

BLUEHAT

IL 2022

Focusing on the Fjords



Stav Shulman and
Yuri Rozhansky



MANDIANT[®]



Focusing on the Fjords



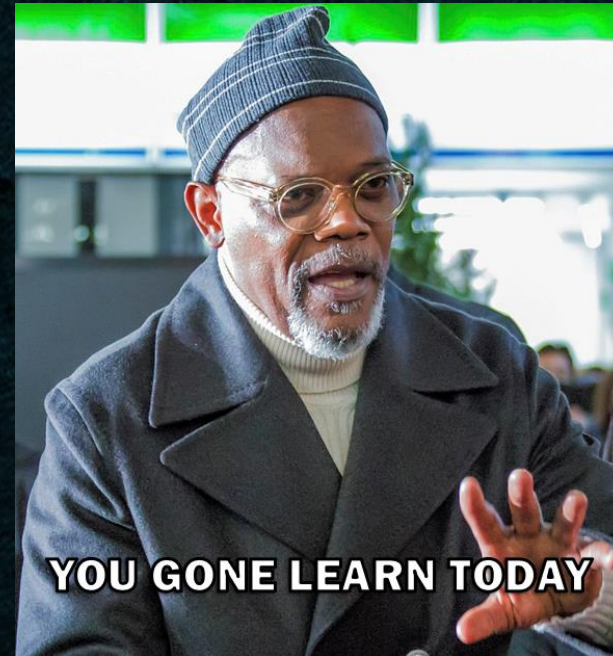
Stav Shulman and
Yuri Rozhansky



MANDIANT[®]

Agenda

- UNC215 makes Aliyah
- Patchwork
- Following the m&m model
- Compile, panic, evolve repeat
- Conclusions



UNC215 Makes Aliyah

WELCOME TO

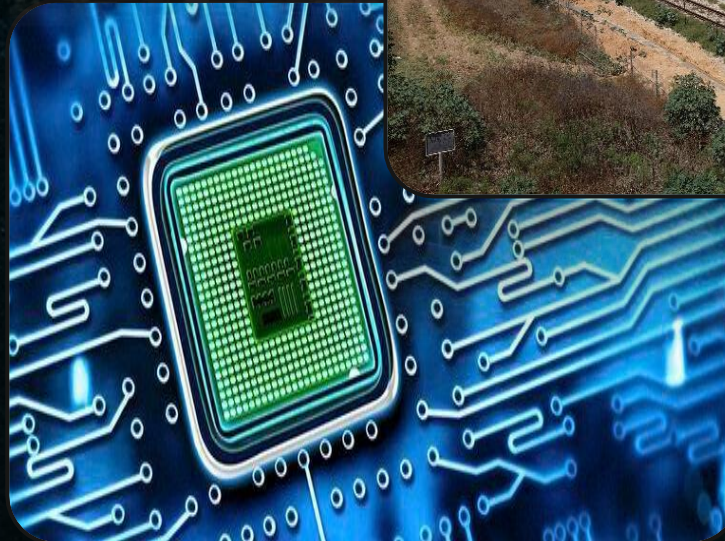
ISRAEL

Chinese Cyber Space



- Global targeting
- Dozens of threat actors
- Engaged in espionage, cyber crime and information operations
- Derived by territorial integrity and expanding global influence

Chinese Interests in Israel



Who is **UNC215**?

- Operating since 2014
- Low confidence relation to APT27
- Global targeting
- Middle Eastern focus
- Interests in Government, Health, Technology, Communication, Finance, Defence

UNC215 Toolkit

- One-Day vulnerabilities
- CHINACHOPPER webshells
- Distinct loading chain
- Customized shellcode packer
- FOCUSFJORD and HYPERBRO backdoors





Patchwork

Raining with a 100% chance of OneDays

➤ We all idolize and focus on ZeroDays

➤ We neglect “old” vulnerabilities

“one might think that more recent vulnerabilities would be more common However, as we saw last year, it is actually the **older vulnerabilities that are leading the way.**”

- Verizon 2021-data-breach-investigations-report

“State sponsored actors continue to exploit a collection of older vulnerabilities — in some cases, more than **5 years old**”

- CISA, 2019

Raining with a 100% chance of OneDays

FIGURE 3. Did any of these breaches occur because a patch was available for a known vulnerability but not applied?

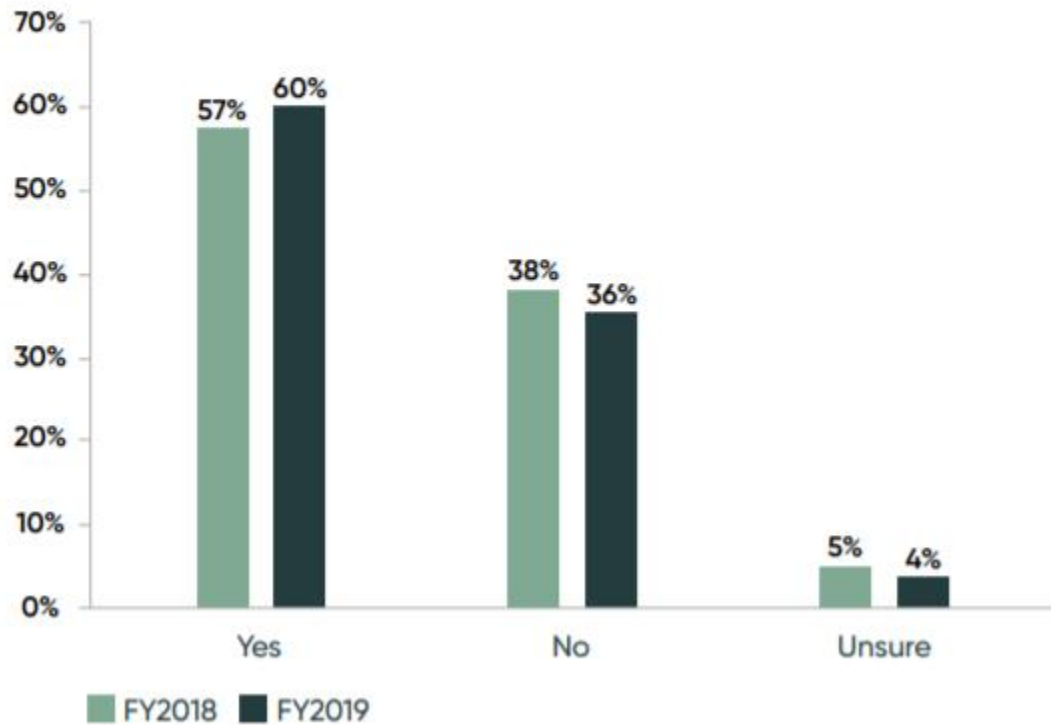
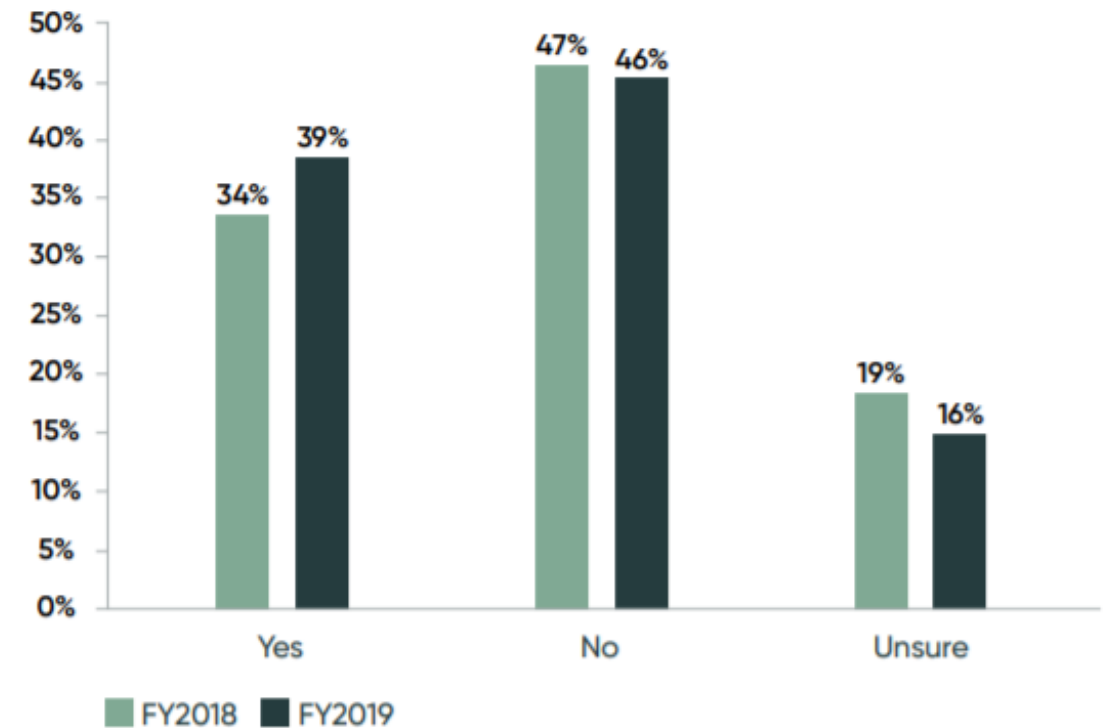
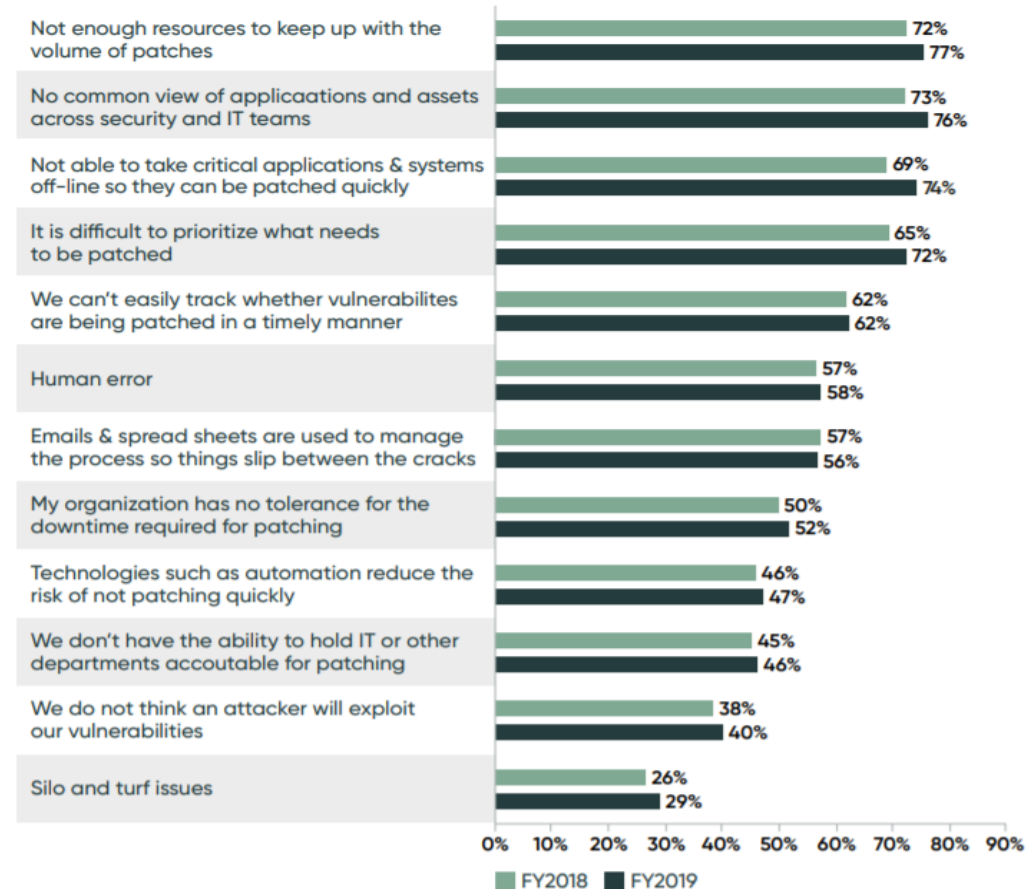


FIGURE 4. Was your organization aware it was vulnerable prior to the data breach?

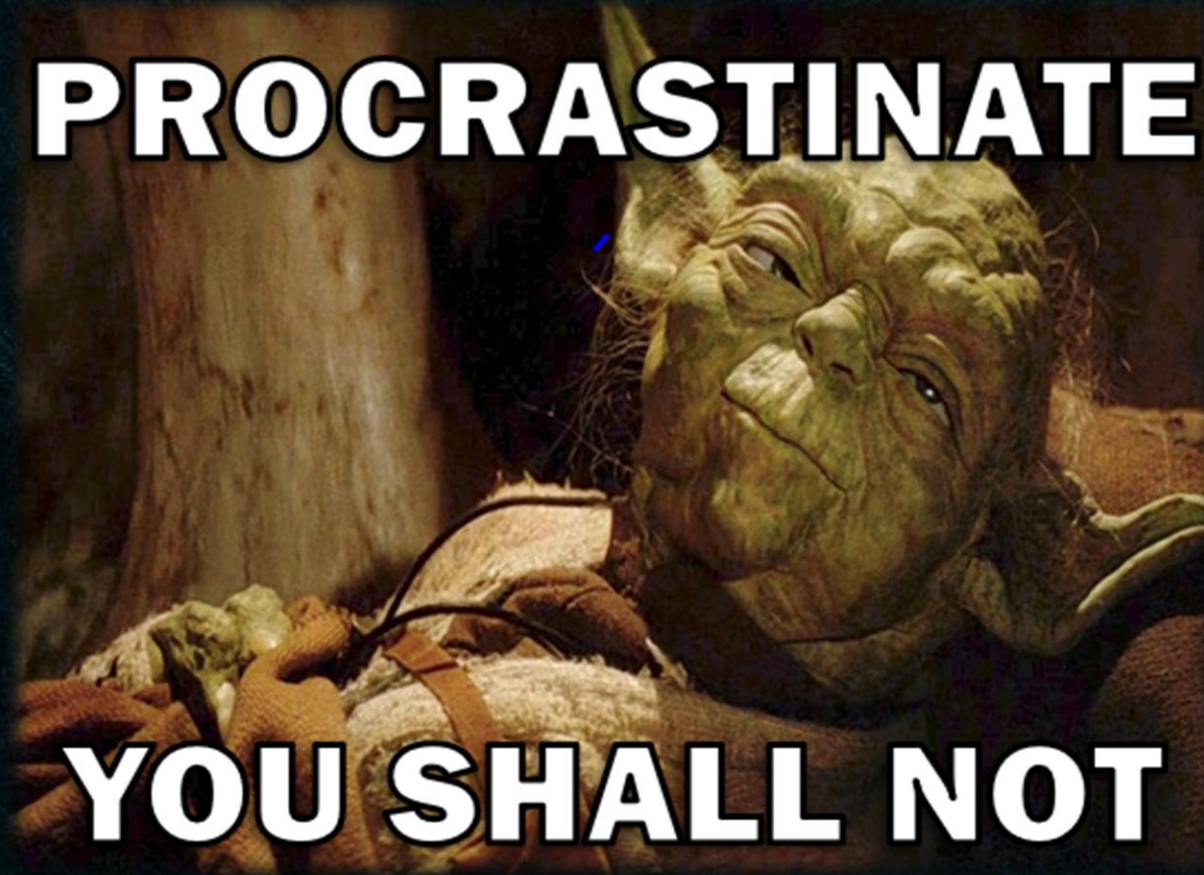


Raining with a 100% chance of OneDays

FIGURE 15. Why major delays occur in vulnerability patching. More than one response permitted



Raining with a 100% chance of OneDays



POC For Procrastination

- CVE-2019-0604
- Disclosed in the beginning of 2019
- Vulnerability for Microsoft share point servers
- Allows execution of malicious serialized XML's
- UNC215 usage
 - Starts March 2019, peaks 2020



POC For Procrastination

GET /_layouts/Picker.aspx
MultiSelect=False&CustomProperty=User%3B%3B15%3B%
3B%3BFalse&DialogTitle=Select%20People&DialogImage=
%2F%5Flayouts%2Fimages%2Fpeople%2Egif&PickerDialogType=Microsoft%2ESharePoint%2EWebControls%2EPeoplePickerDialog%2C%20Microsoft%2ESharePoint%2C%20Version%3D14%2E0%2E0%2E0%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D71e9bce111e9429c&ForceClaims=False&DisableClaims=False&EnabledClaimProviders=&EntitySeparator=%3B%EF%BC%9B%EF%B9%94%EF%B8%94%E2%8D%AE%E2%81%8F%E1%8D%A4%D8%9B&DefaultSearch= 80 MCAP\M34815





Following the m&m Model



Nibbling Inside the Crust

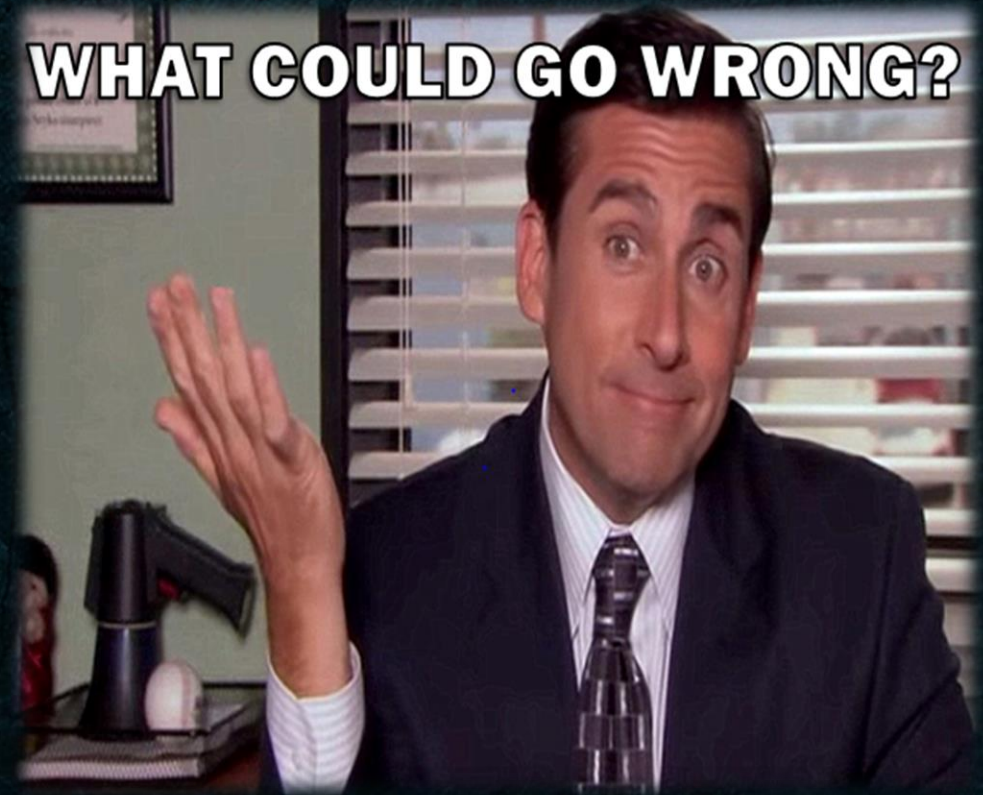
- Networks have a fragile outer shell
- Internal assets are often left behind
- Monitoring usually applied to main exists and entries only
- Misconception that nothing can barge in

FOCUSFJORD 101

- First stage downloader
- Delivered via **UNC215's** unique loading chain
- Never physically written to the disk
- Safe and stable solution to maintain access to infected EP

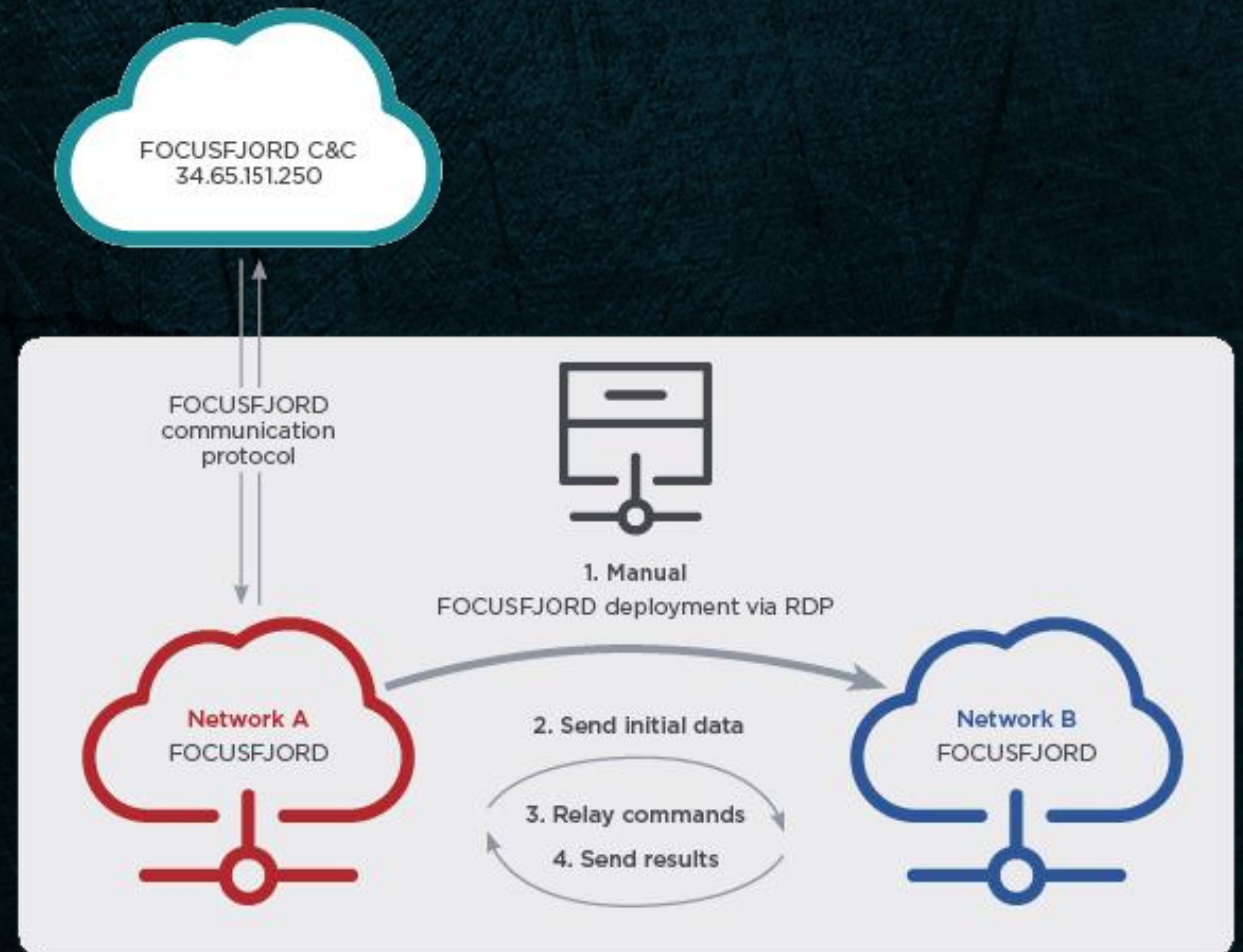
FOCUSFJORD 101

- Loading chain binaries might quarantine
- Connection between infected EP and C&C might be blocked



Minimized Outbound Footprint

- Custom binary protocol
- Internal C&C hierarchy
- 1-2 exit nodes per victim



Minimized Outbound Footprint



Network B
Internally Configured FOCUSFJORD

Win [REDACTED]
[REDACTED].gov.il
SYSTEM
(10.x.x.132)10.x.x.132

1
[REDACTED]
\iceland
619DE05BE7509A0551ED6C2CEDA0451B
[REDACTED]:164:32251
auto:34.65.151.250:443

C:\windows\EPSP18131235931481\
EPSP18131235931481\5ck\wc6ix
EPSP18131235931481\rtqx7ucxcn
C:\windows\EPSP18131235931481\EPSP18131235931481.exe
C:\windows\EPSP18131235931481\SETUPENGINE.dll
C:\windows\EPSP18131235931481\config.data

Victim Server OS
Victim Server Name

Victim Internal IP Address

Registry key 12, manually set by actor
Registry key 13
Unique identifier for each victim
Public IP Address of Network A
External C&C Address



Command results



Network A
Externally Configured FOCUSFJORD

tcp:34.65.151.250:80(PID:3448)
s3-1

External C&C Address
Communication Identifier

Compile, Panic, Evolve, Repeat

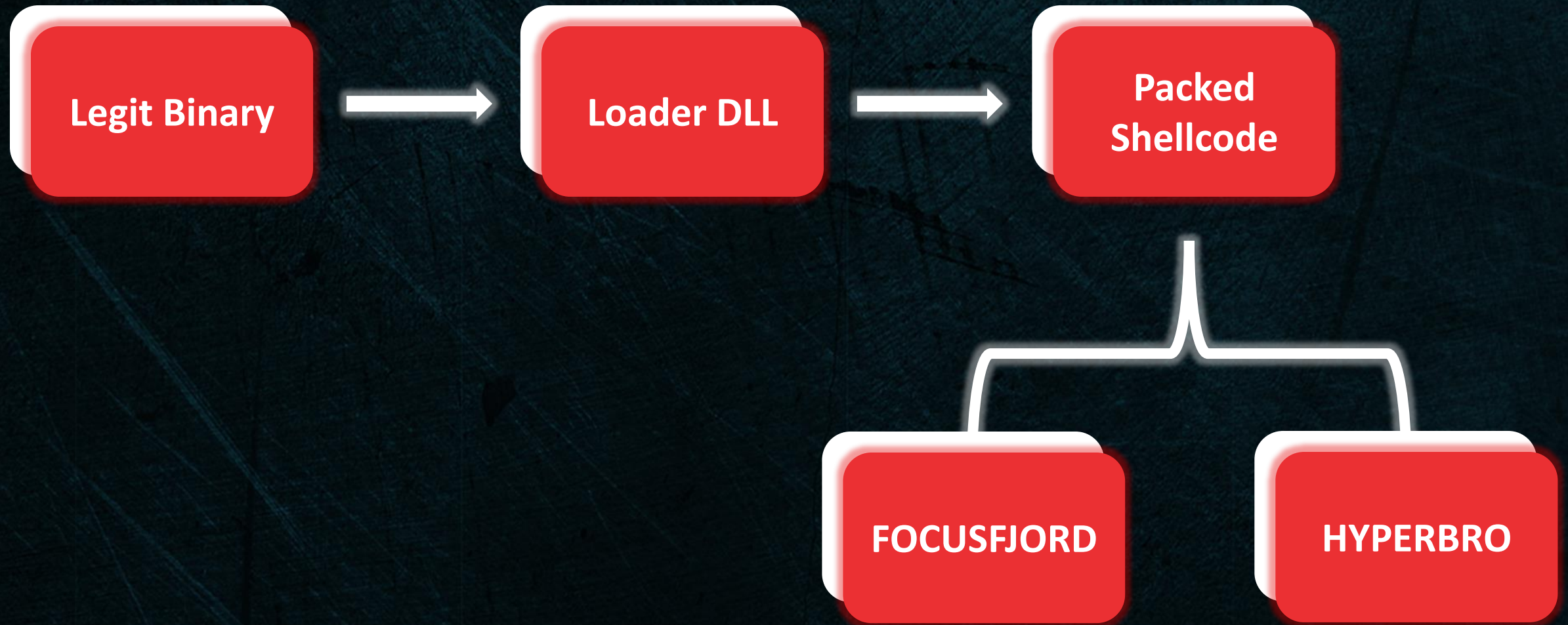
```
while (alive) {  
    eat();  
    sleep();  
    code();  
    repeat();  
}
```



Modus Operandi

- **UNC215** appreciates comfort and have trustworthy malwares
- Very capable of operating under pressure and offer quick fixes
- In special occasions would demonstrate exceptional development skills

The Comfort of The Chain



“Signature” Configuration Mechanism

- Cleartext configuration block
- Stored under dedicated registry entry upon first execution
- For FOCUSJORD would also encrypt before storing

```
Size          dd 93h          ; DATA :
a1395981253443 db '139.59.81.253:443;',0
               ; DATA :

a11_0         db '1:1',0
aCfgwizExe    db 'cfgwiz.exe',0
aFpmmcDll     db 'FPMMC.DLL',0
aGvg36a467c6hke db 'GvG36a467C6Hkea',0
aCfgwiz       db 'cfgwiz',0
aSvchostExe  db 'svchost.exe',0
aCfgwizbe7bk281 db 'cfgwizBe7BK2816',0
aCfgwizbe7bk281_0 db 'cfgwizBe7BK2816',0
aDefault     db 'Default',0
aHelen       db 'helen',0
a1137389743nxsh_0 db '1137389743nxshkhjhgee',0
```


Quarantine 101

- IR investigations
- Multiple organizations in Israel
 - Government related
- Super high value targets
- Operations interrupted
 - Quarantine of various binaries



Alert #1

➤ Compiling dedicated utilities during real time

➤ FJORDOHELPER

- Access and update FOCUSFJORD registry configuration
- Remove FOCOSFJORD persistence and binaries

➤ PROXYFJORD

- Stand alone communication module
- Allows decreased number of backdoor instances in the field

Alert #2

➤ Introduction of upgraded HYPERBRO to the field

➤ Quick and dirty fixes

- Replacing vulnerable legit binary
- Loader DLL name changed accordingly
- Added capabilities to the backdoor

➤ **BIG** MISTAKE. **BIG**. **HUGE**.

Don't Panic, Take a Deep Breathe

- Need to disable Windows Defender and EDRs
- Looking for solutions to access protected processes
- Go where all developers in need go to
 - Stack Overflow, GitHub



The “aha” Moment



☰ README.md

KDU

Kernel Driver Utility

System Requirements

- x64 Windows 7/8/8.1/10/11;
- Administrative privilege is required.

Purpose and Features

The purpose of this tool is to give a simple way to explore Windows kernel/components without doing a lot of additional work or setting up local debugger. It features:

- Protected Processes Hijacking via Process object modification;
- Driver Signature Enforcement Overrider (similar to DSEFlx);

Currently Supported Providers

Provider Id	Product Vendor	Driver	Software package	Code base	Version
0	Intel	IQVM64/Nal	Network Adapter Diagnostic Driver	Original	1.03.0.7
1	MSI	RTCore64	MSI Afterburner	Semi-original	4.6.2 build 15658 and below
2	Gigabyte	Gdrv	Gigabyte TOOLS	MAPMEM NTDDK 3.51	Undefined
3	ASUSTeK	ATSZIO64	ASUSTeK WinFlash utility	Semi-original	Undefined
4	Patriot	MsIo64	Patriot Viper RGB utility	WINIO	1.0
5	ASRock	GLCKIO2	ASRock Polychrome RGB	WINIO	1.0.4
6	G.SKILL	EneIo64	G.SKILL Trident Z Lighting Control	WINIO	1.00.08
7	EVGA	WinRing0x64	EVGA Precision X1	WINRING0	1.0.2.0
8	Thermaltake	EneTechIo64	Thermaltake TOUGHRAM software	WINIO	1.0.3

Always Appreciate a Good Vintage

☰ README.md

Stryker

Multi-purpose proof-of-concept tool based on CPU-Z CVE-2017-15303

System Requirements

- x64 Windows 7/8/8.1/10;
- Stryker designed only for x64 Windows;
- Administrative privilege is required.

Features

- Driver Signature Enforcement Override (similar to DSEFlx);
- Protected Processes Hijacking via Process object modification;
- Driver loader for bypassing Driver Signature Enforcement (similar to TDL).

Usage

STRYKER -dse on | off

STRYKER -prot ProcessID (ProcessID in decimal form)

And...It Works!

The Windows Update service entered the **stopped state**. Event ID 7036

The EDR service **terminated unexpectedly**. It has done this 1 time(s).
The following corrective action will be taken in 5000 milliseconds: Restart the service. Event ID 7031

The Windows Defender service is marked as an **interactive service**.
However, the system is configured to not allow interactive services.
This service may **not function properly**.

Evolution of Bad

- High value target
- Accumulated knowledge of “Stryker”
- Higher detection rates for FOCUSFIORD and HYPERBRO
- Development of new module that remains persist in kernel space



1
Unknown Dropper
↓
creates service
creates entries wdsz...

2
Xsg.exe

side loads

SETUP ENGINE.DLL

GUARDVAIL + OPSEC - Timestamp

loads

SETUPENGINE.HLP
packed (silkwrap)
shellcode

↓ Extract & load

EXECUTES

3
new instance

Sychost.exe

logger component

writes

Wdszupdate // Payload.dll

read & decrypt & inject

THA sig so
SPASCH

PASSAMDATA/x.log

documents
next loading chain
cleartext

4

CPUZ

Wdszupdate /
read & decrypt & loads

read & decrypt loads
Wdszupdate

5

Shellcode
Prcp...

Wdszupdate

6

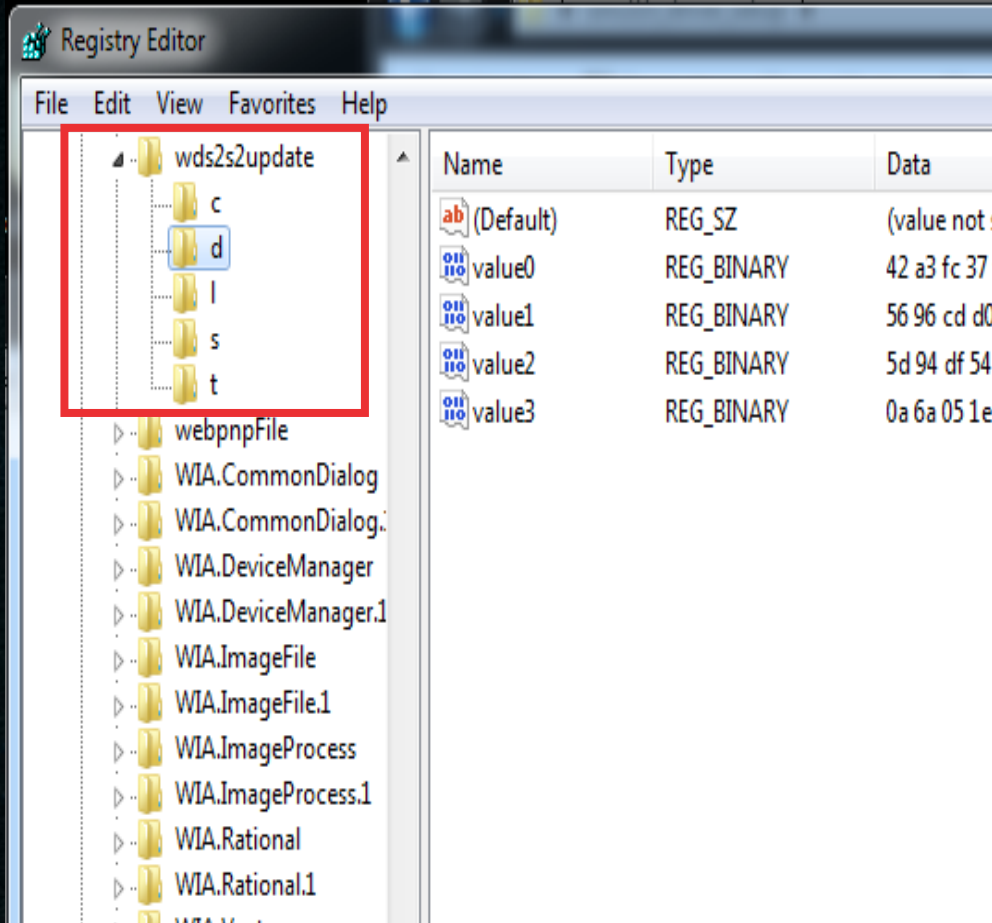
Fileless Kernel Driver

Wdszupdate
communication blobs

7

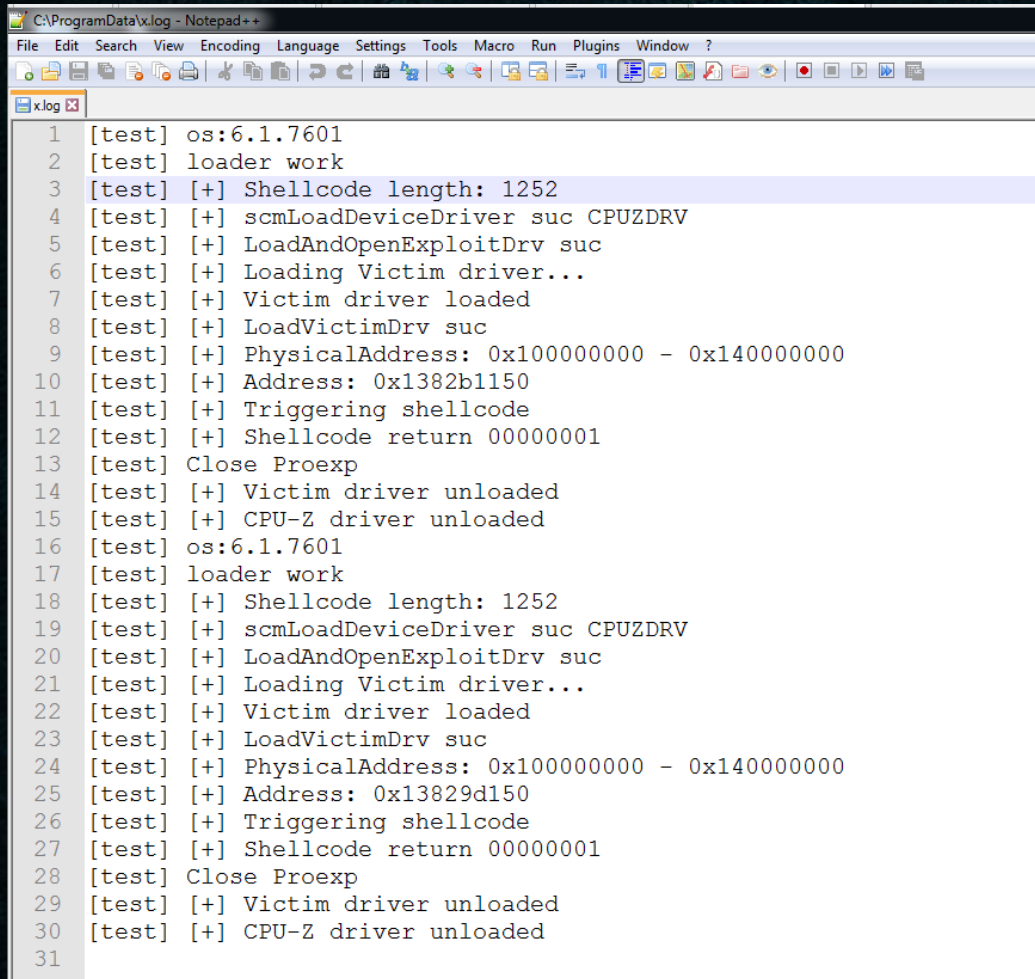
SSAS.exe

Setting Up Evil



- Classic **UNC215** loading chain routine
- Requires prior setup
 - Execution begins by a previously installed service
 - Payloads should already exist on host's registry
- New payload extracted from the shellcode
 - Begins the new chain
 - Decrypts and execute the first registry entry

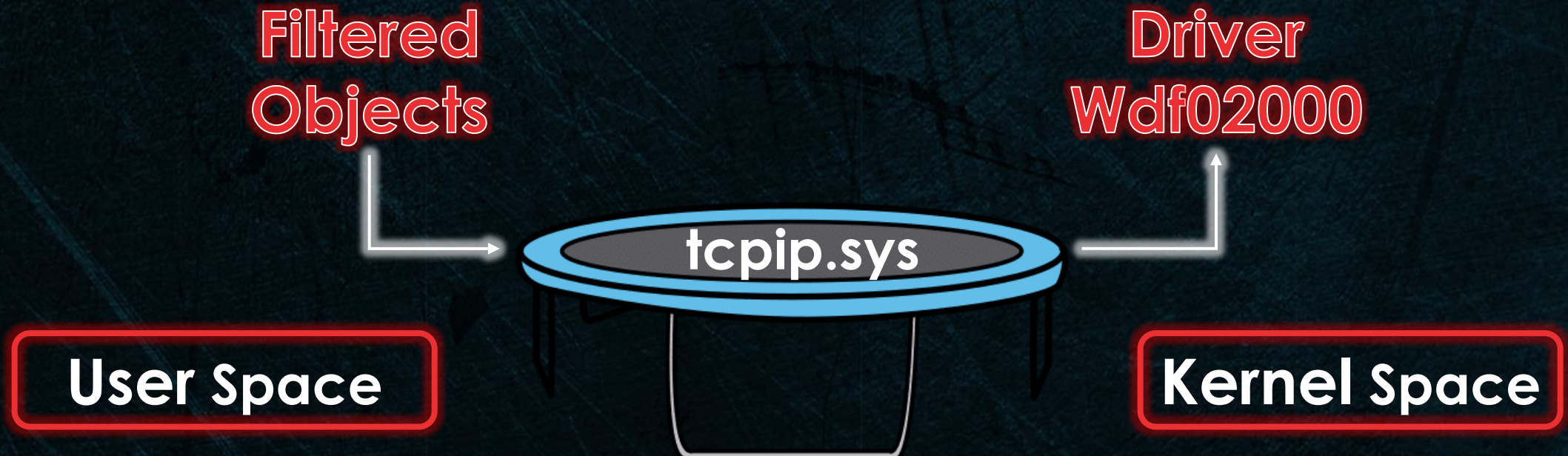
Setting Up Evil



```
1 [test] os:6.1.7601
2 [test] loader work
3 [test] [+] Shellcode length: 1252
4 [test] [+] scmLoadDeviceDriver suc CPUZDRV
5 [test] [+] LoadAndOpenExploitDrv suc
6 [test] [+] Loading Victim driver...
7 [test] [+] Victim driver loaded
8 [test] [+] LoadVictimDrv suc
9 [test] [+] PhysicalAddress: 0x100000000 - 0x140000000
10 [test] [+] Address: 0x1382b1150
11 [test] [+] Triggering shellcode
12 [test] [+] Shellcode return 00000001
13 [test] Close Proexp
14 [test] [+] Victim driver unloaded
15 [test] [+] CPU-Z driver unloaded
16 [test] os:6.1.7601
17 [test] loader work
18 [test] [+] Shellcode length: 1252
19 [test] [+] scmLoadDeviceDriver suc CPUZDRV
20 [test] [+] LoadAndOpenExploitDrv suc
21 [test] [+] Loading Victim driver...
22 [test] [+] Victim driver loaded
23 [test] [+] LoadVictimDrv suc
24 [test] [+] PhysicalAddress: 0x100000000 - 0x140000000
25 [test] [+] Address: 0x13829d150
26 [test] [+] Triggering shellcode
27 [test] [+] Shellcode return 00000001
28 [test] Close Proexp
29 [test] [+] Victim driver unloaded
30 [test] [+] CPU-Z driver unloaded
31
```

- Based on “Stryker” with notable changes
- Responsible for creating and updating log file
- Extracts shellcode from registry
- Loads vulnerable driver “cpuz141.sys”
- Loads abused driver “procexp152.sys”,
overwrites dispatch handler
- Trigger shellcode – loads fileless malicious
driver
- Unload drivers

Playground for Filter Managers



So Safe Much Hidden

- Full backdoor injected to lsass.exe
- Supported communication path masquerades as legit web server
- Magic cookie value
- Using WFP to inject traffic directly to TCPSTACK





Same same, but DIFFERENT

- Registry stored artifacts
- Same loading chain – host name-based guardrail
- Stealthier backdoor, same capabilities
- Same driver – now with more memory!

```
result = GetModuleHandleW(0);
v1 = result;
if ( result )
{
    Sleep(7u);
    v2 = (char *)v1 + *((_DWORD *)v1 + 15);
    if ( v2 )
    {
        v3 = (char *)v1 + *((_DWORD *)v2 + 10);
        if ( v3 )
        {
            v4 = &loc_1000161B - (_UNKNOWN *)v3;
            v5 = &loc_10001001 - (_UNKNOWN *)v3;
            v6 = 8;
            do
            {
                v3[v4] ^= *v3;
                v3[v5] ^= *v3;
                ++v3;
                --v6;
            }
        }
    }
}
```

```
memset(buffer, 0, sizeof(buffer));
if ( GetComputerNameA(Buffer, &i_1) )
{
    my_key_size = i_1;
    v6 = my_module_offset[1];
    Buffer[i_1] = *my_module_offset;
    Buffer[my_key_size + 1] = v6;
    enc_buffer_size = (char *)DllMain - (char *)text_section;
    my_tot_key_size = my_key_size + 2;
    my_buffer_loc = 0;
    cur_loc = 0;
    for ( i_1 = (char *)DllMain - (char *)text_section;
          my_buffer_loc < enc_buffer_size;
          my_buffer_loc += my_tot_key_size )
    {
        for ( i = 0; i < my_tot_key_size; ++cur_loc )
        {
            if ( cur_loc >= enc_buffer_size )
            {
                break;
            }
            *((_BYTE *)text_section + i + my_buffer_loc) ^= Buffer[i];
            enc_buffer_size = i_1;
            ++i;
        }
    }
}
```


Conclusions

- **China** spies on Israel
- Global fails for defenders
- **UNC215** – engineers, not researchers
- Dedicated resources assigned for Middle Eastern targeting



Thank You!

Stav Shulman
Yuri Rozhansky

MANDIANT®