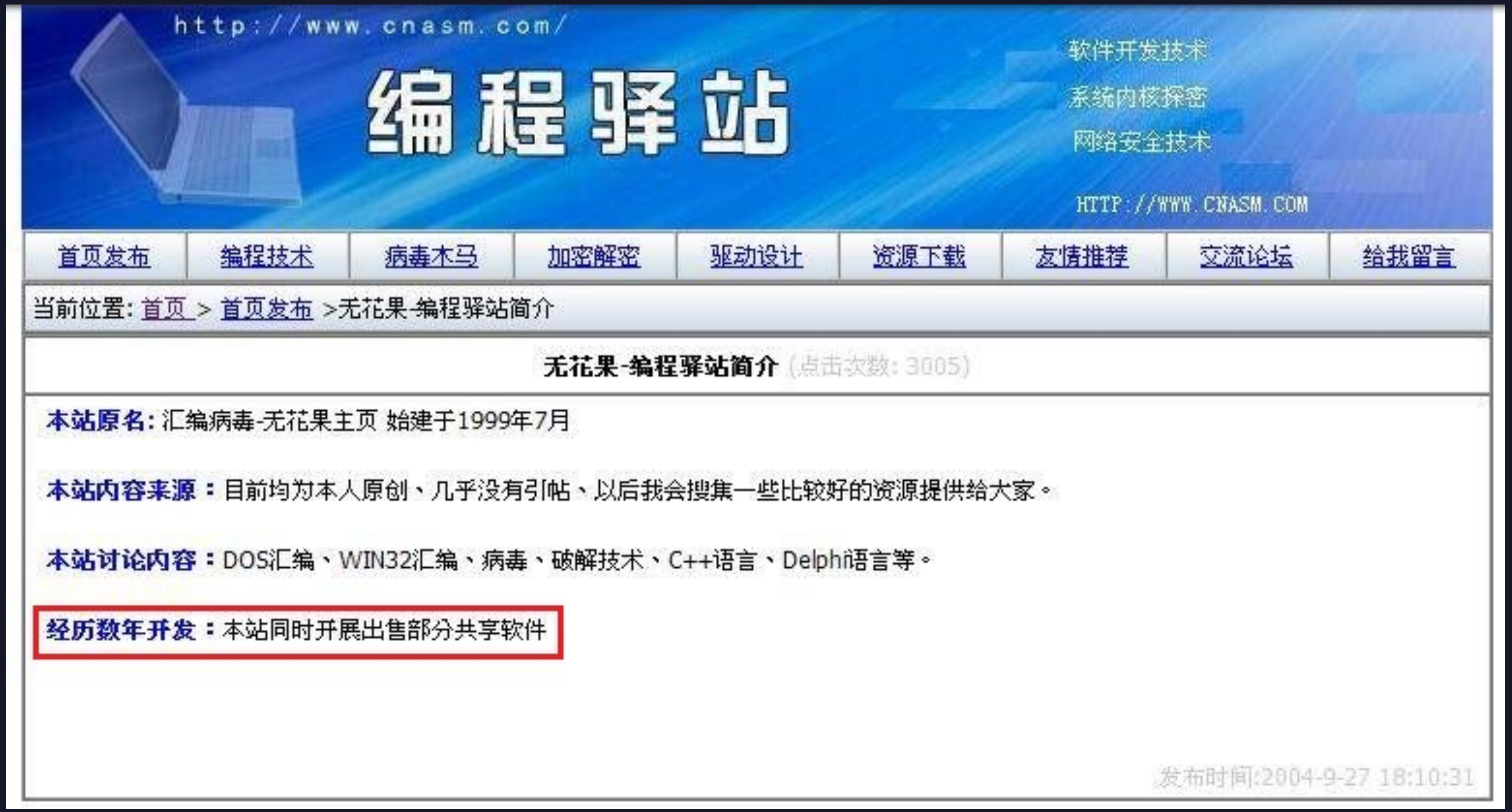
- The relationship between ShadowPad and PlugX
  - Comparisons on their codes have been discussed[1]
  - They share the same project name “SC” according to the PDB strings of their controllers
    - PlugX Controller: D:\My2014\SController(5.6)(天道)(匙)\SC\
    - ShadowPad Controller: X:\My2015\SC(1.1)\x64\Release\SoSvr.pdb

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

The alleged author of PlugX: whg

- whg aka 无花果, based in the Sichuan province of China
- His nickname was found in some of the PlugX samples[2]:
  - C:\Documents and Settings\whg\桌面\Plug\FastGui(LYT)\Shell\Release\Shell.pdb
  - C:\Users\whg\Desktop\Plug\FastGui(LYT)\Shell\Release\Shell.pdb

- He had a solid track record of developing backdoors and hacking tools, while he claimed to sell some "shared software".
  - Also, he had deep connection with Rose, one of the threat actors in APT41.



当前位置: 首页 > 首页发布 >无花果-编程驿站简介

无花果-编程驿站简介 (点击次数: 3005)

本站原名: 汇编病毒-无花果主页 始建于1999年7月

本站内容来源: 目前均为本人原创、几乎没有引帖、以后我会搜集一些比较好的资源提供给大家。

本站讨论内容: DOS汇编、WIN32汇编、病毒、破解技术、C++语言、Delphi语言等。

经历数年开发: 本站同时开展出售部分共享软件

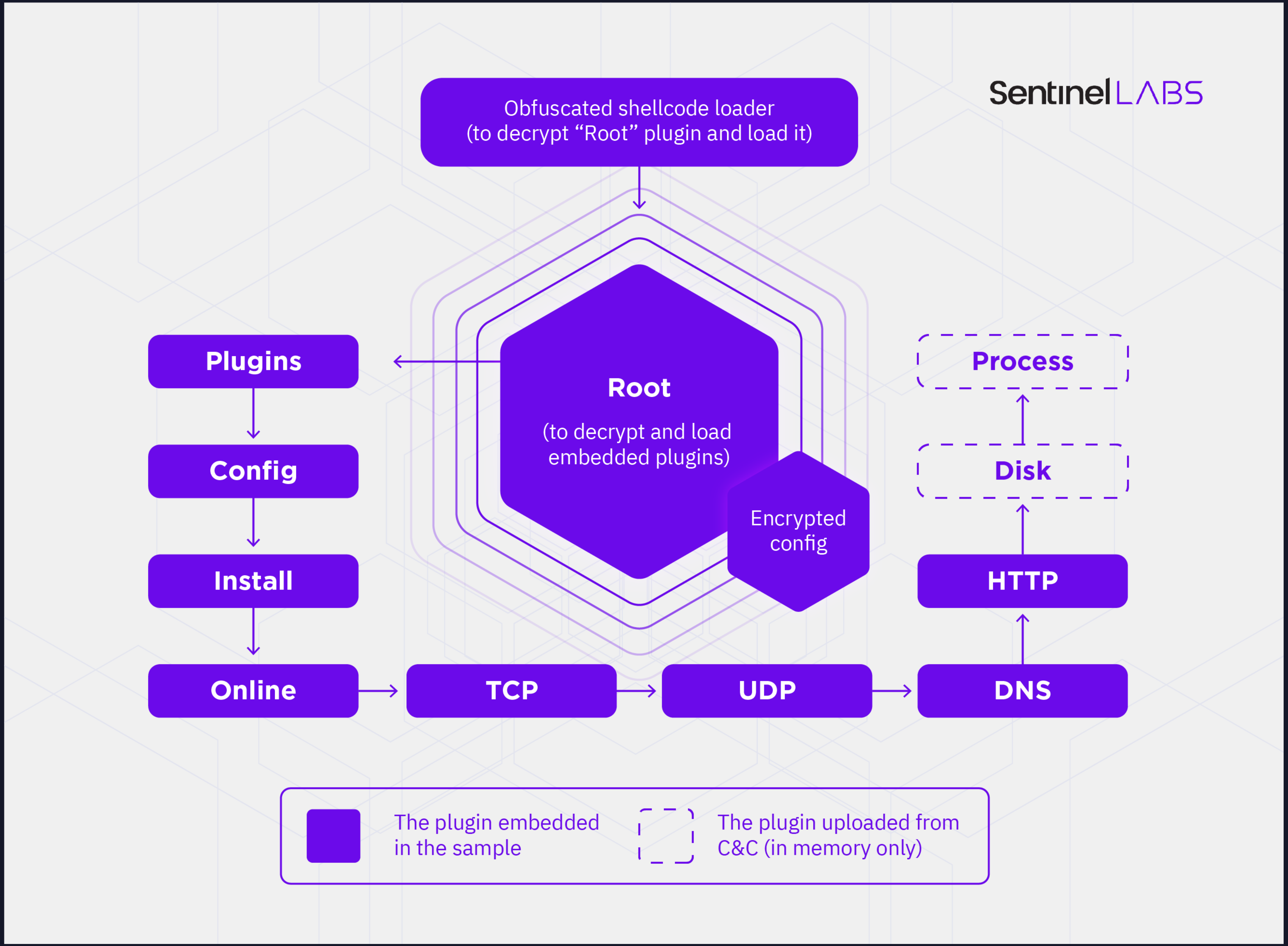
发布时间:2004-9-27 18:10:31

[2] https://cybersecurity.att.com/blogs/labs-research/tracking-down-the-author-of-the-plugx-rat

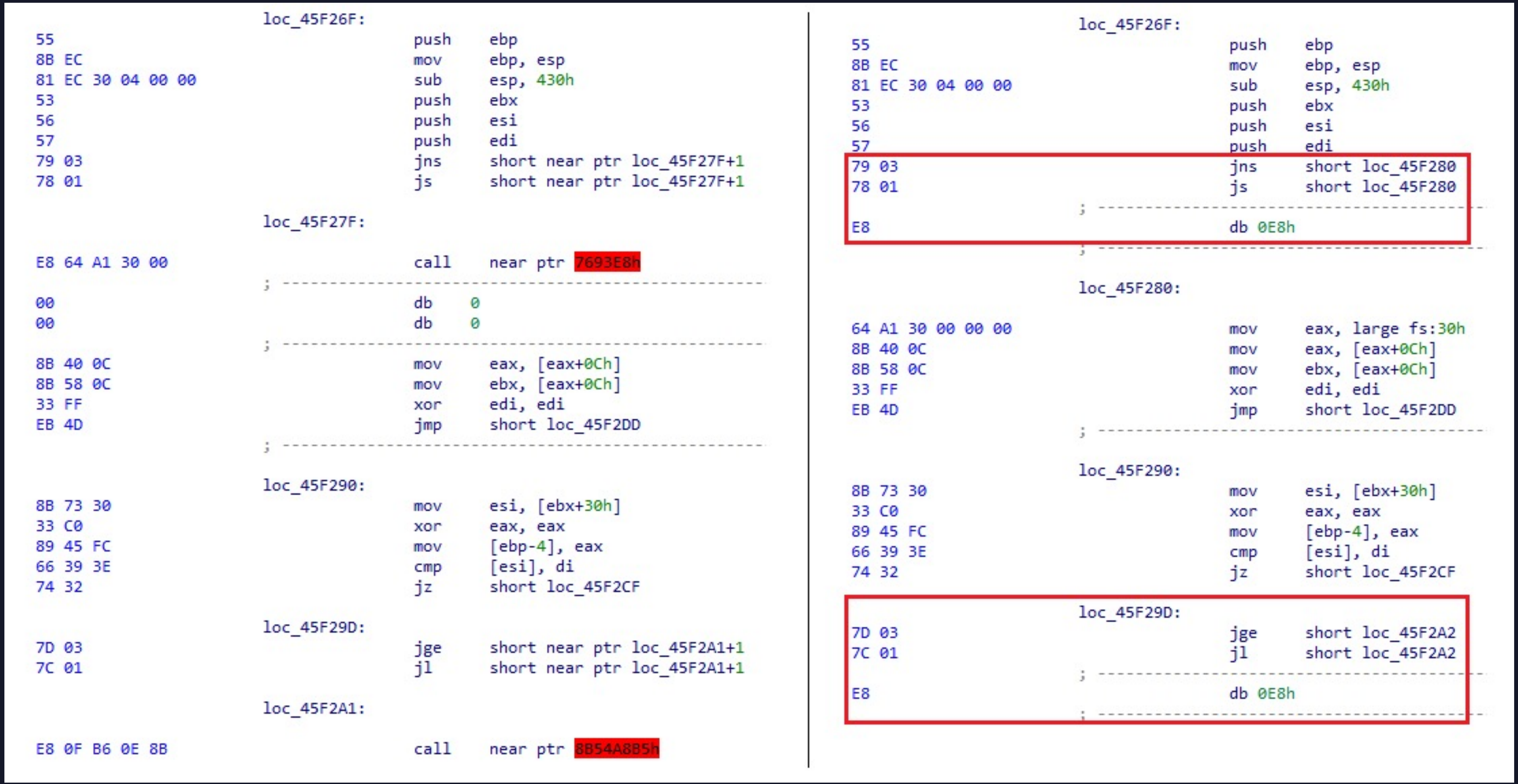
SentinelOne®

Technical overview

The modular design


SentinelLABS
Obfuscated shellcode loader (to decrypt "Root" plugin and load it)
Root
(to decrypt and load embedded plugins)
Encrypted config
Plugins
Config
Install
Online
TCP
UDP
DNS
HTTP
Disk
Process
The plugin embedded in the sample
The plugin uploaded from C&C (in memory only)

The shellcode loader

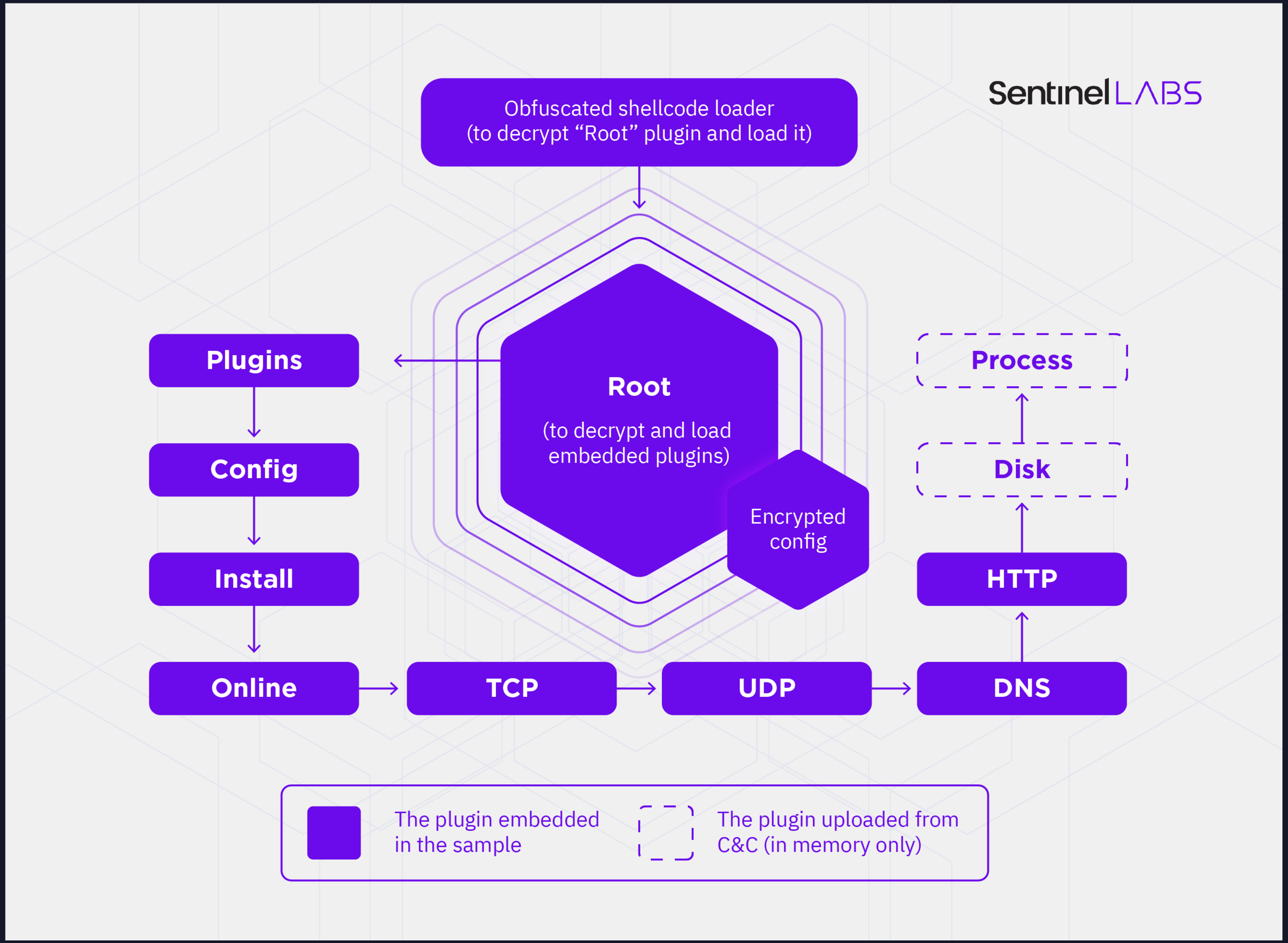


```
                        loc_45F26F:
55                                      push    ebp
8B EC                                   mov     ebp, esp
81 EC 30 04 00 00                       sub     esp, 430h
53                                      push    ebx
56                                      push    esi
57                                      push    edi
79 03                                   jns     short near ptr loc_45F27F+1
78 01                                   js      short near ptr loc_45F27F+1

                        loc_45F27F:

E8 64 A1 30 00                          call    near ptr 7693E8h
                        ; -----------------------------------------------------
00                                      db    0
00                                      db    0
                        ; -----------------------------------------------------
8B 40 0C                                mov     eax, [eax+0Ch]
8B 58 0C                                mov     ebx, [eax+0Ch]
33 FF                                   xor     edi, edi
EB 4D                                   jmp     short loc_45F2DD
                        ; -----------------------------------------------------

                        loc_45F290:
8B 73 30                                mov     esi, [ebx+30h]
33 C0                                   xor     eax, eax
89 45 FC                                mov     [ebp-4], eax
66 39 3E                                cmp     [esi], di
74 32                                   jz      short loc_45F2CF

                        loc_45F29D:
7D 03                                   jge     short near ptr loc_45F2A1+1
7C 01                                   jl      short near ptr loc_45F2A1+1

                        loc_45F2A1:

E8 0F B6 0E 8B                          call    near ptr 8B54A8B5h
```

```
                        loc_45F26F:
55                                      push    ebp
8B EC                                   mov     ebp, esp
81 EC 30 04 00 00                       sub     esp, 430h
53                                      push    ebx
56                                      push    esi
57                                      push    edi
79 03                                   jns     short loc_45F280
78 01                                   js      short loc_45F280
                        ; -----------------------------------------------------
E8                                      db 0E8h
                        ; -----------------------------------------------------

                        loc_45F280:

64 A1 30 00 00 00                       mov     eax, large fs:30h
8B 40 0C                                mov     eax, [eax+0Ch]
8B 58 0C                                mov     ebx, [eax+0Ch]
33 FF                                   xor     edi, edi
EB 4D                                   jmp     short loc_45F2DD
                        ; -----------------------------------------------------

                        loc_45F290:
8B 73 30                                mov     esi, [ebx+30h]
33 C0                                   xor     eax, eax
89 45 FC                                mov     [ebp-4], eax
66 39 3E                                cmp     [esi], di
74 32                                   jz      short loc_45F2CF

                        loc_45F29D:
7D 03                                   jge     short loc_45F2A2
7C 01                                   jl      short loc_45F2A2
                        ; -----------------------------------------------------
E8                                      db 0E8h
                        ; -----------------------------------------------------
```

The plugins

- Every plugin is decrypted, loaded into memory, and referenced in a LinkedList.
- Additional plugins could be uploaded from the C&C servers.

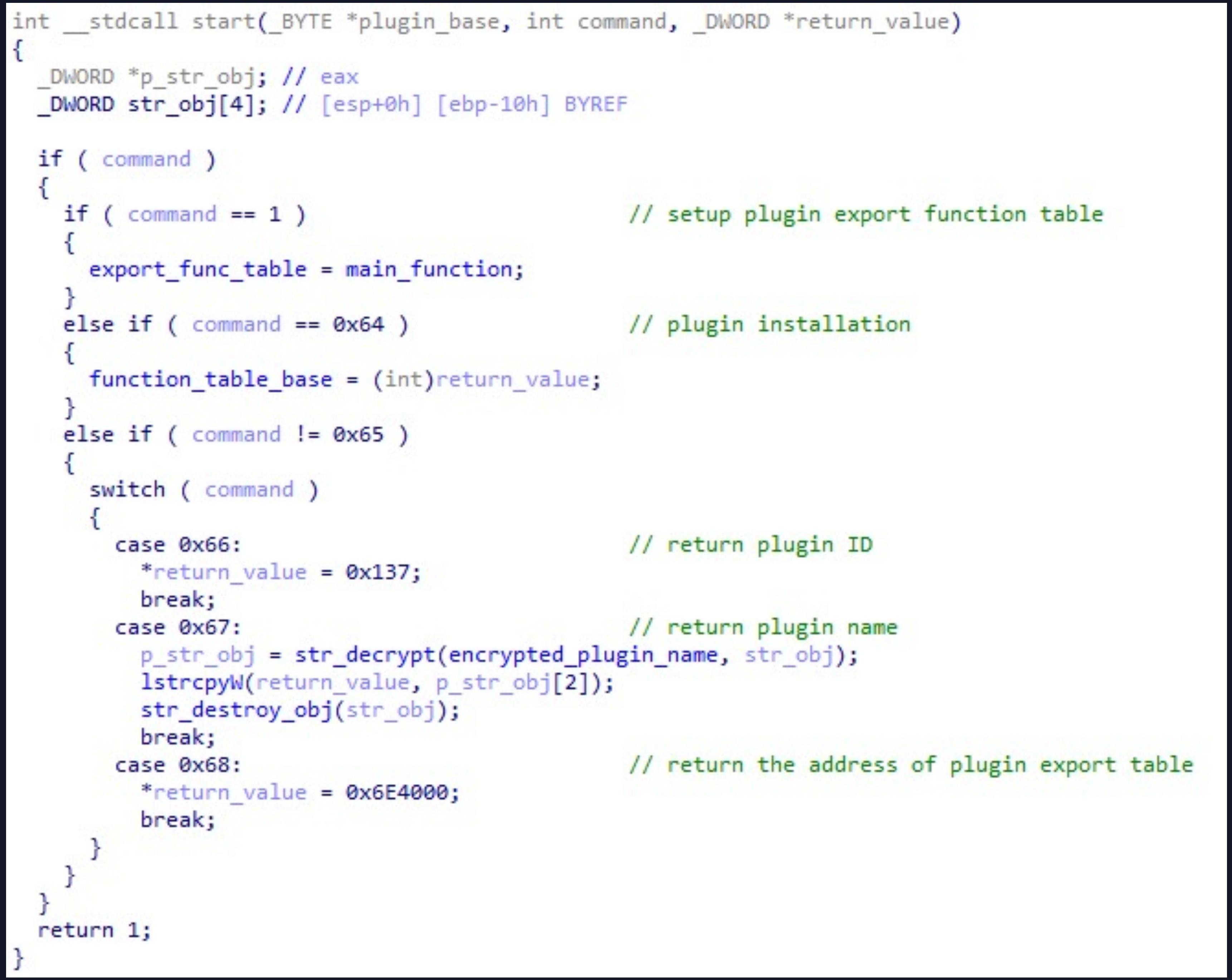


SentinelLABS
Obfuscated shellcode loader (to decrypt “Root” plugin and load it)
Root (to decrypt and load embedded plugins)
Encrypted config
Plugins
Config
Install
Online
TCP
UDP
DNS
HTTP
Disk
Process
The plugin embedded in the sample
The plugin uploaded from C&C (in memory only)

```
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;
}
```

The start function of a plugin

- 0x01: Setup the export function table of the plugin
- 0x64: Setup the plugin
- 0x66: Return **the plugin ID**
- 0x67: Return **the plugin name**
- 0x68: Return the address of the export function table



```
int __stdcall start(_BYTE *plugin_base, int command, _DWORD *return_value)
{
  _DWORD *p_str_obj; // eax
  _DWORD str_obj[4]; // [esp+0h] [ebp-10h] BYREF

  if ( command )
  {
    if ( command == 1 )                              // setup plugin export function table
    {
      export_func_table = main_function;
    }
    else if ( command == 0x64 )                      // plugin installation
    {
      function_table_base = (int)return_value;
    }
    else if ( command != 0x65 )
    {
      switch ( command )
      {
        case 0x66:                                   // return plugin ID
          *return_value = 0x137;
          break;
        case 0x67:                                   // return plugin name
          p_str_obj = str_decrypt(encrypted_plugin_name, str_obj);
          lstrcpyW(return_value, p_str_obj[2]);
          str_destroy_obj(str_obj);
          break;
        case 0x68:                                   // return the address of plugin export table
          *return_value = 0x6E4000;
          break;
      }
    }
  }
  return 1;
}
```

22 unique plugins

Basic Set

- Root
- Plugins
- Config
- Install
- Online
- TCP
- HTTP
- UDP
- DNS

- ImpUser
- PIPE
- Disk
- Process
- Servcie
- Register
- Shell
- PortMap
- Keylogger

Utilities

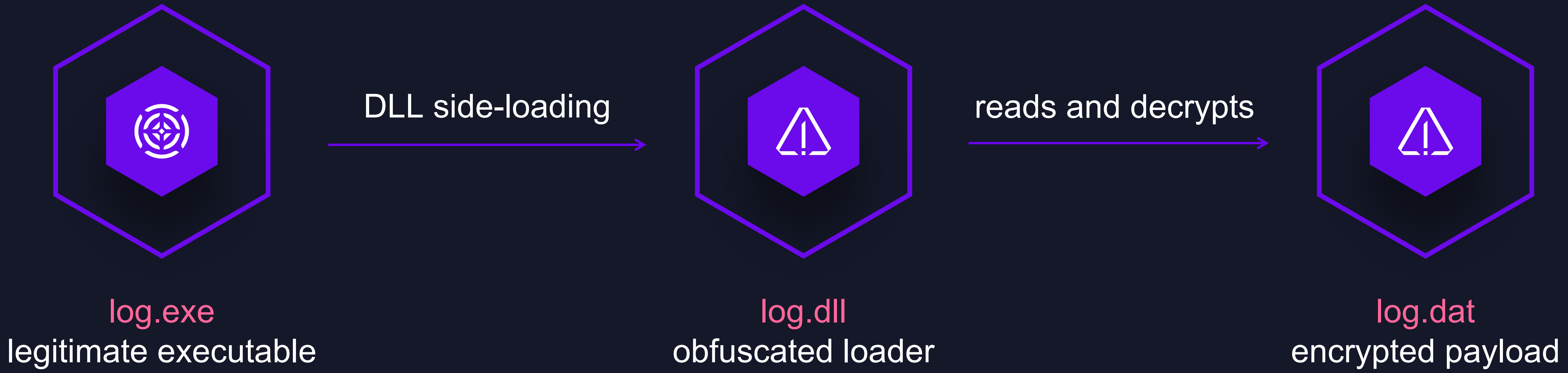
- Screen
- Software
- Hardware
- RecentFiles

The configuration

Offset	Data Type	Column
0x00	WORD	offset_product_key
0x02	WORD	offset_note
0x04	WORD	offset_binary_path
0x06	WORD	offset_service_name (default: MyTest)
0x08	WORD	offset_service_display_name (default: MyTest)
0x0A	WORD	offset_service_description (default: MyTest)
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

New version: the infection chain

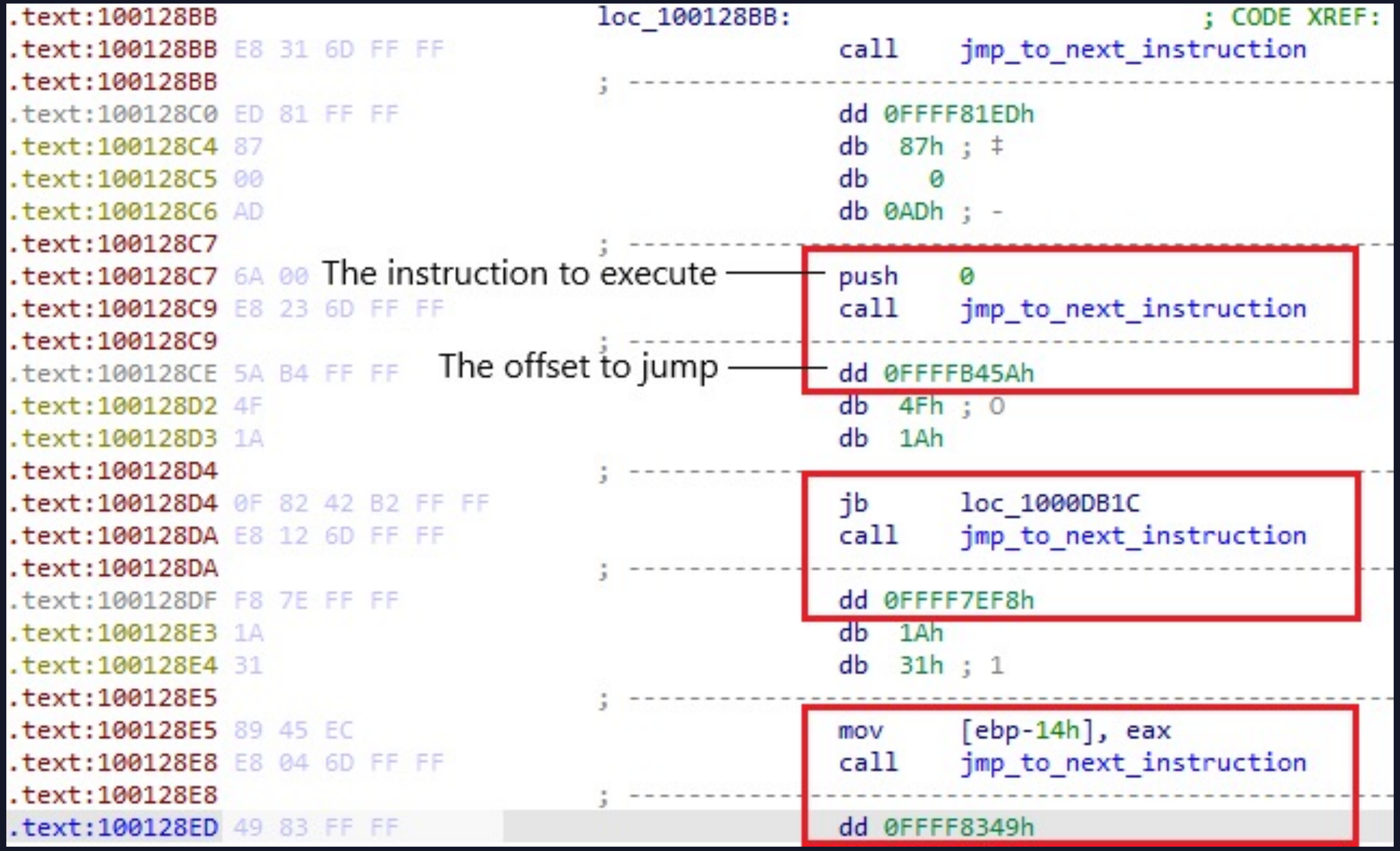
- First found in 2020 by PT security[3]



[3] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/#id6

New version, more obfuscation

- First found in 2020 by PT security[3]
- The control flow is flattened by instruction



```
.text:100128BB                        loc_100128BB:                           ; CODE XREF:
.text:100128BB E8 31 6D FF FF                         call    jmp_to_next_instruction
.text:100128BB                        ; ---------------------------------------------------
.text:100128C0 ED 81 FF FF                            dd 0FFFF81EDh
.text:100128C4 87                                     db  87h ; ‡
.text:100128C5 00                                     db    0
.text:100128C6 AD                                     db 0ADh ; -
.text:100128C7                        ; ---------------------------------------------------
.text:100128C7 6A 00                                  push    0
.text:100128C9 E8 23 6D FF FF                         call    jmp_to_next_instruction
.text:100128C9                        ; ---------------------------------------------------
.text:100128CE 5A B4 FF FF                            dd 0FFFFB45Ah
.text:100128D2 4F                                     db  4Fh ; O
.text:100128D3 1A                                     db  1Ah
.text:100128D4                        ; ---------------------------------------------------
.text:100128D4 0F 82 42 B2 FF FF                      jb      loc_1000DB1C
.text:100128DA E8 12 6D FF FF                         call    jmp_to_next_instruction
.text:100128DA                        ; ---------------------------------------------------
.text:100128DF F8 7E FF FF                            dd 0FFFF7EF8h
.text:100128E3 1A                                     db  1Ah
.text:100128E4 31                                     db  31h ; 1
.text:100128E5                        ; ---------------------------------------------------
.text:100128E5 89 45 EC                               mov     [ebp-14h], eax
.text:100128E8 E8 04 6D FF FF                         call    jmp_to_next_instruction
.text:100128E8                        ; ---------------------------------------------------
.text:100128ED 49 83 FF FF                            dd 0FFFF8349h
```

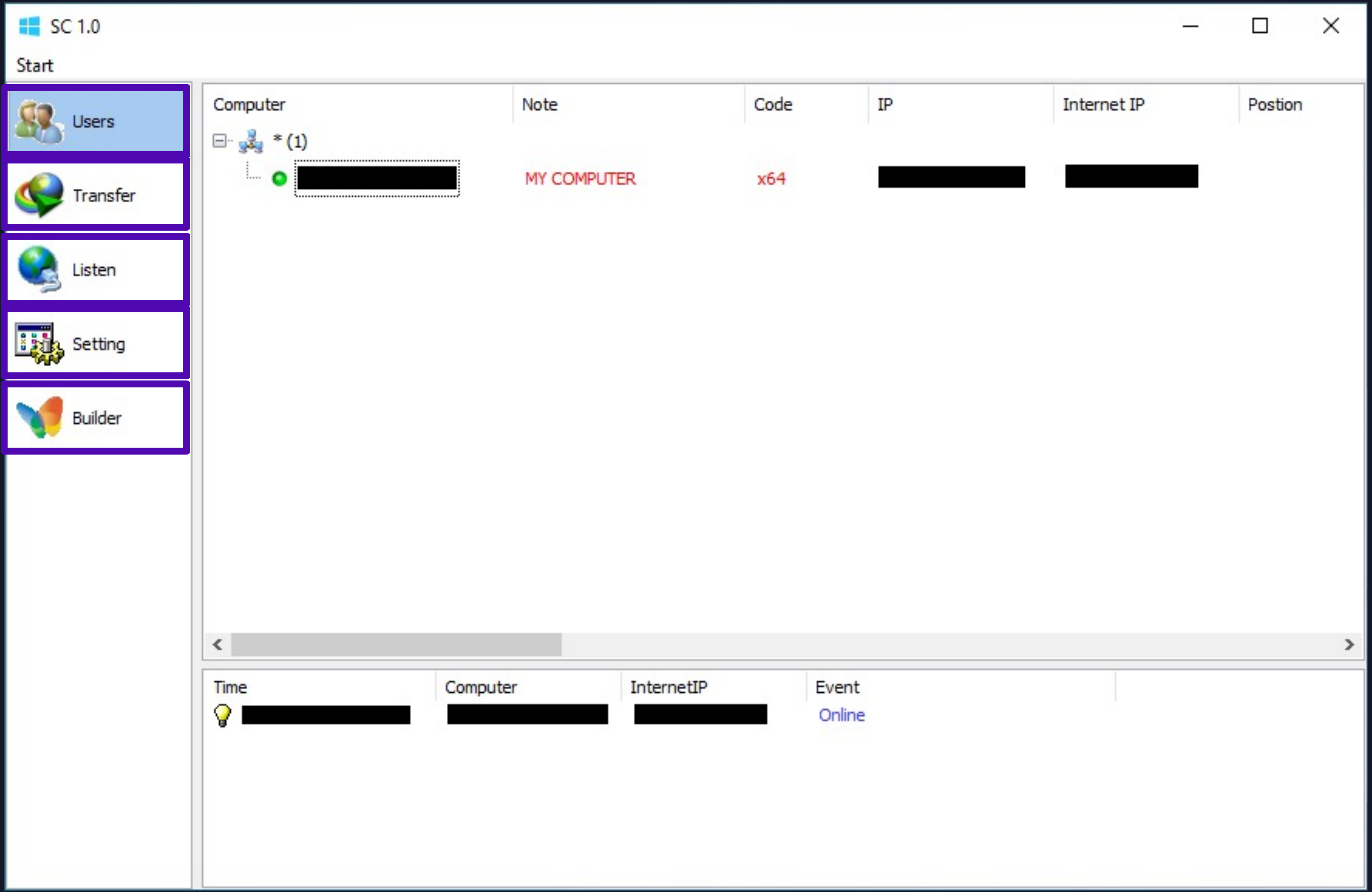
The configuration of the new version

Offset	Data Type	Column
0x00	WORD	offset_date (product key)
0x02	WORD	offset_note
0x04	WORD	offset_install_directory
0x06	WORD	offset_executable_name
0x08	WORD	offset_loader_name
0x0A	WORD	offset_payload_name
0x0C	WORD	offset_service_name
0x0E	WORD	offset_service_display_name
0x10	WORD	offset_service_description
0x12	WORD	offset_reg_key
0x14	WORD	offset_reg_value
0x16 - 0x1D	WORD	offset_process_spawn_and_inject 1-4
0x1E - 0x4F	WORD	offset_c2 1-16
0x50 - 0x57	WORD	offset_proxy_type 1-4
0x58 - 0x67	DWORD	DNS 1-4
0x68	DWORD	timeout_multiplier

SentinelOne

The controller

- Version 1.0, 2015
- Written in Delphi
- All-in-one:
  builder + C&C listener

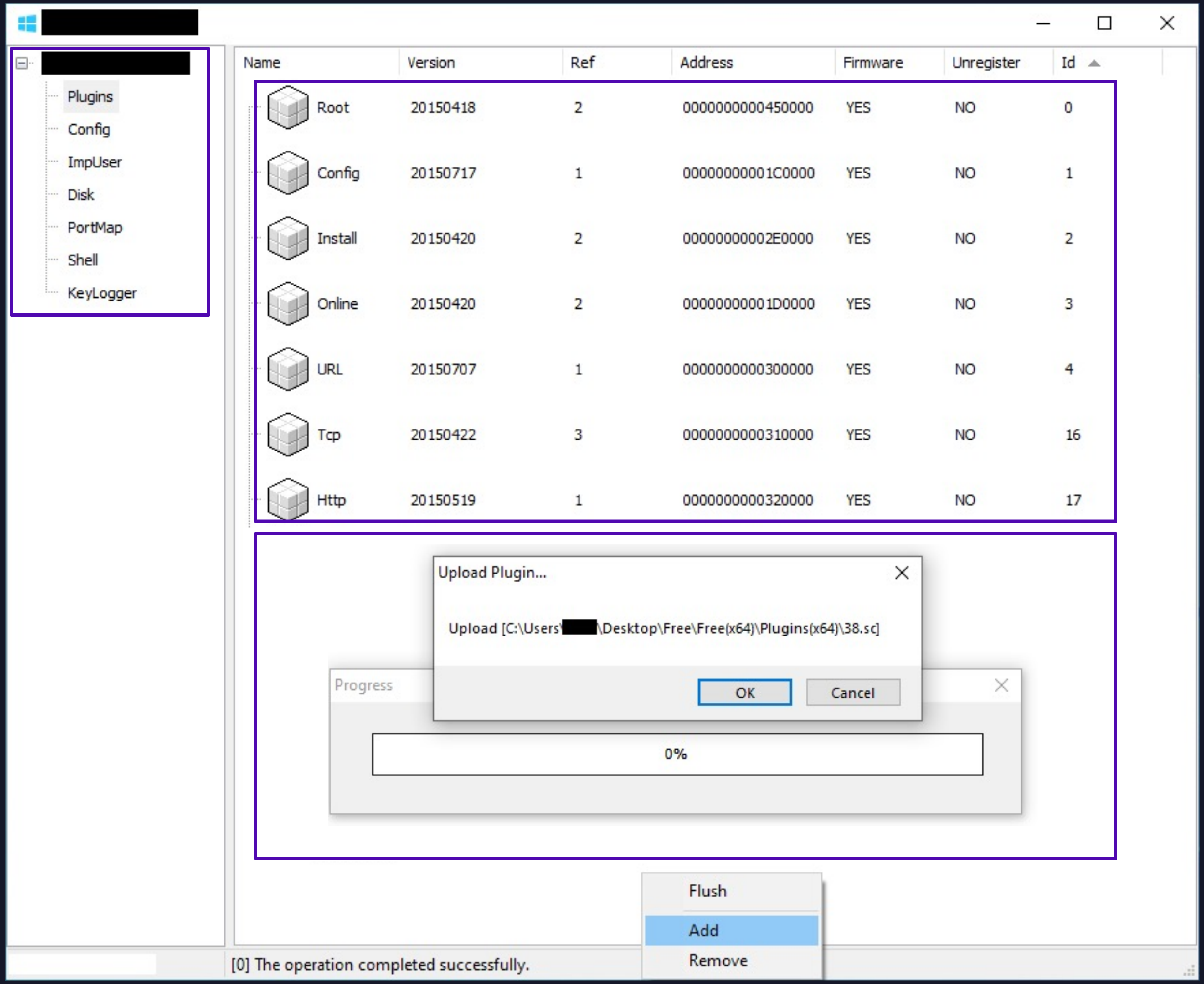


Computer	Note	Code	IP	Internet IP	Postion
* (1)					
[redacted]	MY COMPUTER	x64	[redacted]	[redacted]	

Time	Computer	InternetIP	Event
[redacted]	[redacted]	[redacted]	Online

The management console

- Default plugins v.s. uploaded plugins
- The control pages of the plugins are fixed



[redacted]

[redacted]
- Plugins
- Config
- ImpUser
- Disk
- PortMap
- Shell
- KeyLogger

Name	Version	Ref	Address	Firmware	Unregister	Id
Root	20150418	2	0000000000450000	YES	NO	0
Config	20150717	1	00000000001C0000	YES	NO	1
Install	20150420	2	00000000002E0000	YES	NO	2
Online	20150420	2	00000000001D0000	YES	NO	3
URL	20150707	1	0000000000300000	YES	NO	4
Tcp	20150422	3	0000000000310000	YES	NO	16
Http	20150519	1	0000000000320000	YES	NO	17

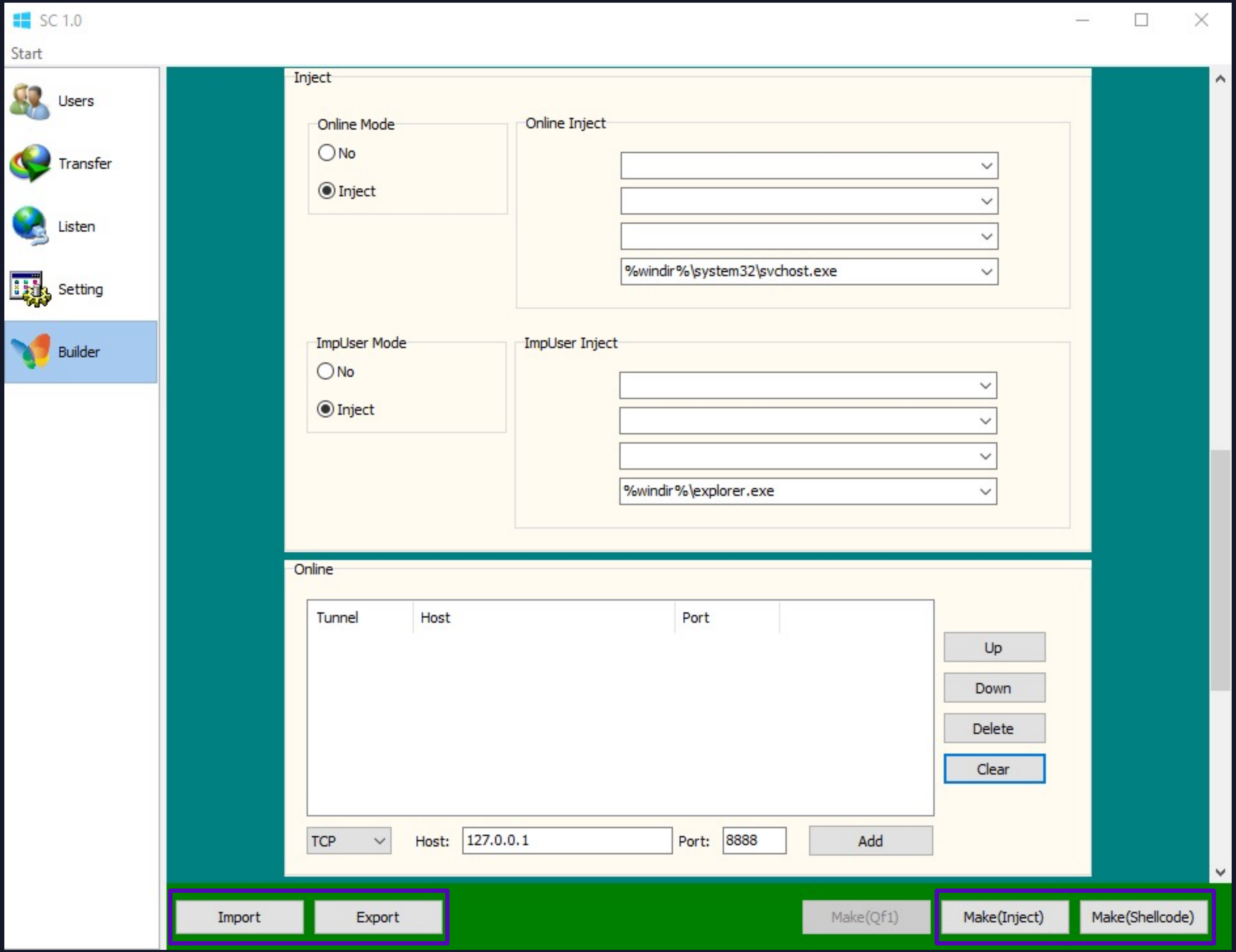
Upload Plugin...

Upload [C:\Users\[redacted]\Desktop\Free\Free(x64)\Plugins(x64)\38.sc]

[0] The operation completed successfully.

The builder

- Campaign code
- Notes
- Anti-debugger settings
- Installation settings (service and registry)
- Process injection settings
- C&C servers
- Connection modes



Online Mode: No [✓ Inject]

Online Inject: %windir%\system32\svchost.exe

ImpUser Mode: No [✓ Inject]

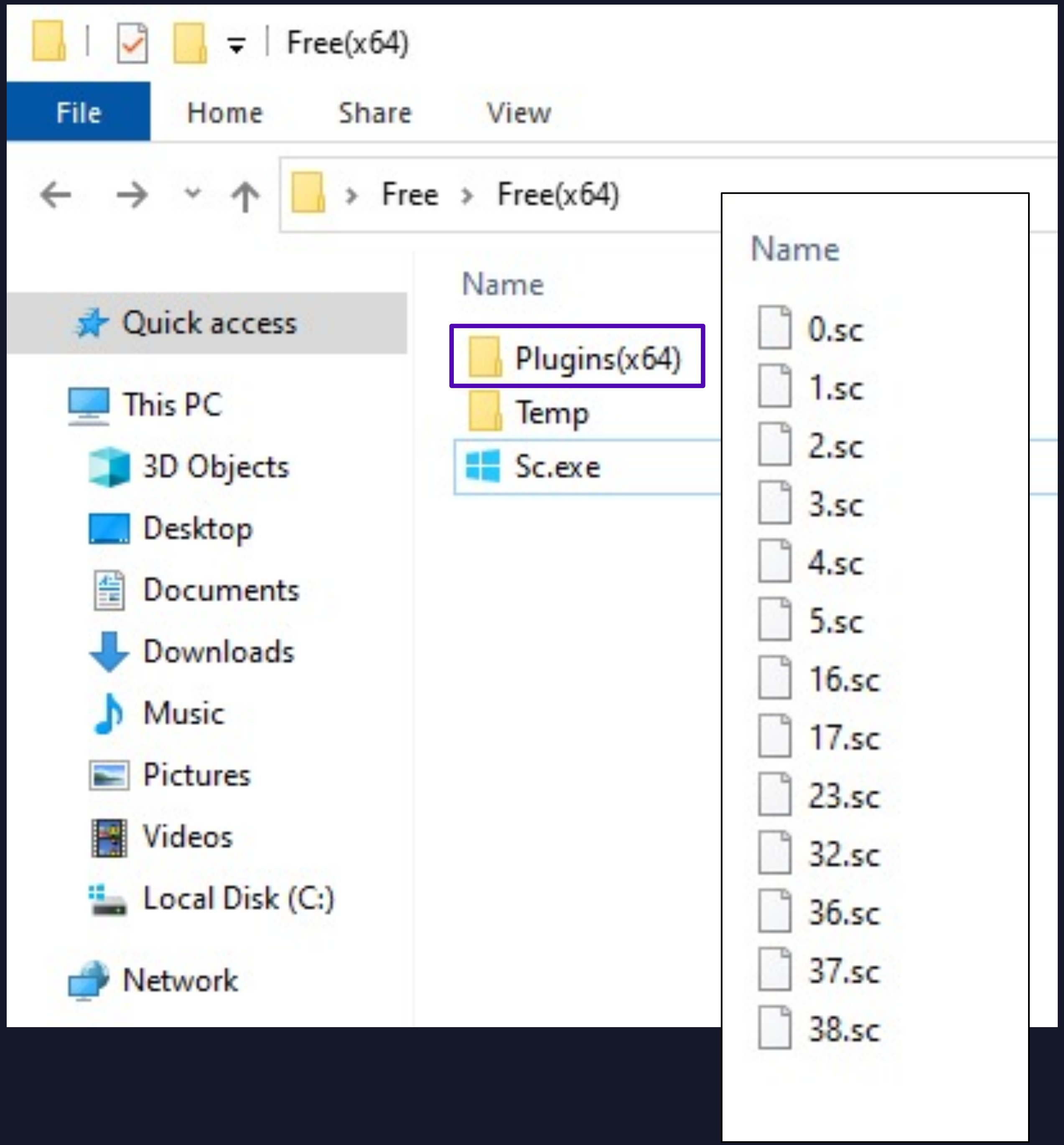
ImpUser Inject: %windir%\explorer.exe

TCP Host: 127.0.0.1 Port: 8888

SentinelOne®

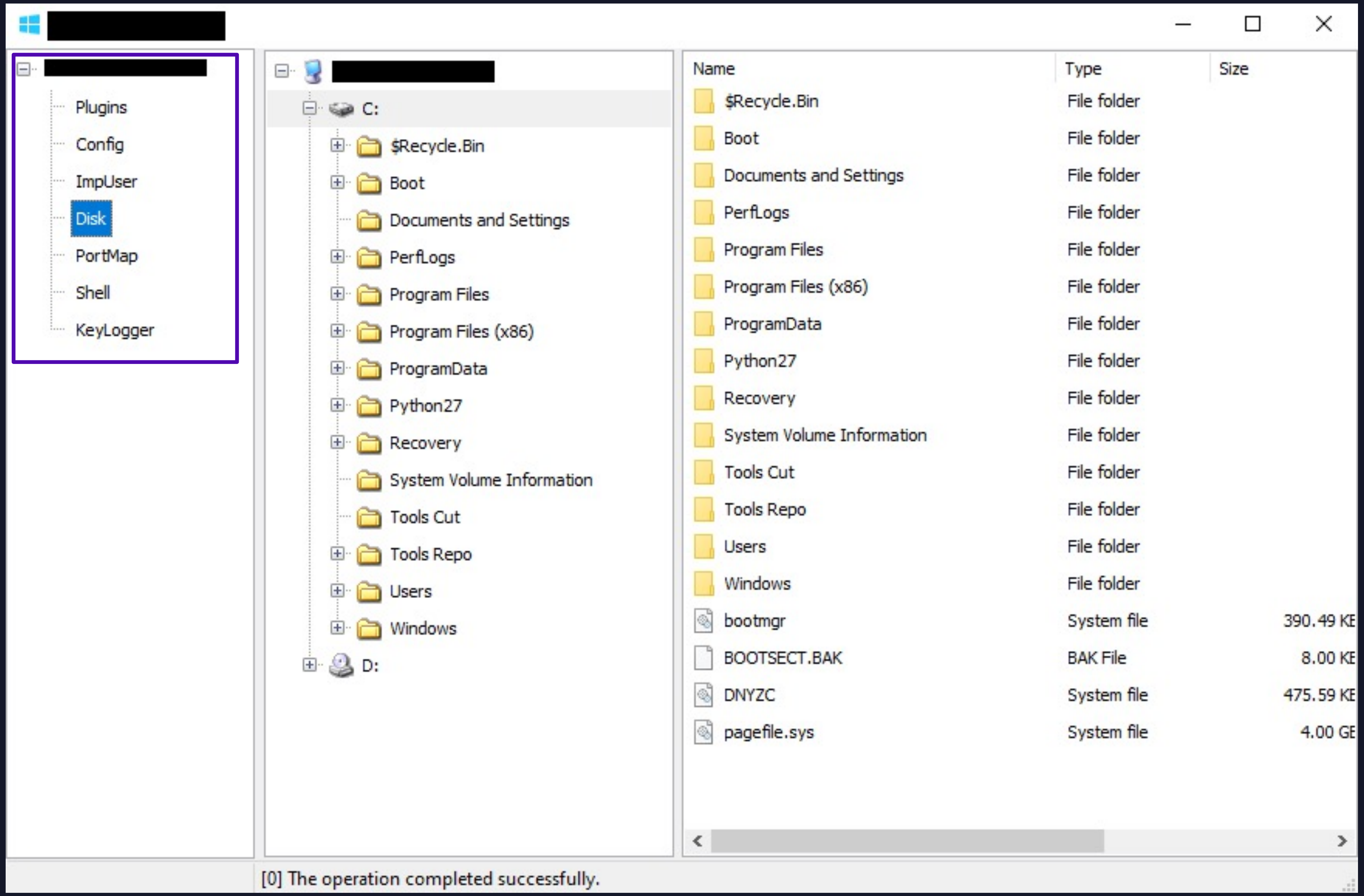
The business model of ShadowPad

How flexible is the controller?



- The plugins are place in a directory.
- In theory, you can upload any plugin within the correct format.

How flexible is the controller?


[redacted]

[redacted]
- Plugins
- Config
- ImpUser
- Disk
- PortMap
- Shell
- KeyLogger

[redacted]
- C:
  - $Recycle.Bin
  - Boot
  - Documents and Settings
  - PerfLogs
  - Program Files
  - Program Files (x86)
  - ProgramData
  - Python27
  - Recovery
  - System Volume Information
  - Tools Cut
  - Tools Repo
  - Users
  - Windows
- D:

Name	Type	Size
$Recycle.Bin	File folder	
Boot	File folder	
Documents and Settings	File folder	
PerfLogs	File folder	
Program Files	File folder	
Program Files (x86)	File folder	
ProgramData	File folder	
Python27	File folder	
Recovery	File folder	
System Volume Information	File folder	
Tools Cut	File folder	
Tools Repo	File folder	
Users	File folder	
Windows	File folder	
bootmgr	System file	390.49 KB
BOOTSECT.BAK	BAK File	8.00 KB
DNYZC	System file	475.59 KB
pagefile.sys	System file	4.00 GB

[0] The operation completed successfully.

- … but the user cannot interact with the plugins without an interface
  - The interfaces are hardcoded in the controller
  - No options to add a new interface

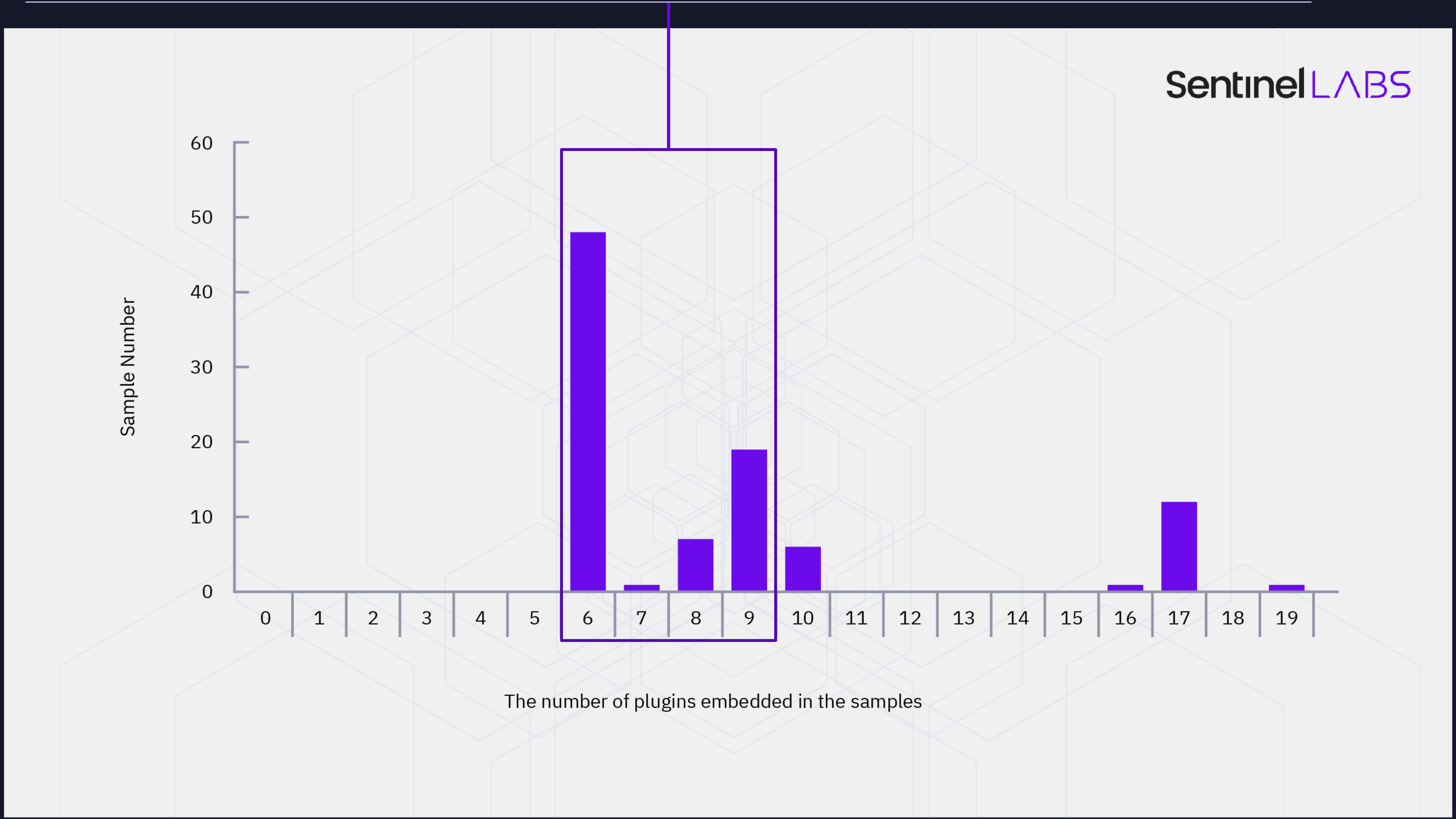
A piece of sold malware with extendibility

- ShadowPad is not extendible by the users except the original developer.
  - Not originally designed as a framework.

- The developer can remove a plugin from the package easily.
  - Just remove the plugins from the directory.

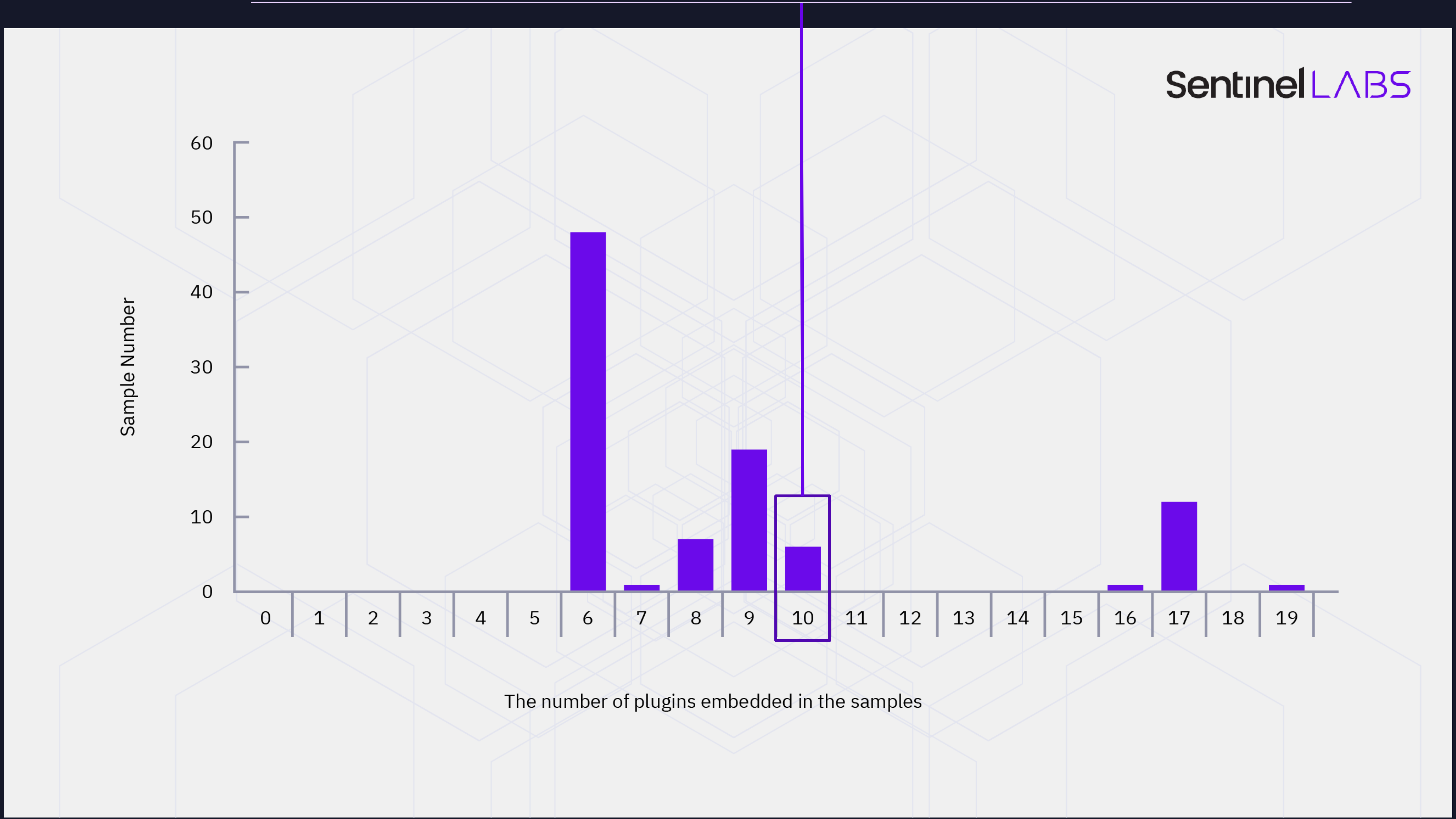
Selling the plugins separately

Basic set: Root, Plugins, Config, Install, Online, TCP, HTTP, UDP, DNS

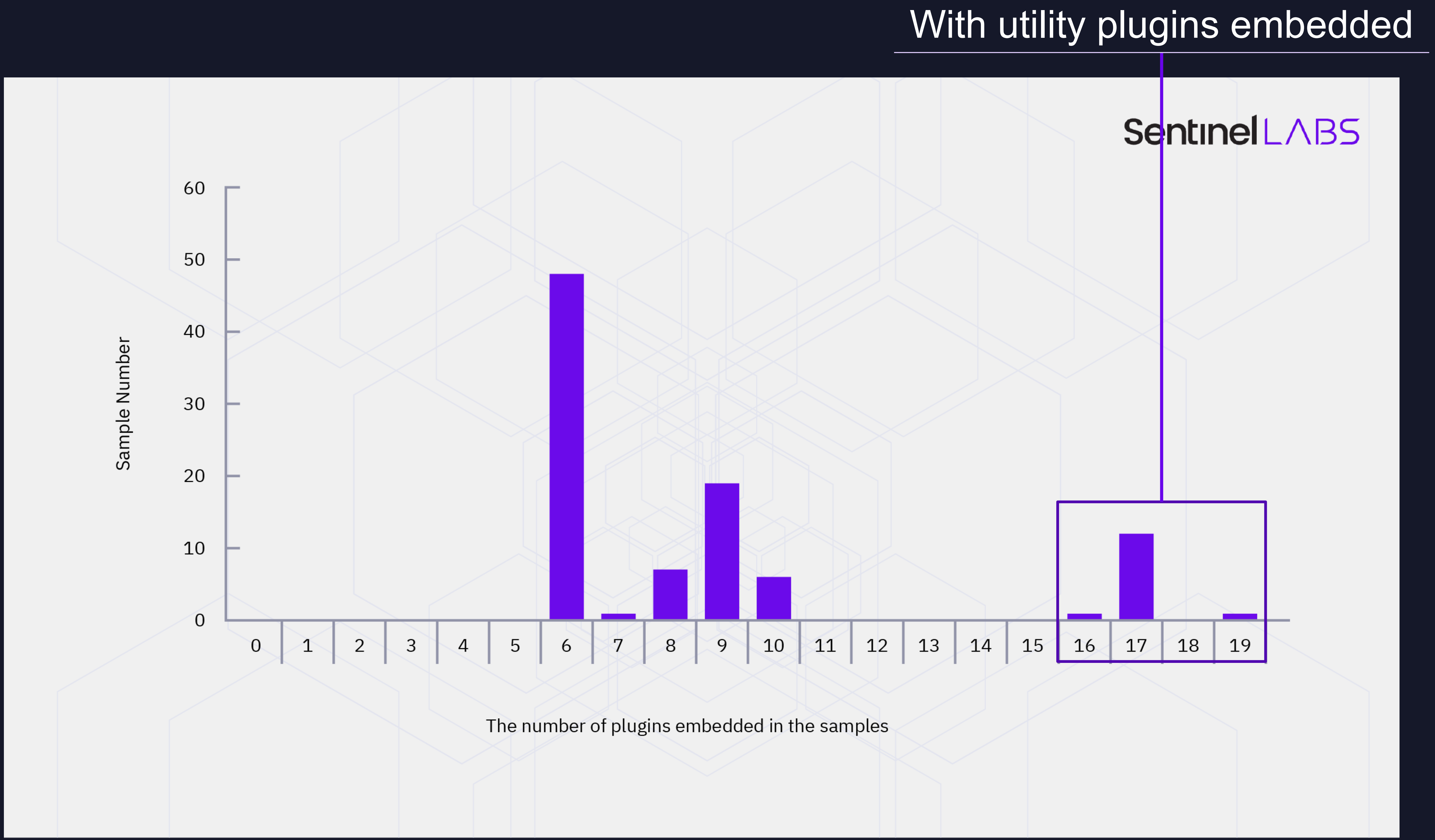


Selling the plugins separately

A special version: packed by VMProtect, different plugin IDs



Selling the plugins separately

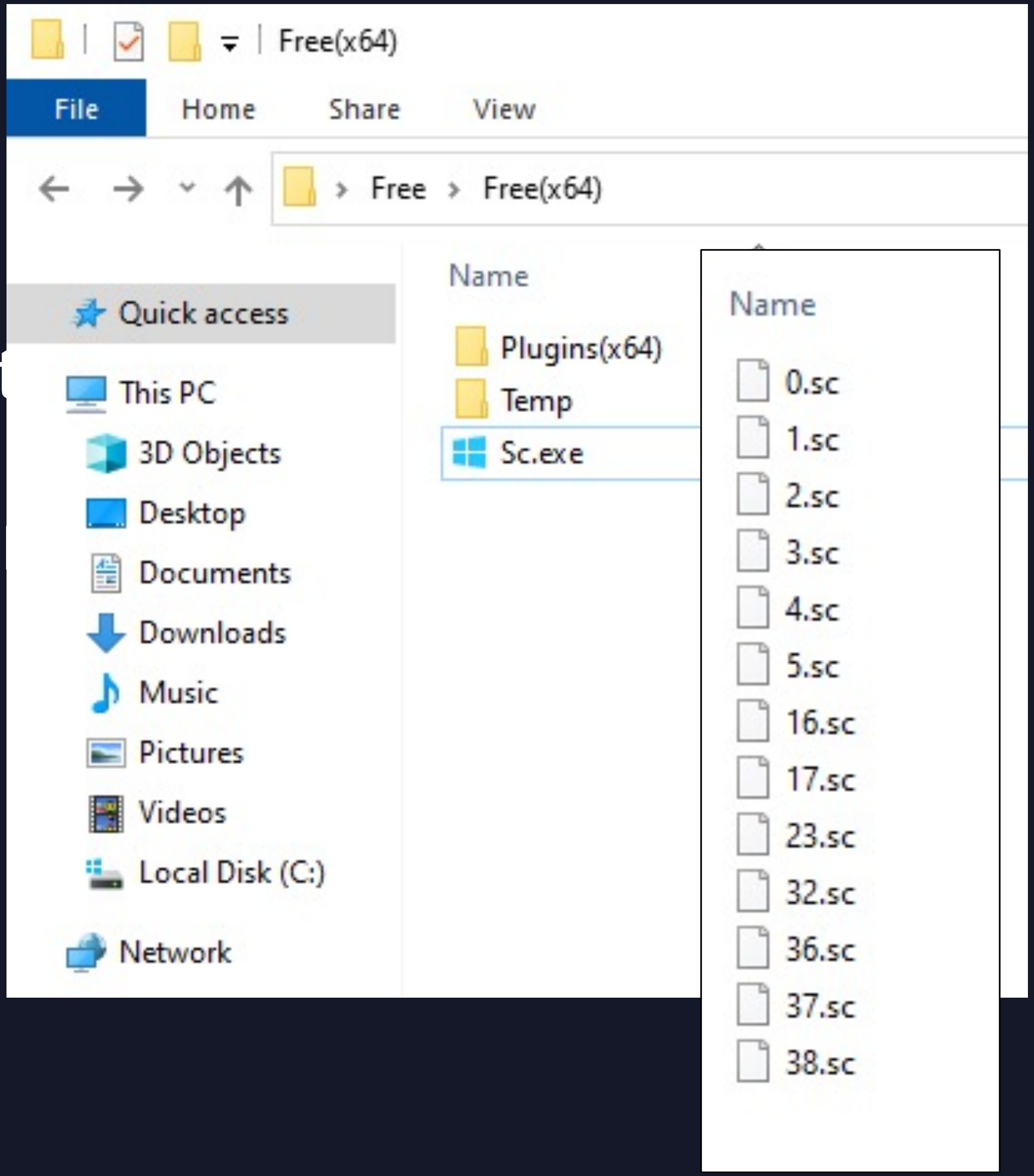


Selling the plugins separately (cont.)

- Most of the samples do not have utility plugins embedded in them.
  - Need to upload other plugins remotely through the controllers.
  - The plugins are placed in the directory:
    easy to be removed from a package

- Tick – an active user of ShadowPad – developed a tool wi
  plugin “Software” in an overlapped timeframe.
  - Tick did not have access to that plugin while it was already avai

- The plugins should be provided separately.
  - Not given in a full bundle.



Plugins(x64)
Temp
Sc.exe

Name
0.sc
1.sc
2.sc
3.sc
4.sc
5.sc
16.sc
17.sc
23.sc
32.sc
36.sc
37.sc
38.sc

The business model of ShadowPad

- ShadowPad is a sold malware.
- The plugins need to be acquired separately.
- It is only sold to a limited set of users.

- Why is ShadowPad a good choice for the attackers:
  - The cost to develop a stable backdoor/RAT is high.
  - The plugins (functionalities) are complete, and the attackers can choose which they want.
    - ShadowPad was the primary backdoor for long-term espionage in several campaigns.
  - The use of a shared backdoor reduces the chance to be attributed.

SentinelOne®

Which threat actors are using ShadowPad?

Which threat actors are using ShadowPad?

WINNTI/APT41

Operation Redbonus

Fishmonger

Tick and Tonto Team

Operation Redkanku

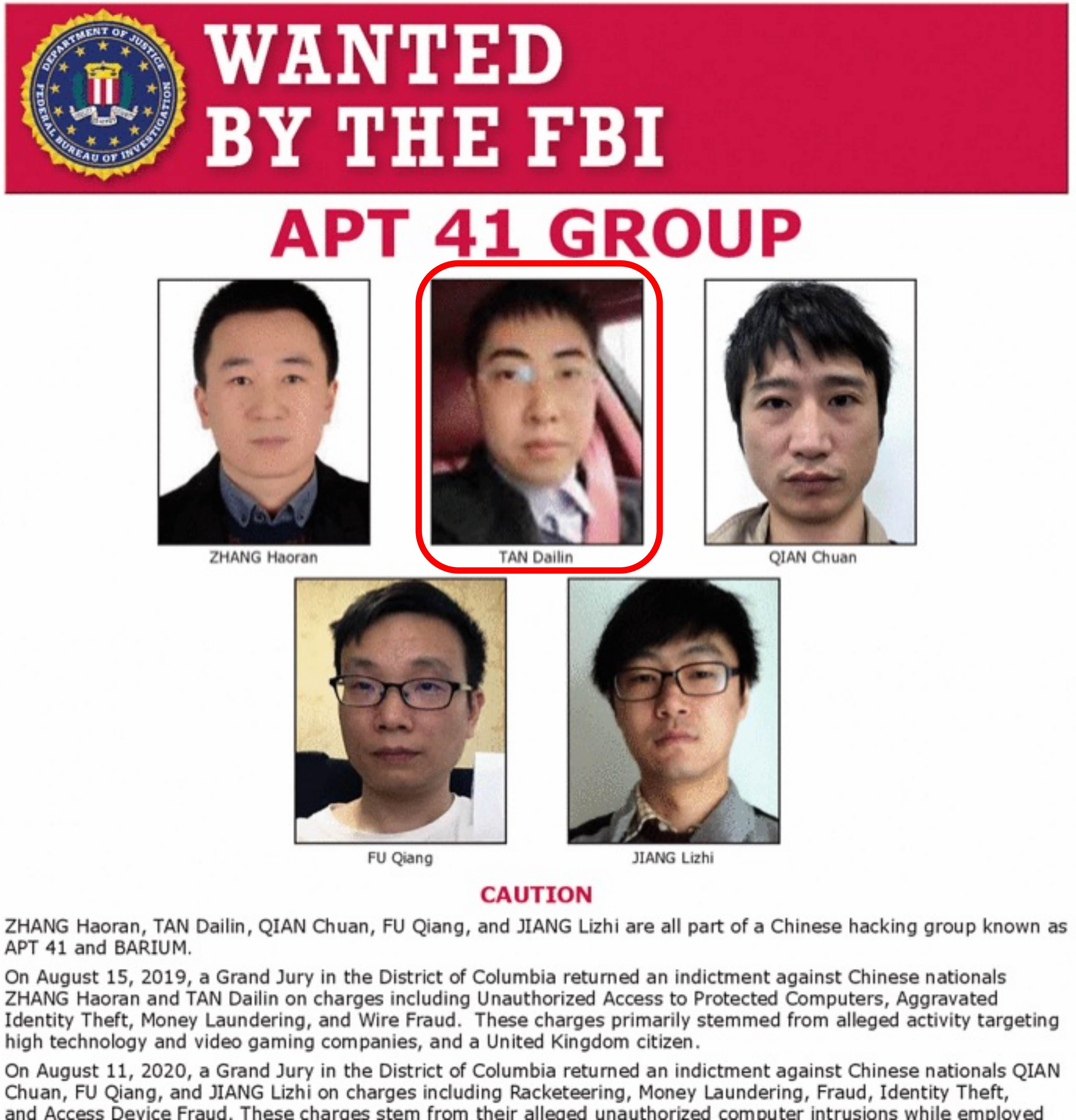
Tropic Trooper

LuckyMouse

WINNTI/APT41

Two sub-groups of WINNTI/APT41

- BARIUM (Tan Dailin aka Rose and Zhang Haoran)
  - Against the gaming industry and several supply chain attacks, e.g., NetSarang, ASUS, and allegedly, CCleaner
- LEAD (Chengdu 404 Network Technology Co., Ltd)
  - Attack for financial and espionage purposes



WANTED BY THE FBI

APT 41 GROUP

ZHANG Haoran

TAN Dailin

QIAN Chuan

FU Qiang

JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

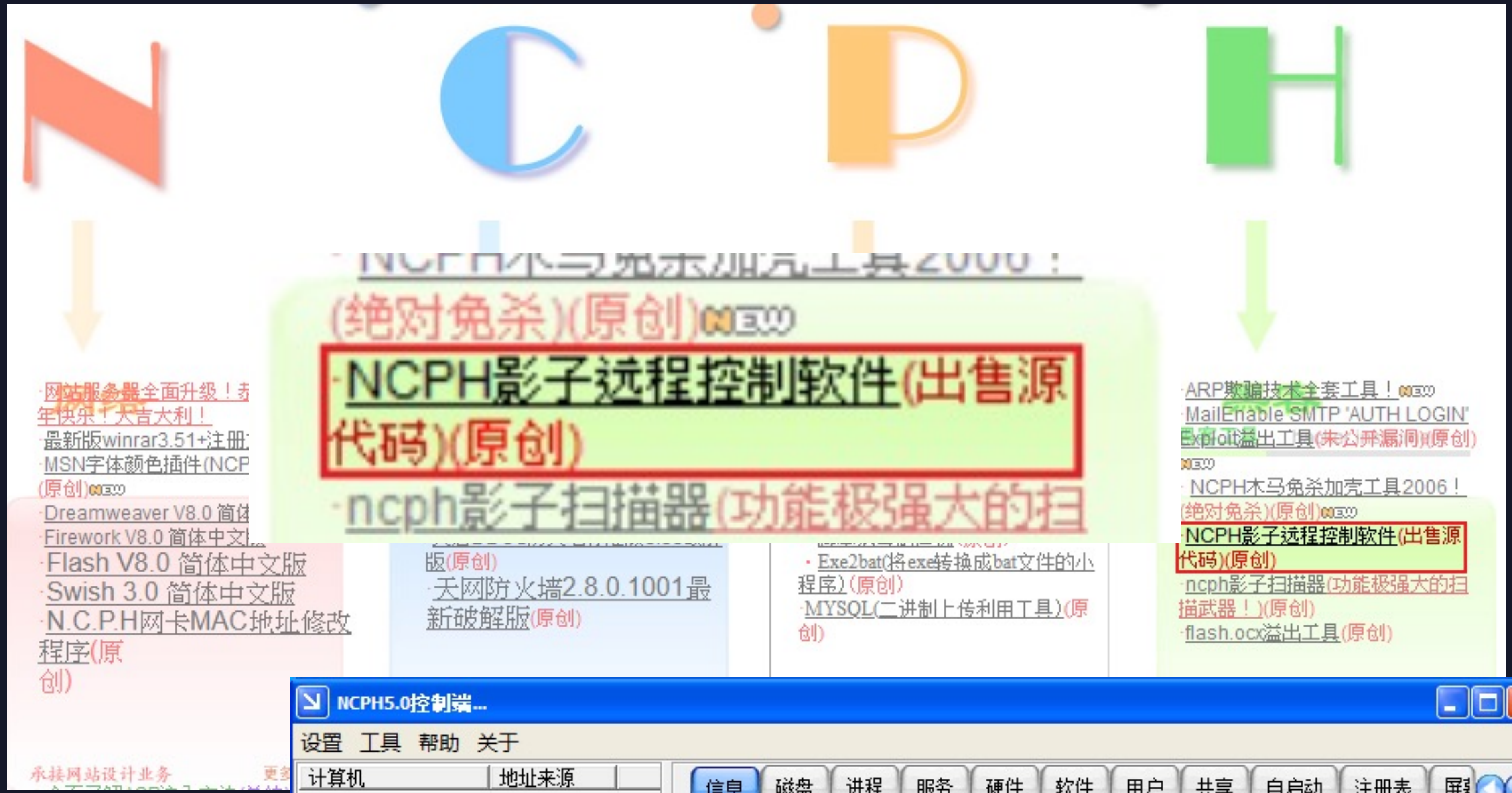
On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed

What is NCPH

A hacking group that developed lots of tools and freely shared on NCPH websites

- They also declared that the source code was on sale
- Rose and whg have collaboration on malware development since 2006

Rose likely had high privilege access – or was a co-developer – to ShadowPad



NCPH木马免杀加壳工具2006！(绝对免杀)(原创)NEW

NCPH影子远程控制软件(出售源代码)(原创)

ncph影子扫描器(功能极强大的扫

网站服务器全面升级！⋯年快乐！大吉大利！

最新版winrar3.51+注册⋯

MSN字体颜色插件(NCP⋯(原创)NEW

Dreamweaver V8.0 简体⋯

Firework V8.0 简体中文⋯

Flash V8.0 简体中文版

Swish 3.0 简体中文版

N.C.P.H网卡MAC地址修改程序(原创)

版(原创)

天网防火墙2.8.0.1001最新破解版(原创)

Exe2bat(将exe转换成bat文件的小程序)(原创)

MYSQL(二进制上传利用工具)(原创)

ARP欺骗技术全套工具！NEW

MailEnable SMTP 'AUTH LOGIN' Exploit溢出工具(未公开漏洞)(原创) NEW

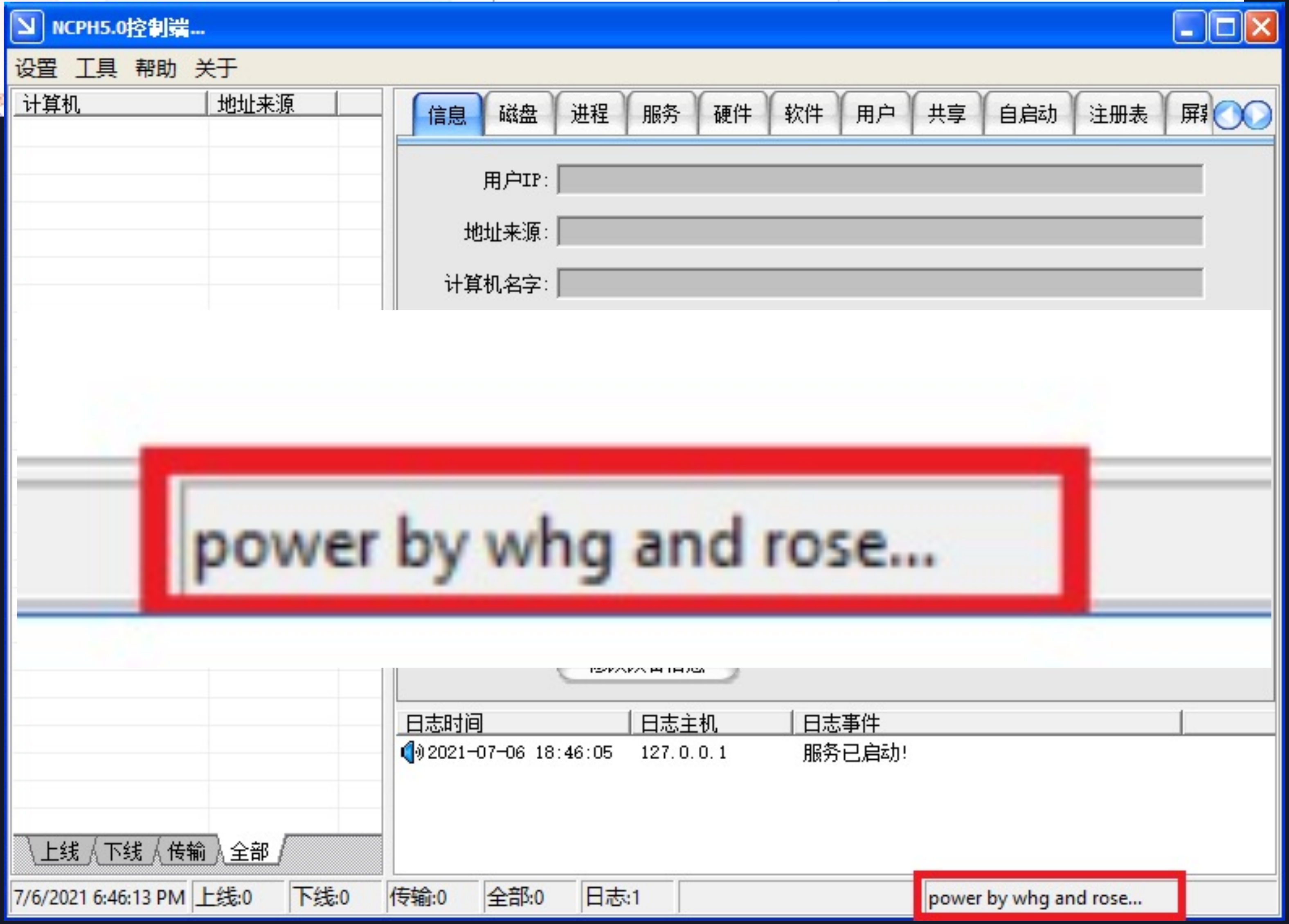
NCPH木马免杀加壳工具2006！(绝对免杀)(原创)NEW

NCPH影子远程控制软件(出售源代码)(原创)

ncph影子扫描器(功能极强大的扫描武器！)(原创)

flash.ocx溢出工具(原创)

承接网站设计业务



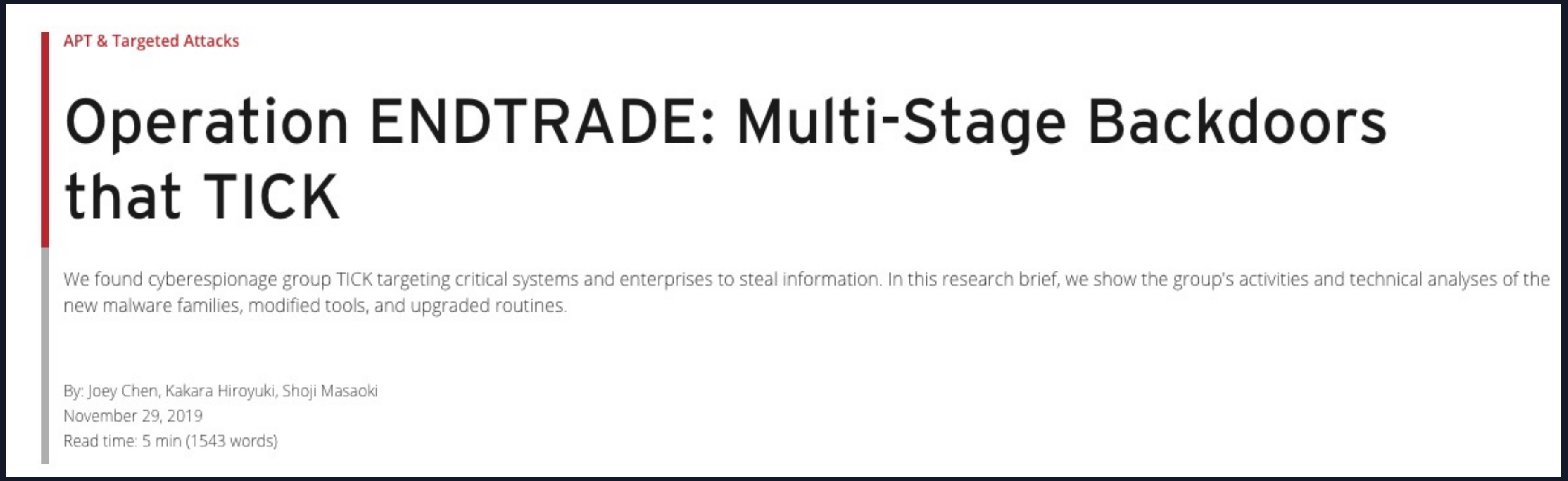
power by whg and rose...

```
2021-07-06 18:46:05   127.0.0.1   服务已启动!
```

7/6/2021 6:46:13 PM 上线:0 下线:0 传输:0 全部:0 日志:1 power by whg and rose...

Tick and Tonto Team

- Two groups amalgamated into a new institution during the reorganization of PLA
- Started to use ShadowPad as their primary backdoor for conducting intrusion
- TICK
  - Sent spear phishing emails to deliver ShadowPad
- Tonto Team
  - Exploited CVE-2019-9489 and CVE-2020-8468 in Trend Micro's security solutions to deliver ShadowPad

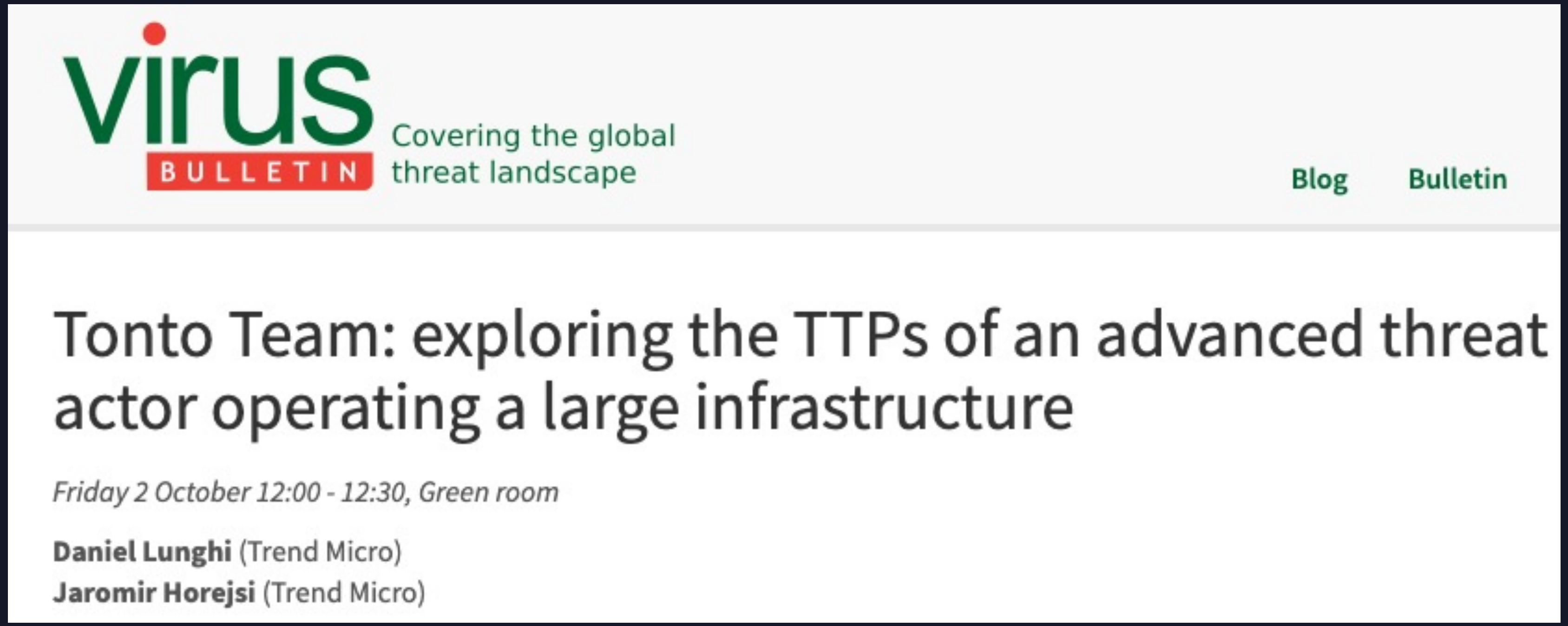


APT & Targeted Attacks

Operation ENDTRADE: Multi-Stage Backdoors that TICK

We found cyberespionage group TICK targeting critical systems and enterprises to steal information. In this research brief, we show the group's activities and technical analyses of the new malware families, modified tools, and upgraded routines.

By: Joey Chen, Kakara Hiroyuki, Shoji Masaoki
November 29, 2019
Read time: 5 min (1543 words)



virus BULLETIN Covering the global threat landscape

Blog Bulletin

Tonto Team: exploring the TTPs of an advanced threat actor operating a large infrastructure

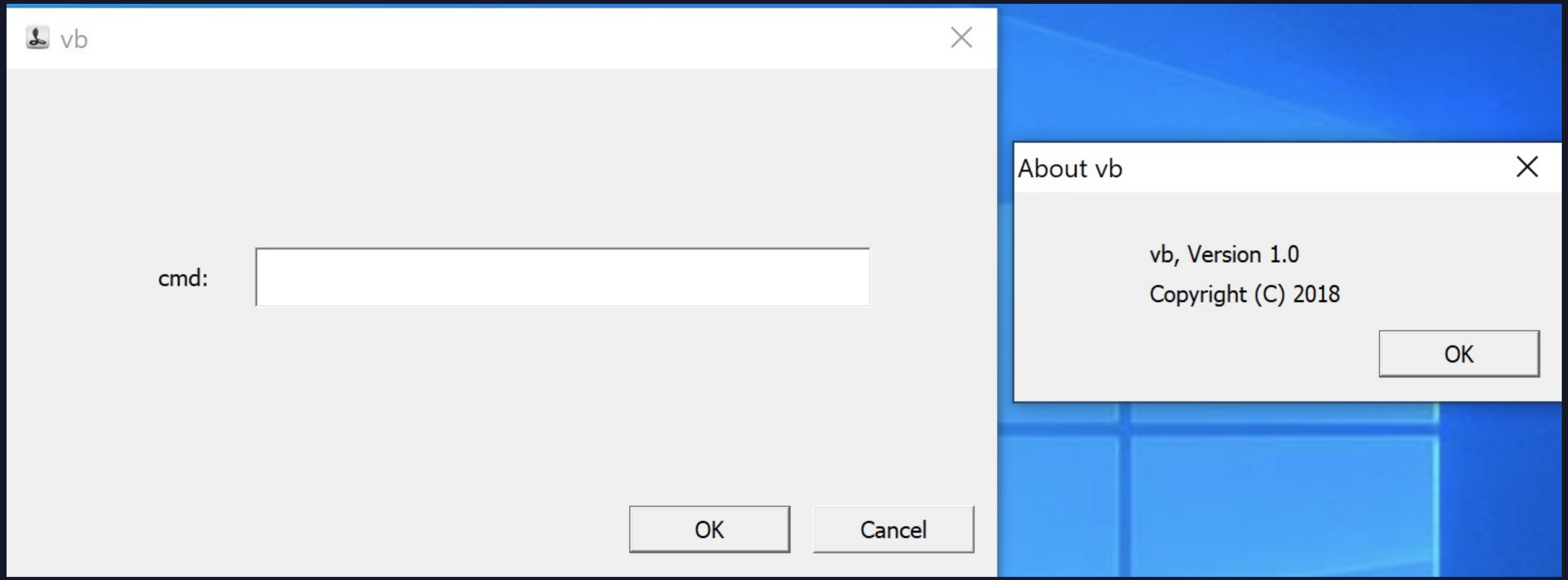
Friday 2 October 12:00 - 12:30, Green room

Daniel Lunghi (Trend Micro)
Jaromir Horejsi (Trend Micro)

Customized tools for intrusion

Customized tools

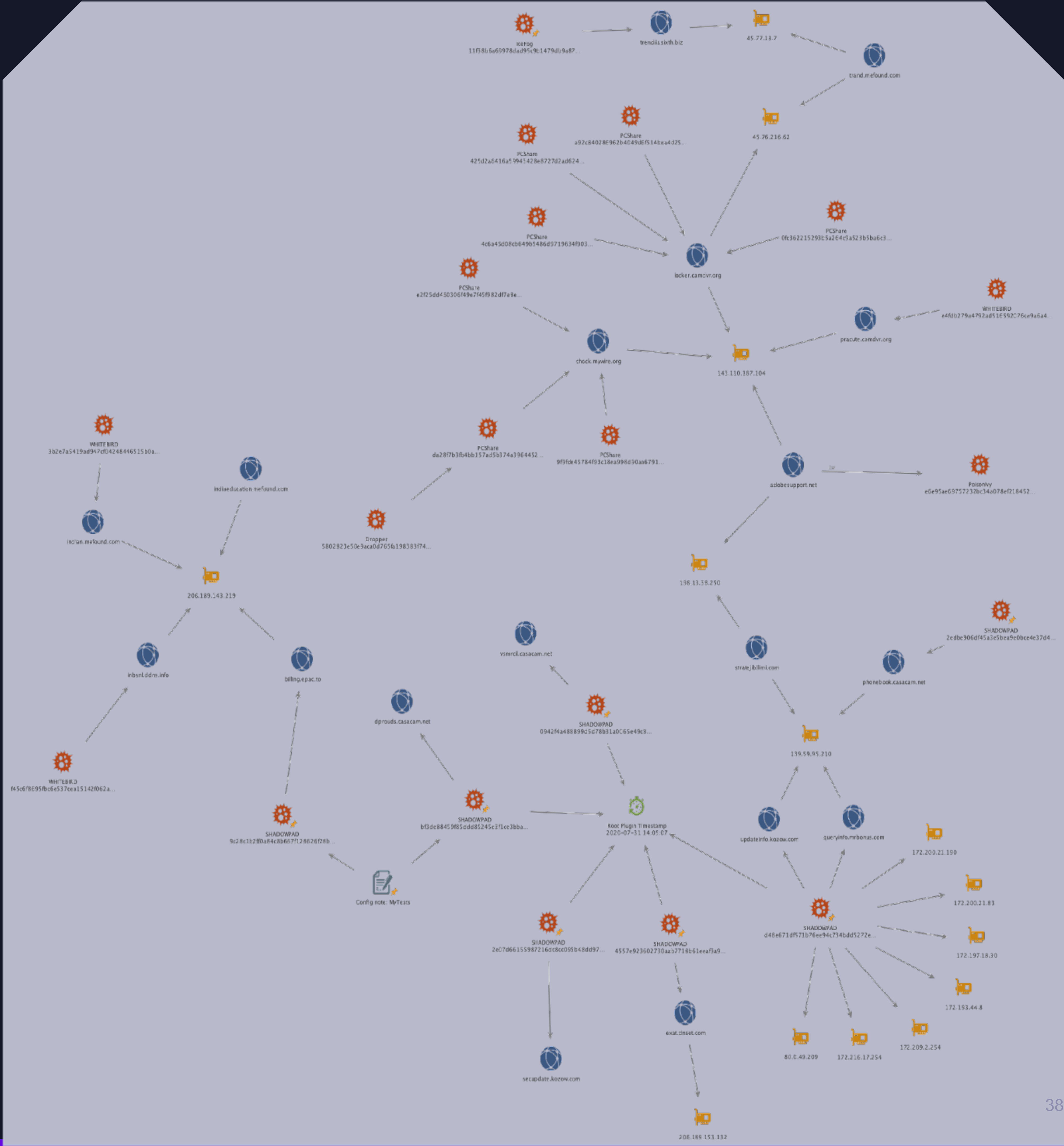
- Modified mimikatz
- Screen capture tool
- Packet transmission tool
- Tool to list the software installed on a computer
  - ShadowPad has a plugin with the same functionality
- VBScript command executor tool
  - Generate a payload of VBScript
  - Bypass TrendMicro products



vb, Version 1.0
Copyright (C) 2018

Operation Redbonus

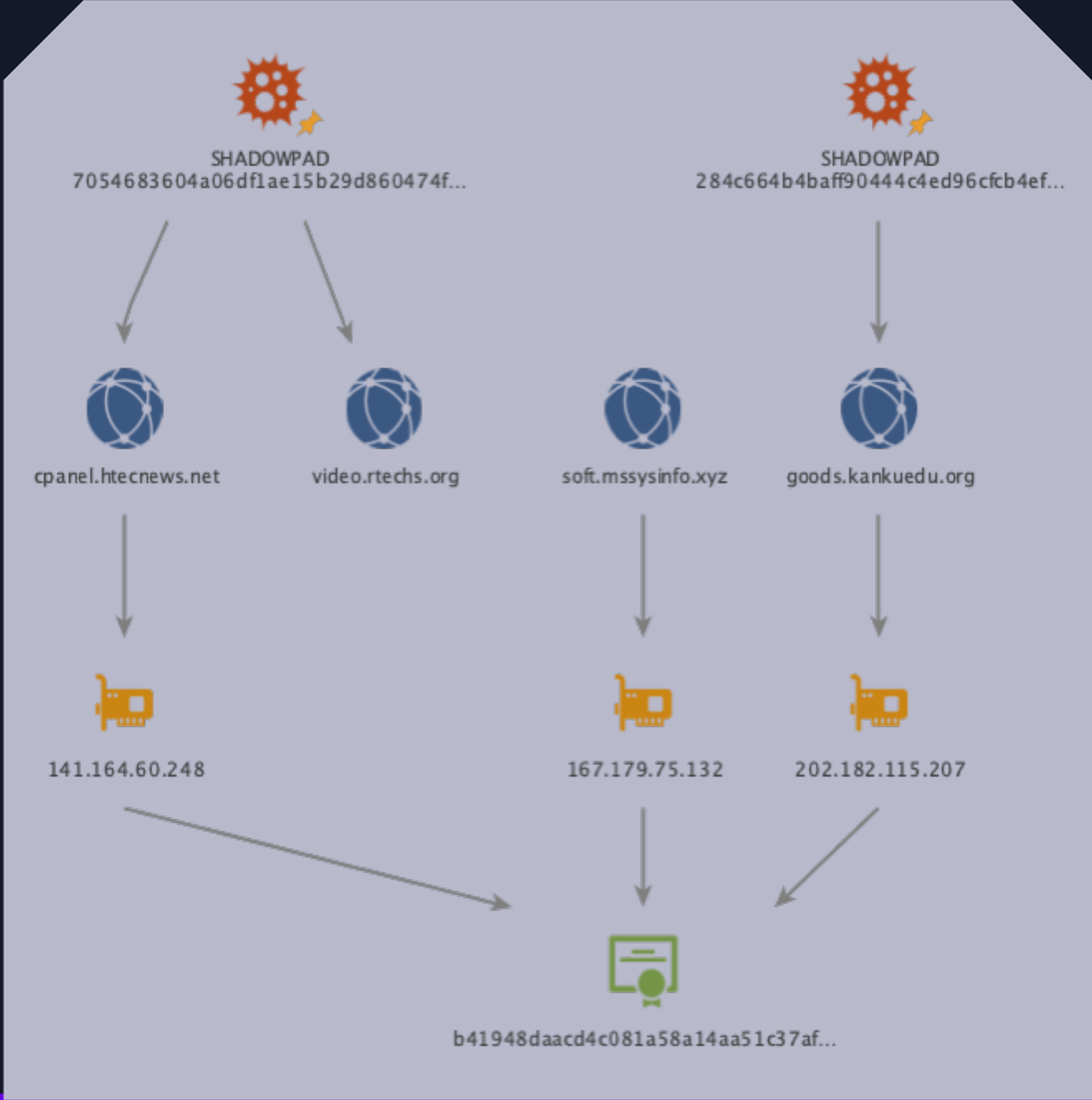
- Against Indian country
- Other backdoors in use, such as Whitebird, IceFog and a customized instance of PCShare


IceFog 11f38b6a69978dad95c9b1479db9a87...
trendiis.sixth.biz
45.77.13.7
trand.mefound.com
PCShare a92c840286962b4049d6f514bea4d25...
45.76.216.62
PCShare 425d2a6416a59943428e8727d2ad624...
PCShare 4c6a45d08cb649b5486d9719634f903...
PCShare 0fc362215293b5a264c9a523b5ba6c3...
locker.camdvr.org
PCShare e2f25dd460306f49e7f45f982df7e8e...
WHITEBIRD e4fdb279a4792ad516592076ce9a6a4...
pracute.camdvr.org
chock.mywire.org
143.110.187.104
WHITEBIRD 3b2e7a5419ad947cf04248446515b0a...
PCShare da28f7b3fb4bb157ad5b374a3964452...
PCShare 9f9fde45784f93c18ea998d90aa6791...
indiaeducation.mefound.com
adobesupport.net
Poisonlvy e6e95ae69757232bc34a078ef218452...
indian.mefound.com
Dropper 5802823e50e9aca0d765fa198383f74...
206.189.143.219
198.13.38.250
SHADOWPAD 2edbe906df45a3e5bea9e0bce4e37d4...
inbsnl.ddns.info
billing.epac.to
vsmrcl.casacam.net
stratejibilimi.com
phonebook.casacam.net
dprouds.casacam.net
SHADOWPAD 0942f4a488899d5d78b31a0065e49c8...
139.59.95.210
WHITEBIRD f45c6f8695fbc6e537cea15142f062a...
SHADOWPAD 9c28c1b2ff0a84c8b667f128626f28b...
SHADOWPAD bf3de88459f85ddd85245e3f1ce3bba...
Root Plugin Timestamp 2020-07-31 14:05:07
updateinfo.kozow.com
queryinfo.mrbonus.com
172.200.21.190
172.200.21.83
Config note: MyTests
SHADOWPAD d48e671df571b76ee94c734bdd5272e...
172.197.18.30
SHADOWPAD 2e07d66155987216dc8cc095b48dd97...
SHADOWPAD 4557e923602730aab7718b61eeaf3a9...
172.193.44.8
exat.dnset.com
80.0.49.209
172.216.17.254
172.209.2.254
secupdate.kozow.com
206.189.153.132

SentinelOne

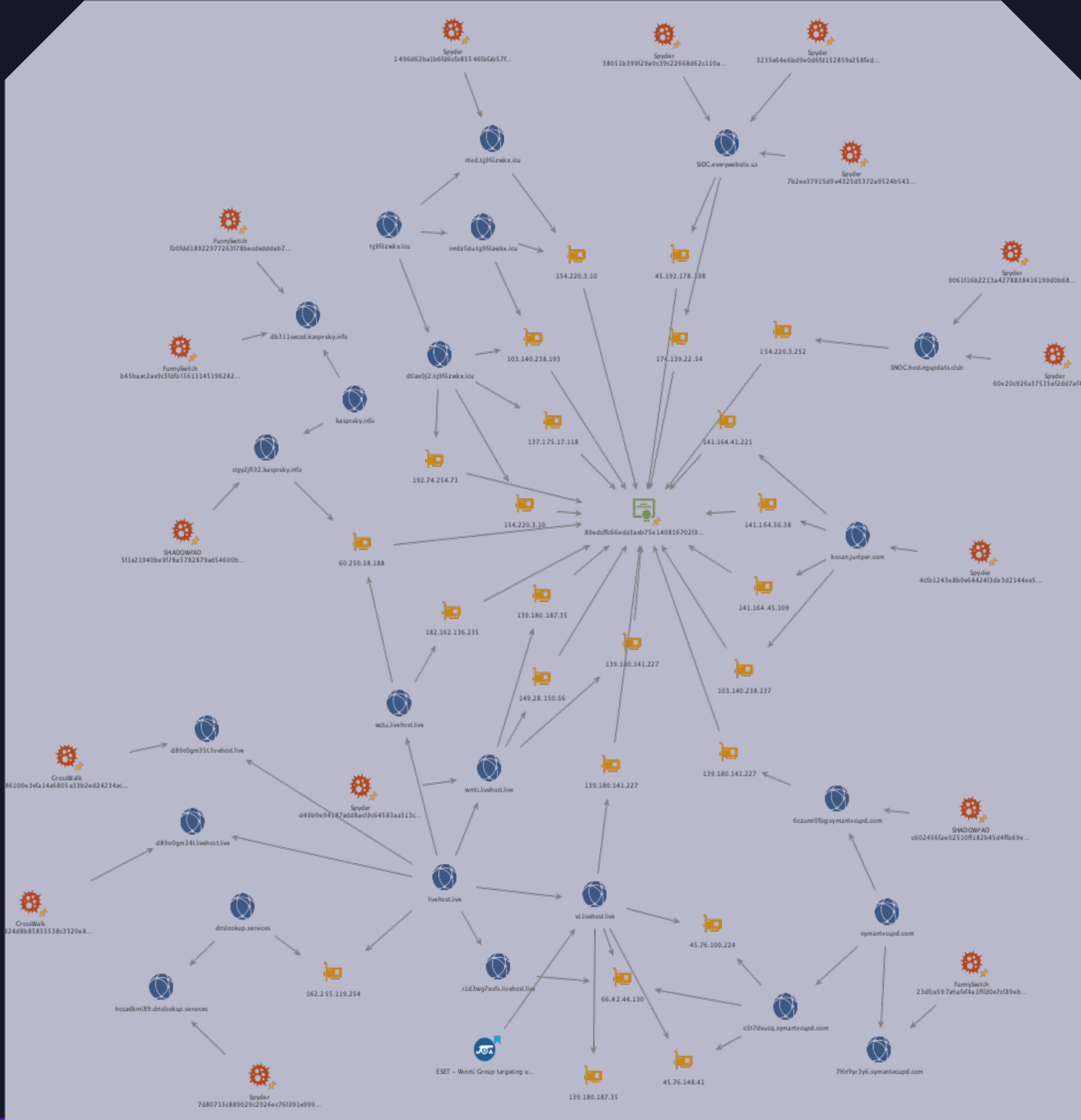
Operation Redkanku

- All of the C&C servers had a self-signed certificate
- Some related samples were documented to be a part of t he ProxyLogon attacks



Fishmonger

- New version of ShadowPad which had updates and more advanced obfuscation techniques
- They are interested in COVID-19 research in Hong Kong, Taiwan, India and the US.
- ShadowPad and Spyder as their primary backdoors for long-term monitoring
- A self-signed certificate is installed on several C&C servers of ShadowPad and Spyder



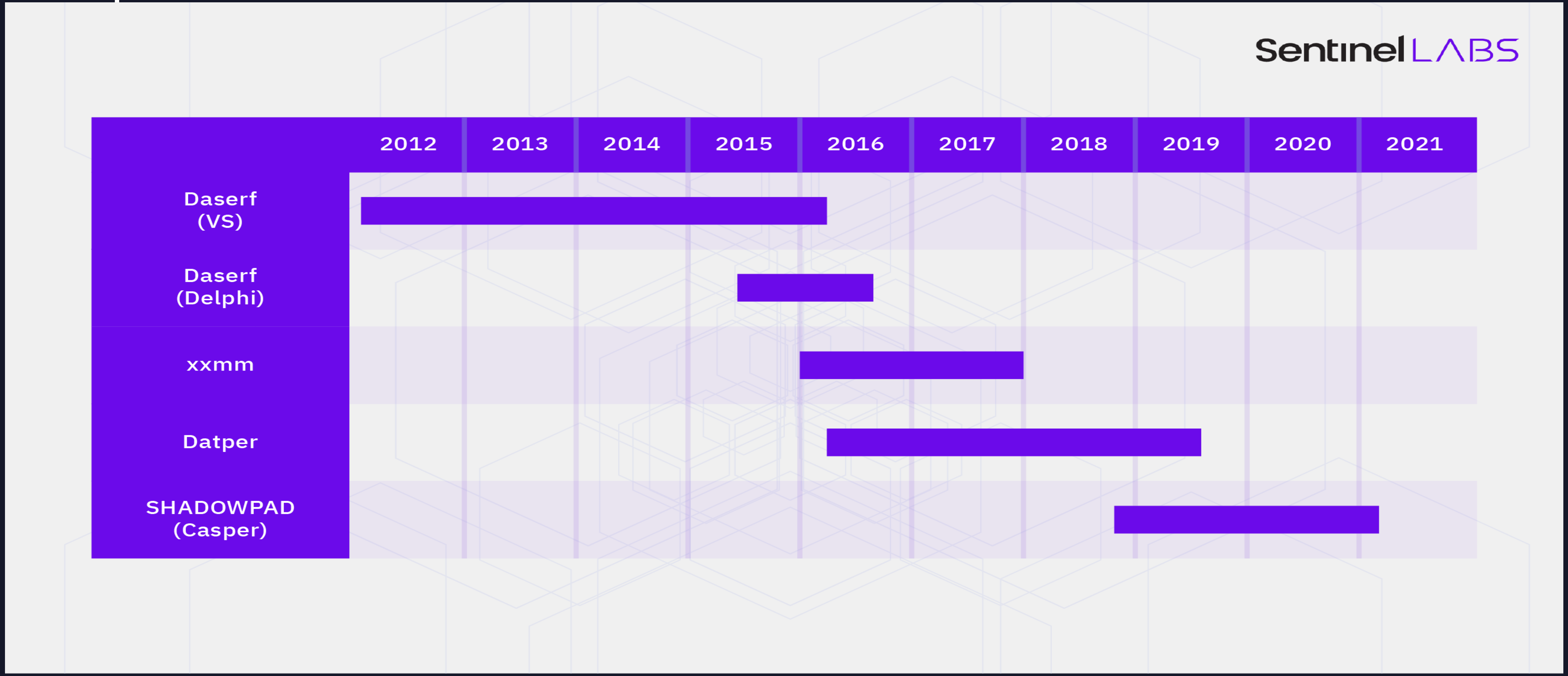
SentinelOne

SentinelOne

Landscape shift

From developing backdoors to acquiring backdoors

- Past
  - Chinese threat actors develop their own tool sets based on their needs during operations
- Now
  - The popularity of malware such as ShadowPad and CobaltStrike among Chinese espionage groups
  - Here is an example about Tick's timeline of backdoor



The benfit of acquiring backdoors

- Lower the cost
  - Reduces the cost of a well-designed piece of malware
  - Reduces the human resource to develop the malware in-house
- Keeps enhancing the stability and usability
  - The service provider will provide newest version of the backdoor with new features added
  - Unlike much of the commodity malware found in cybercriminal circles or underground forums

SentinelOne®

Mitigation advice

Mitigation advice for ShadowPad

- Audit the services and the registries to find any suspicious items
- Monitor dynamic behaviors of “spawning a new process” and “process injection”
- Apply memory forensics periodically to identify malware which resides in-memory
- Adopt an Endpoint Detection and Response (EDR) solution across your organization
- A well consolidated monitoring capability provides visibility into cyber threats

SentinelOne®

Conclusion

Conclusion

- Why do the actors choose to use ShadowPad?
  - Experienced developers to develop something much better with active updates
  - Reducing the cost of operation and development
  - Harder for security company to do further research
- Why ShadowPad is not disappearing?
  - Still under updates with more advanced obfuscation and persistence techniques
  - A powerful backdoor with more functionalities so good for long-term espionage operations and keep stealthy under the radar
- How ShadowPad affect threat intelligence?
  - Need to develop more systematic ways for attribution

Thank You

SentinelOne®

sentinelone.com