viettel security | #FIRSTCON24

DEFENSIVE SOLUTIONS

- The Golden Gate for Targeted Attack

Hoang *Vu Duc*, **Tu** *Nguyen Thanh*, **Quang** *Tran Minh*

Viettel Threat Intelligence, Viettel Cyber Security

ABOUT US

viettel security

HOANG VU DUC
Threat Analyst
hoangvd7@viettel.com.vn

TU NGUYEN THANH
Threat Intelligence Manager
tunt22@viettel.com.vn

QUANG TRAN MINH
Cyber Security Service Director
quangtm4@viettel.com.vn

VIET NAM

CONTENT

viettel security

viettel security

1. INTRODUCTION

Threat Hunting – ZeroTrust (1)

We has developed an advanced malware scanning toolkit:

Covering MITRE ATT&CK

Capable of detecting advanced malware using Process Injection techniques.

Leave no small sign unnoticed

How did we find it?

CommandLine	"C:\Windows\TEMP\KAVREM~1\A72617~1\exec\fake.exe"
CurrentDirectory	C:\Windows\TEMP\KAVREM~1\A72617~1\exec\
User	NT AUTHORITY\SYSTEM
LogonGuid	{75aa81f9-d615-6627-e703-000000000000}
LogonId	0x3e7
TerminalSessionId	0
IntegrityLevel	System
Hashes	MD5=944F7C9DB34B4C5587DCFCEA865A6A06,SHA256=BA20EB674FBB0A6E4300F66150589FF6842D3989A098B9C2DFA93E1823E618C
ParentProcessGuid	{75aa81f9-f3c5-664f-de0a-000000001400}
ParentProcessId	6444
ParentImage	C:\Windows\Temp\KAV Remote Installations\a726170c-83a0-4ea5-b282-4fa81bce645dc2879ca1-7fe5-4c56-9db7-19fd56148f58\setup.exe
ParentCommandLine	"C:\Windows\TEMP\KAV Remote Installations\a726170c-83a0-4ea5-b282-4fa81bce645dc2879ca1-7fe5-4c56-9db7-19fd56148f58 \setup.exe" /s /z"/p\"TASK_ID=a726170c-83a0-4ea5-b282-4fa81bce645d\""
ParentUser	NT AUTHORITY\SYSTEM

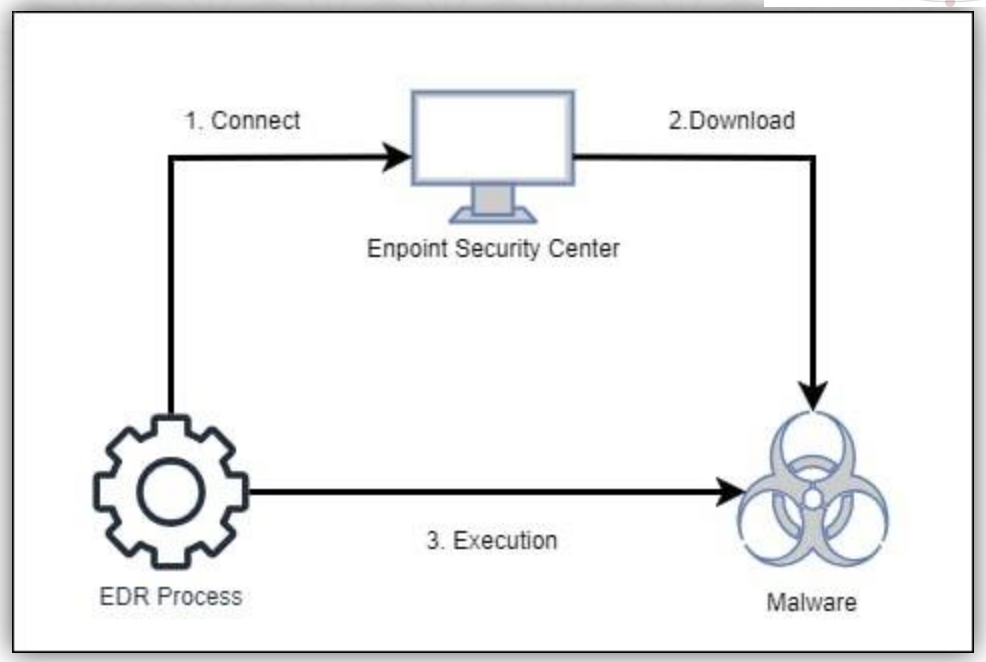
How did we find it?

svchost.exe	5320		C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	NT AUT...\LOCAL SERVICE	
avpsus.exe	340		"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avpsus.exe"	NT AUTHORITY\SYSTEM	
klnagent.exe	1004	2.50	"C:\Program Files (x86)\Kaspersky Lab\NetworkAgent\klnagent.exe"	NT AUTHORITY\SYSTEM	274.61 kB...
vapm.exe	4952	0.02	"C:\Program Files (x86)\Kaspersky Lab\NetworkAgent\vapm.exe"	NT AUTHORITY\SYSTEM	
cmd.exe	3264		/c "C:\Windows\TEMP\KAV Remote Installations\a726170c-83a0-4ea5-b282-4fa81bce645dc2879ca1-7fe5...	NT AUTHORITY\SYSTEM	
setup.exe	6444	0.01	"C:\Windows\TEMP\KAV Remote Installations\a726170c-83a0-4ea5-b282-4fa81bce645dc2879ca1-7fe5-4c...	NT AUTHORITY\SYSTEM	824 B/s
fake.exe	5480		"C:\Windows\TEMP\KAVREM~1\A72617~1\exec\fake.exe"	NT AUTHORITY\SYSTEM	
avp.exe	6856		"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe" -r	NT AUTHORITY\SYSTEM	
avpui.exe	4672		"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avpui.exe" -hidden	DESKTOP-QT0...\windows	

Threat Hunting – ZeroTrust (2)

We detected the 1st incident:

- Detected malware on a system protected by EDR.
- EDR Process executed Malware Process.
- Malware binary was downloaded from Endpoint Security Center.



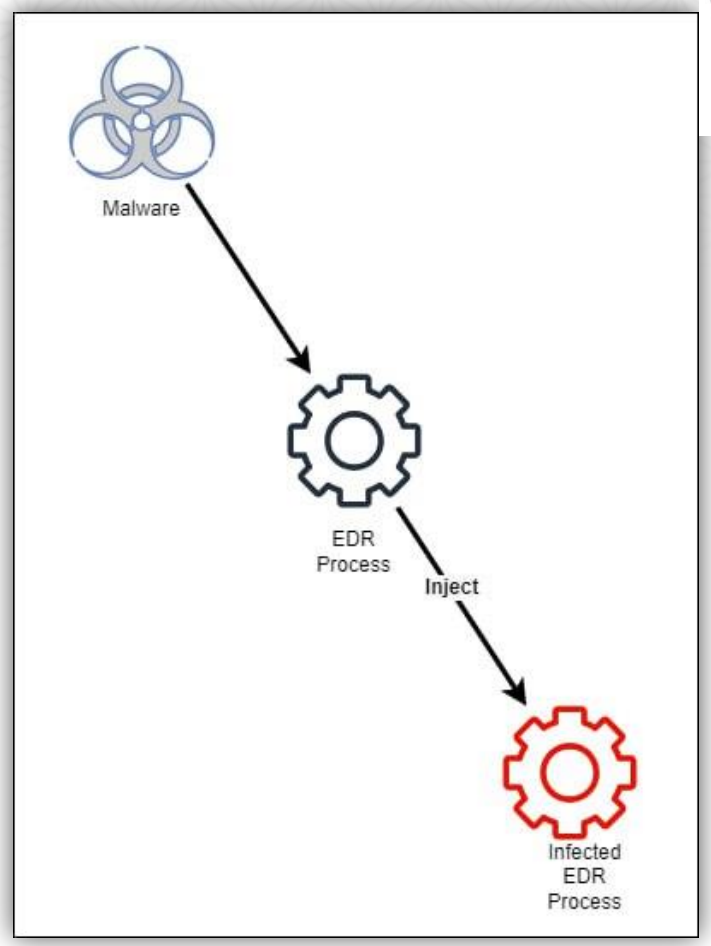
How did we find it?

Time of D...	Process Name	PID	Operation	Path	Result	Detail	
11:45:32.4...	ksnagchk.exe	2876	Load Image	C ksnagchk.exe	SUCCESS	Image Base: 0x4000...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffd4...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775e...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffd4...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffd4...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x775d...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76ca...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x7725...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x76f7...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\win32u.dll	SUCCESS	Image Base: 0x76e8...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x7695...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Image Base: 0x7568...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: 0x7717...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\ucrtbase.dll	SUCCESS	Image Base: 0x7683...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x76ab...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x755c...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x75d0...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x75c4...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x7559...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C PAVSHLD.dll	SUCCESS	Image Base: 0x7473...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x76ea...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x75ba...	4156
11:45:38.1...	OneDriveStandal...	1372	Load Image	C:\Windows\System32\msxml6.dll	SUCCESS	Image Base: 0x7ffd3...	1368

Threat Hunting – ZeroTrust (3)

We detected the 2nd incident:

- Detected malware on a system protected by EDR.
- The malware was running on EDR's Process.
- Malware binary lied in the installation directory of EDR



What did we have?

- Endpoint detection and response (EDR)
- Anti-virus (AV)
- Network Security Monitoring (NSM)
- Email Security Gateway (ESG)
- Security Information and Event Management (SIEM)

KEY FINDINGS

1. While scanning malware, it is crucial to pay attention to all processes, even those with signatures, whether they are from Windows or currently running software.
2. Security solutions can be utilized to distribute or conceal malware.
3. DLL Sideloading and Process Injection techniques are still commonly used by APT groups
4. APT groups understand both security solutions and malware scanning tools that the target using.

viettel security

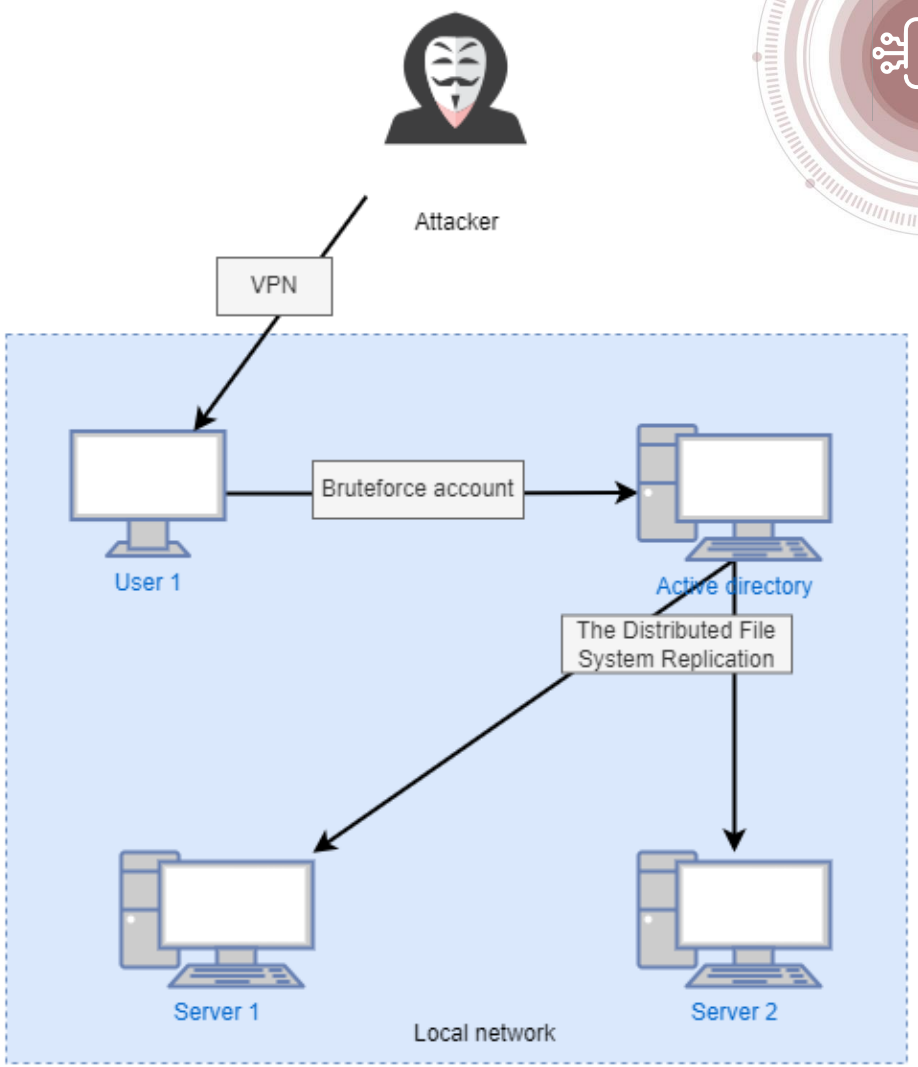
2. THE ATTACK

Attack Scenario (1)

Step 1: Attacker penetrates the internal network through VPN.

Step 2: Attacker successfully brute forces an admin domain account.

Step 3: Attacker gains access to AD and distributes file to other servers.

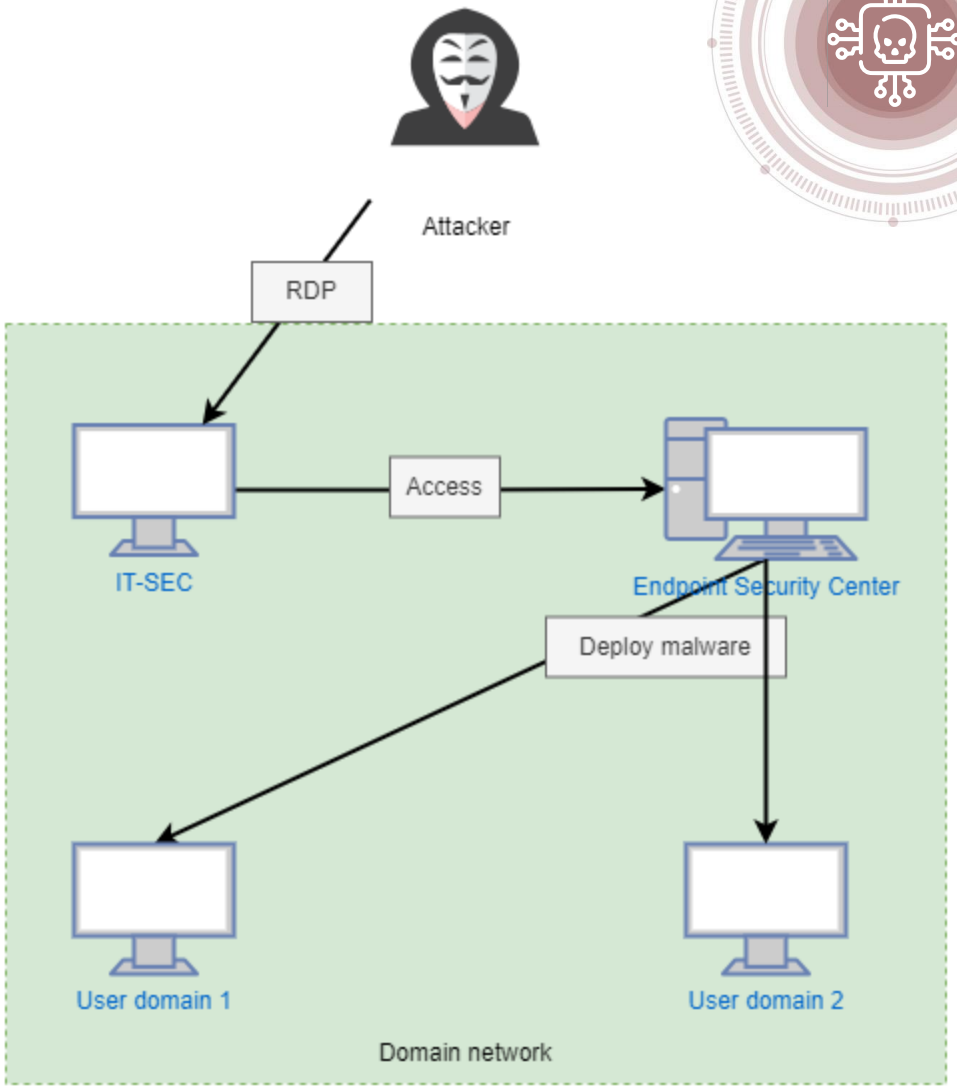


Attack Scenario (2)

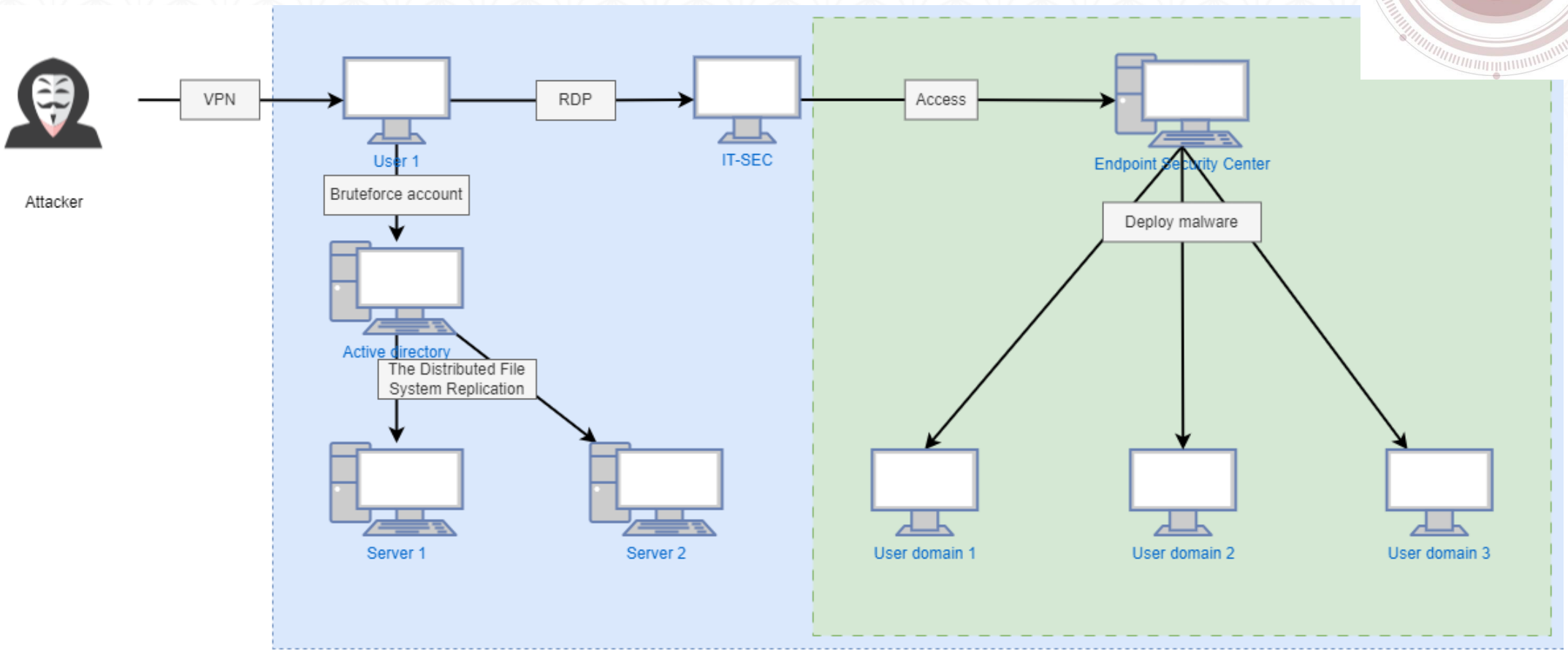
Step 1: Attacker uses RDP to an IT-SEC computer.

Step 2: Attacker gains access to Enpoint Security Center.

Step 3: Attacker deploys malware to all computers.

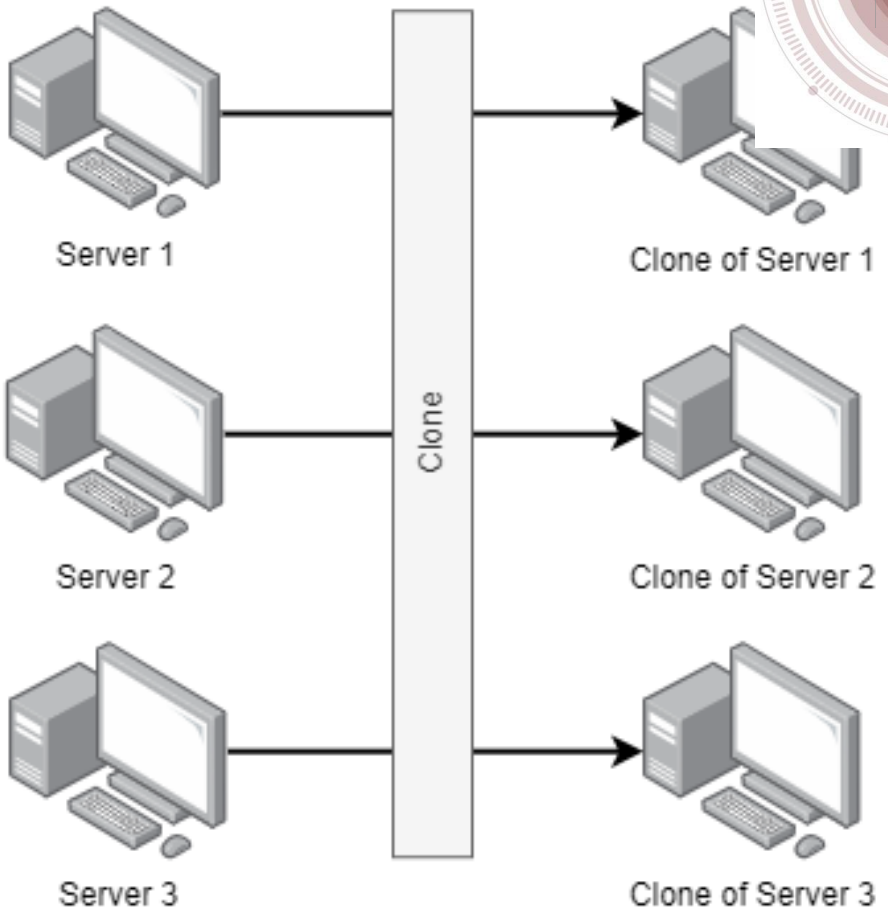


Comprehensive Attack Scenario



Account Security Center

- The organization reused a cloned version of the system in the past.
- Security Center admin account's password has not been changed.
- There was an incident where hackers gained access to Server Security Center.



What is EDR?

EDR solutions must provide four primary capabilities:

- Detect security incidents
- Investigate security incidents
- Contain the exploit at the endpoint
- Provide guidance for remediation

Source: https://www.gartner.com/en/documents/3978685

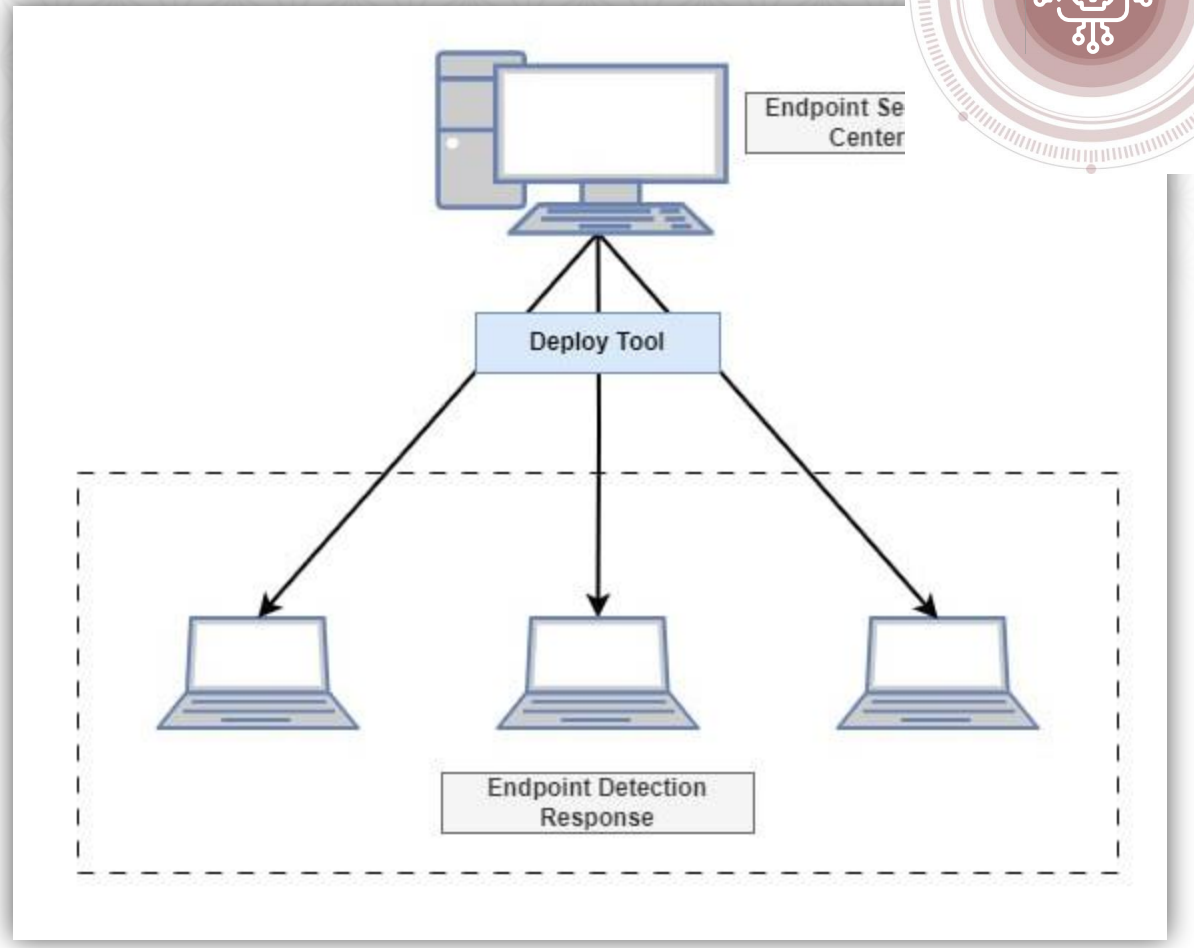
ENDPOINT DETECTION & RESPONSE

(EDR)

“Deploy tool” Feature

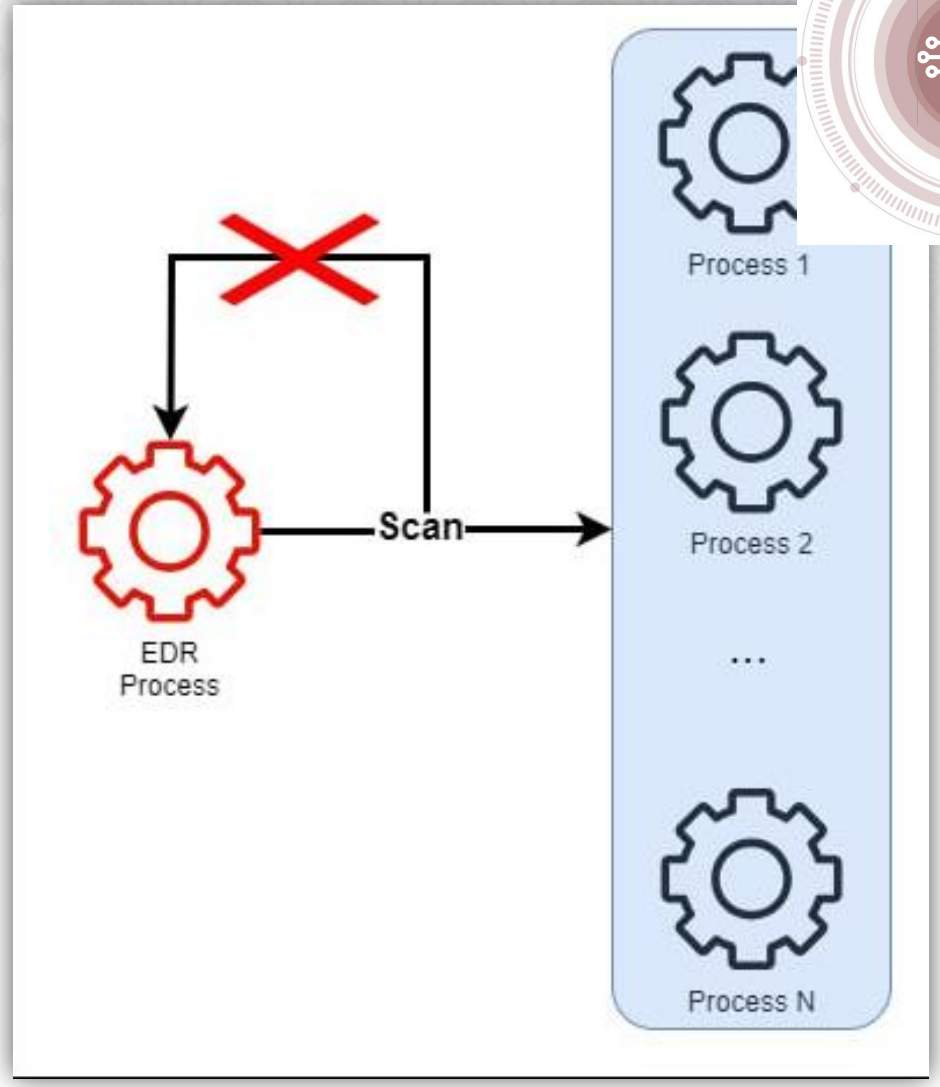
- Deploy a binary file, a script, etc. to endpoint.
- Support Incident response, Forensic, Investigation, etc.

“An excellent feature for distributing malware”



“Infected” EDR

- Tính năng rà quét file không kiểm tra thư mục cài đặt của EDR.
- Tính năng rà quét tiến trình không kiểm tra tiến trình của EDR



“Nơi nguy hiểm nhất chính là nơi an toàn nhất”

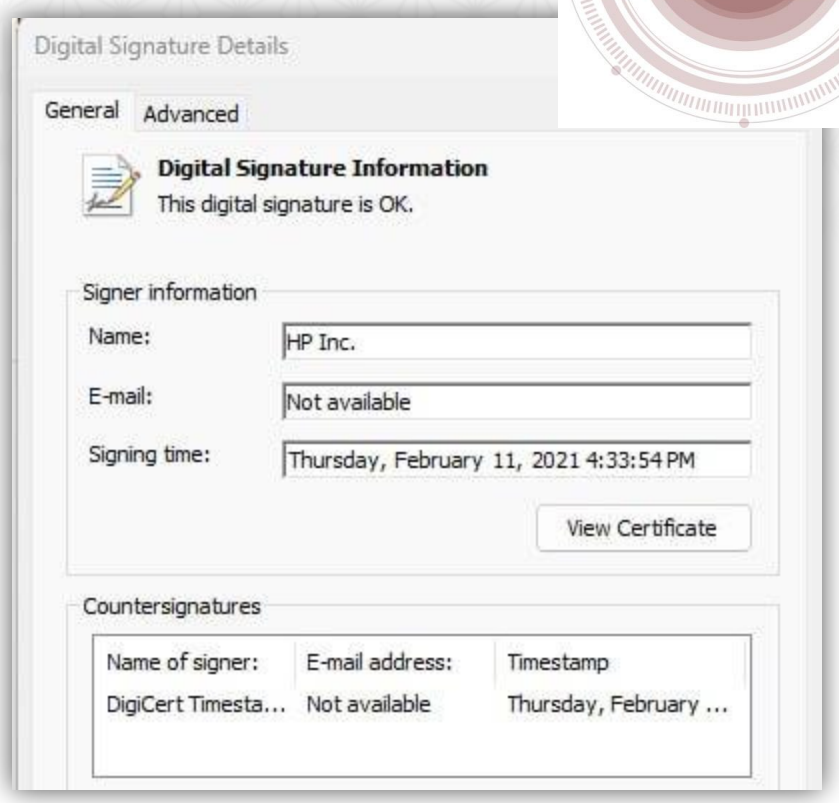
viettel security

3. MALWARE & TOOLS

Cobaltstrike Malware

- The malware leverages binary HPNotifications.exe to conduct DLL Sideloading.
- After being executed, the malware included in WTSAPI32.dll file is triggered and loads Cobaltstrike shellcode.

Module	Party	Path
hpnotifications.exe	User	C:\ProgramData\HPNotifications.exe
wtsapi32.dll	User	C:\ProgramData\WTSAPI32.dll
version.dll	System	C:\Windows\System32\version.dll
apphelp.dll	System	C:\Windows\System32\apphelp.dll
win32u.dll	System	C:\Windows\System32\win32u.dll
kernelbase.dll	System	C:\Windows\System32\KernelBase.dll



viettel security

Cobaltstrike Malware

- C2: opendnsns.net:443
- Domain undetected on Virustotal
- Mutex: guid {75A97DF4-54BC-41AA-AEC7-5B553772017B}

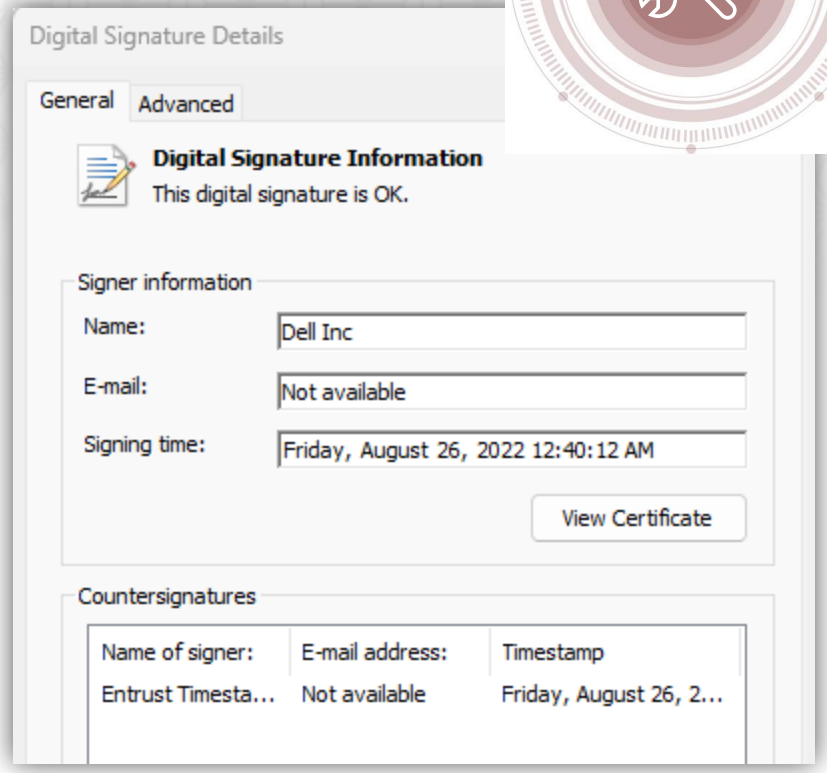
```
b'.' 2e
payload type                    0x0001 0x0002 8 windows-beacon
port                            0x0001 0x0002 443
sleeptime                       0x0002 0x0004 74312
maxgetsize                      0x0002 0x0004 2097180
jitter                          0x0001 0x0002 40
publickey                       0x0003 0x0100 30819f300d06092a864886f70d0101010500
4e5943bbe67fc9b5917fa3e91538c6bdf47089ade3f3d7e9c0f1290df375cca21d3cfab2f5966d6116c
000000000000000000000000000000000000000000000000000000000000000000000000000000000

server,get-uri                  0x0003 0x0100 'opendnsns.net,/v1.0/drive/'
SpawnTo                         0x0003 0x0010 'eö&\x0b§]H<]ÄèÐã¾j«'
spawnto_x86                     0x0003 0x0040 '%windir%\\syswow64\\netcfg.exe'
spawnto_x64                     0x0003 0x0040 '%windir%\\sysnative\\netcfg.exe'
CryptoScheme                    0x0001 0x0002 0
get-verb                        0x0003 0x0010 'GET'
post-verb                       0x0003 0x0010 'POST'
HttpPostChunk                   0x0002 0x0004 0
license-id                      0x0002 0x0004 0 trial or pirated? - Stats uniques
bStageCleanup                   0x0001 0x0002 1
bCFGCaution                     0x0001 0x0002 1
useragent                       0x0003 0x0100 'Mozilla/5.0 (Windows NT 6.3; Win64;
post-uri                        0x0003 0x0040 '/OneCollector/1.0/'
Malleable_C2_Instructions       0x0003 0x0100
form Input: [7:Input,4,1:21,2:7,8]
```

viettel security

NPS Malware

- The malware leverages binary DellcustomerConnect.exe to conduct DLL Sideloading.
- After being executed, the malware included in DellcustomerConnect.dll file is triggered.

Module	Party	Path
dellcustomerconnect.ex	User	C:\ProgramData\McAfee\DellCustomerConnect.exe
dellcustomerconnect.dl	User	C:\ProgramData\McAfee\DellCustomerConnect.dll
apphelp.dll	System	C:\Windows\System32\apphelp.dll
kernelbase.dll	System	C:\Windows\System32\KernelBase.dll
kernel32.dll	System	C:\Windows\System32\kernel32.dll
ntdll.dll	System	C:\Windows\System32\ntdll.dll



viettel security

NPS Malware

- Create tunnel connect to 194.87.45.17:443.
- NPS is open-source, powerful intranet penetration proxy server.
- https://github.com/ehang-io/nps.

```
00 00 00 00 00 00 00 00 ................
00 00 00 00 43 46 4D 54 ............CFMT
36 31 34 39 32 64 32 2D -vkey=061492d2-
66 2D 61 62 39 36 2D 37 0f2b-405f-ab96-7
64 62 34 20 2D 73 65 72 b6b54034db4 -ser
38 37 2E 34 35 2E 31 37 ver=194.87.45.17
70 65 3D 74 63 70 00 00 :443 -type=tcp..
00 00 00 00 00 00 00 00 ................
```

```
OS          windows
Arch        amd64
Compiler    1.18.1 (2022-04-12)
Build ID    76VhzRILUl2vIiY6K6XO/2pLFsDN0Hs9ajxAJB4wA/6DWHuQEUuy58W_kKc
GoRoot      go
Main root   ehang.io\nps\cmd\npc
# main      12
# std       128
# vendor    47
-compiler   gc
-ldflags    -w -s
CGO_ENABLED 0
GOARCH      amd64
GOOS        windows
GOAMD64     v1
```

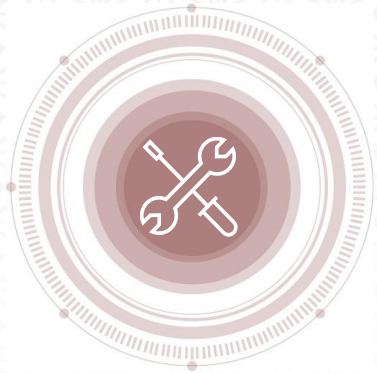
viettel security

Malware embedded within EDR

Time of D...	Process Name	PID	Operation	Path	Result	Detail	
11:45:32.4...	ksnagchk.exe	2876	Load Image	C[redacted]ksnagchk.exe	SUCCESS	Image Base: 0x4000...	
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffd4...	
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775e...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffd4...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffd4...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x775d...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76ca...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x7725...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x76f7...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\win32u.dll	SUCCESS	Image Base: 0x76e8...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x7695...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Image Base: 0x7568...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: 0x7717...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\ucrtbase.dll	SUCCESS	Image Base: 0x7683...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x76ab...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x755c...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x75d0...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x75c4...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x7559...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C[redacted]PAVSHLD.dll	SUCCESS	Image Base: 0x7473...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x76ea...	4156
11:45:32.4...	ksnagchk.exe	2876	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x75ba...	4156
11:45:38.1...	OneDriveStandal...	1372	Load Image	C:\Windows\System32\msxml6.dll	SUCCESS	Image Base: 0x7ffd3...	1368

viettel security

Suspicious DLL files



Detect 4 unsigned dll files in AV's folder:

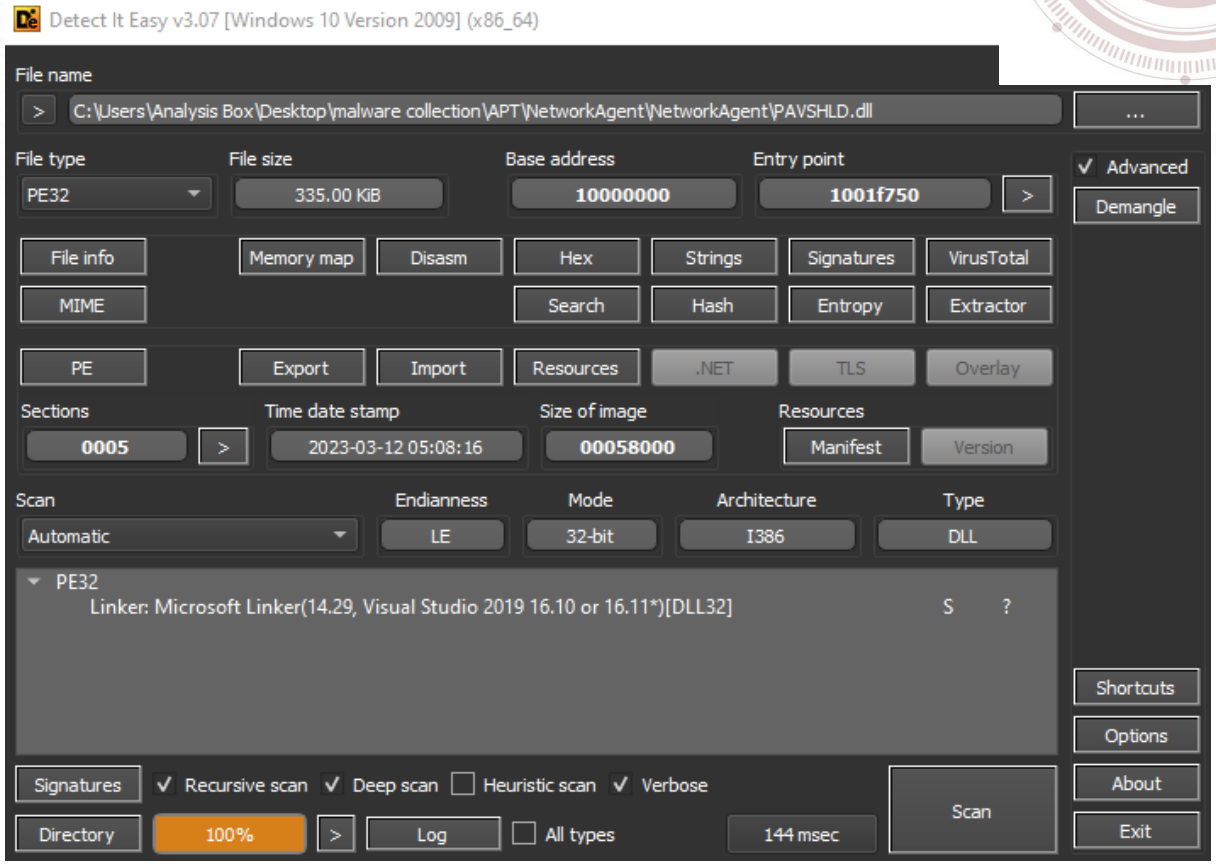
- Windivert.dll: Open-source module used to capture network packets.
- klcssa2.dll: Creates "klcsldcl.exe" process with "-sw" input.
- version.dll and PAVSHLD.dll: 2 main modules of the malware.

```
\NetworkAgent

        Status                                          Path
        ------                                          ----
        NotSigned                                       klcssa2.dll
        NotSigned                                       PAVSHLD.dll
        NotSigned                                       version.dll
        NotSigned                                       WinDivert.dll
```

viettel security

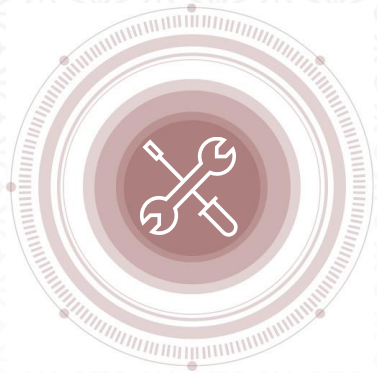
PAVSHLD.DLL Properties

- **Path:** C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- **Create time:** 2023-03-12 05:08:16
- **Tool:** Visual Studio 2019 16.10



viettel security

Malware detecting scan tools



autoruns | checkinject | cigui | listdlls | procdump | procexp | procmon | qrcode | regjump | regswitch | samplecollector | sigcheck | strings | tcpview | vmmap | vscshellscanner | mftrcrd | moveyourmouse | lastactivityview | jumplistsview | winprefetchview

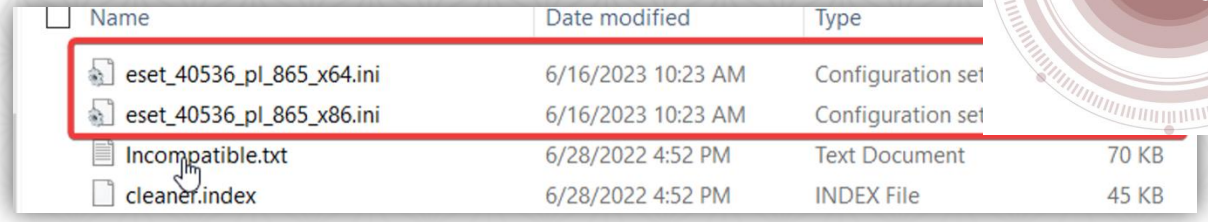
```
v39._Mysize = 0;
v39._Myres = 15;
// autoruns, checkinject, cigui, listdlls, procdump, procexp, procmon, qrcode, regjump, regswitch, samplecollector, sigcheck, strings, tcpvie
std::string(
  &v39,
  "Cei5l6kUAHkNuCgwzVb2lQHWmxRSnitIKsoZLZwh9xgH7rhqJTv9N1ZvWYg7xa6XaUJJXbJn5BrrACOl1plsDT2cKmexfoItP4mG5zp0gsggn9WaPA0i"
  "JVfqDtqykYX37U8lZZnL22U89/AXi2aC3iWcn8JUMLHjZ/iSB+bBxuvaNkvlH7c7DBSNPHoO7ZMZE3VIEL5B2fcDM0zJ7bBttb+2wfKFJNnjU/u3ojBu"
  "ElSWbHHExTdpEYiqqvbqjS4qj9u1YE6xcHY1uyt2IhLmHKCHeScBWtdwwz==",
  0x124u);
rc4_decrypt(
  (size_t *)&v53,
  v39.u._Ptr,
  *((int *)&v39.u._Ptr + 1),
  *((int *)&v39.u._Ptr + 2),
  *((int *)&v39.u._Ptr + 3),
  v39._Mysize,
  v39._Myres);
```

viettel security

Encrypted Payload

The malware searches for Data/Cleaner folder within kaspersky and finds these file:

- eset_40536_pl_865_x86.ini
- eset_40536_pl_865_x64.ini



Name	Date modified	Type	
eset_40536_pl_865_x64.ini	6/16/2023 10:23 AM	Configuration set	
eset_40536_pl_865_x86.ini	6/16/2023 10:23 AM	Configuration set	
Incompatible.txt	6/28/2022 4:52 PM	Text Document	70 KB
cleaner.index	6/28/2022 4:52 PM	INDEX File	45 KB

```
[main]
name=Avast Software 8.0
detect-registry-value=HKEY_LOCAL_MACHINE\SOFTWARE\AVAST Software\Avast\Version=8.0
fullname=Avast Software 8.0
type=detect-only
os=all

[ak]
ak_use=true

[data]
PRYhezd57W+N28MwVj3MrTzbxAFwKipy1rJMqYJTg3wD4yFAPvZDiCT8vb2z4jScCycxRZLZS97f5rwj/ekebjoeFl8ETGwCugy/mkgRjRUyAYOu3TS5rAGbYr9YuwUWzdQBh65L+OT6l5hyY3ACLp
XefXSwPOmXcIcbG3tJzbXks5uXY8HLq2tmJgpi6uCHCO97NZHEdYNxUL1pgVbalIycRrf3SbYd0Mmdnbl3ZjX1T05aBEAQZ7YwqHp/ja+lllqQ/
LrGGRMUkLTgT2KU+gLeUhoy5X1APz8kiqjRDnMIIUcUq2kYaLuo9xW8P9IJoIB4i0IXL0Td71vaop1+Y2A5Hrhm1RyGKhEKGxBEI0v/+wjHjKREE5zG/
0EQ3T3UdFtkQ4m29QgOwm9OvtmO+sNPRvf9zPKIfuT7jwieBA5/vr2qWyz5a+VYX1CusVAaMF24W93CdzK+ZDN42G08hSmpRn0cEk+LPrXTDFk8ne/w+wvsOpQyOdDnU7WRjKJz3Iw5iVeh4aeJ+c
5jL84H3hUy2zAg7jKH5RzMAlanQ9STzgjSOA+g5NAboFyv1+ISNSH3E9xCNvg83xlk37c0l0NmEKmI4G2OYcz13n3pm+GAUcr0sYGTruIQG9SJl9u5XAURUbV8RAvKiyk7X7ner/4v8/
EBE3iSQKzqe8t45/1DxvycCuqu1jXm+O3GZYkexjQIL2fCDAKzyX9n67XM3dl9xagLt9QfgOjKGX5b7YH2PSk362606i5s41XMDNk7cTvS6qzVH/y52TCuaqZFvByzxVRkCjKj3bJLJIt0IqI4/
espUF1gW9izC/FELEx63n8hcgZTOfVIR/Ka0V2lUD4sHZbUPVE6ikeK+rHITBDmkBJsM4GGM0AbXngqHt0AWM8hCXNKHLujxU8GvRA0J8FB7Mj05oLts5hIfGmyln44063Wkxv2dtYycDrEYeHqEeb
G1z932tz5ts7ryaAQ+7p7ckYLiIrUHbi08KGT1FH0s0EIAl9WbeHWX0FWPniWdLHZjuwv7fyRH2k9ZpaBSUNdqWCjwWGTYE4QjDikeiBnS0G2wpWkzxEJMyViSowzReZTAUE0ja6rK
r8J+VhYKinoPh8YazHN7OOD2DG6ln6PRG+Pv9Nrom5Ca0R/ptz35vfF+XrgLMK17BMwrBr2Iy+0vuwLGSTFuZYnQm2q4Tx/5AZhARh9S/
UYpuYAXicTqzMX05KZ2e00GrdRScH2Va6rJZPLvfuDn4WKN1kh/A5Tkw/dmUVlV74clnM3C5bHK73iX6nN8PFkh+6Ozguwjm7uxjehN4iKMlRA3oCdb+swWAHfSs5bvZnpr5rQHnel7I6MDAbj9w/v
MuNcjkhmWcplVLvMzz+lsEmYyPup1IEaMGdztWX2hDyXxEjr8uw5o4zriHzdFBCi5NUUvkjnECj3CB1d4liCX8DNn0xzJGmU86QPSM43ROqcjP+pI+WX+H+VqBZ00YZ9aMfKvNeDj1HwP8VJoQtvVW
1SOXBIP7virTsNqvDtXqJV4ohbwRAooJI3pIQbGsQUYAavzNXvAqU3YGnCtL0JEHq/jvV0QSE2oFuUkYHwQINDpXzGZxAbNuADPZe3/
OUQdfIXcGWkpTw7mdMUcb8HOQWPuxqwnMTj4fB6+QSMTA6lCXxnb7FrZP/9nxN3Ihq3W+4EakFaPJEBnyYm1jnwsvivIF5zWCFJUo6oQl+5nPln7BBpBI/OQcDaZieyju/
nxTEAd9f//Gfj2Te26o+IAWEXzk43lYE111lvpPjkhtVQGutExEZsaPXzlyjZLH9UD29bTfbVOGcG/
XQnDsDKerWi1h235Nvt1BP7mVuGnAg7k0vrpaN070gk+q15dSzo2XuoJeh5Tev9y6Ps7V9oF0gwpECpTk/yhjvHAGjQ6bvfb1Qha+P61YoslWAdUpebYg1dH5HCQzOJWq/Uzy/fLut7lZwu/4bU8GN
e21cFxZfSf1855tZtZZE05LVq3C459jS+yr2mIXnpOa4yq9YxlGAIuv3pcl6gBSH10b2PRPvmGfTBX2+Nk9JlXjQJGLRP13jMK0fu3kqJQ9amtUchR0+FpqOto19hJPLWJEUw5RZNgNnHSFtLlPRPH
OVCtJ5o2Bcy4GJ/kLxK4IU6txzCJxIPJJdbTFKaXegVIoS1RFTrRjdEhHe+86sFpwyAXtje4oFoPc2fmDusq0yrerP3ZJEv/9YlNS6WM8RripPxc2U0X/
uZFpMDZsQmDAOnhpskDYySCg28pJGLNDlTbVZ/DJ5Y3Z8PlwOX2oGaeSNzgWrxCprLNwGz9sYehAJ3oAUf9XhMbu0cFZw2n9gVkaFEqzofwOmxUPem/
s6ORj38Q2ip4A9F56temEKG39YRRBHyQtxoNsR5VbtbxCao/LalT4sD0V7dH2eOyd+5UDkqLHH25ziyEFX/l/fFiK7q/br3xpcoKUdN8wTxsfdsWeosgiVkMnU3Bu/
c40XYrSdFI1XIFvjZQwDS0MSjPBctsngZxpwzwXXNhvaPtMOKsah+X2x34epeburK66RhOkbglZ9DdfDz/
55STRWav2EGE1dWGFDl2yjPEhwC4F6mCG8a0SE7+RsoOKHS5sByFslkjSe9P0Q587oriBvwn2PxZ0LQwZVhbfRO34C9yRpX/W+5sDMmuRPWGU2mCXTwxzXEYO5wmo1sBG0Gigkhy8ONmjdtHhyC2/
sXDVFLWeEGZdehDmDYjB1jpC0AjobFltVuqfQg/aZ7IGHXnFMkOYPhe2b11jrUTAYZhzX3HLzfZ8eQhAGqI4iAB5H9CLnLDUgJqQp7Wdq6gScmpXUCAtpAUiAJB2ReluktmYmmfdqkCoi3VBvS7BJ
tOmRmmk9bKcVBkHCoaO7reUeJKyEdsnOesxtBb2+8Xy99A5cD2A3F21cybpFH236yz8hmS3CKFmO4QYfkbS/BVhEa79aVtxPx9DL6uCq4VXw0UN5CF4RxP8xgIYZH8n2LCn0tGm4W/
HZClQ4sJxU17SRAlr5lRfoYoAASuhgHP6+l0tuHxjLO5Yd9HC2k1y8JACGPyaqkP9TkFVdj/gAim/
FJw6T4NhpGcuZVPamfmUYgqtDLRSXfVy+tsKssGWbmQdhr1bzgzxuUpHBgXSOMNuWfP5qjNE4Mhw6lbgUw4J6vRnLCcA2AY9TDxVHPtWRtgZ4/Q3Pbmz2LziSktzVnd2aWpKFHxVJKM4g0tY4/
B9IprJJmlBXjtGIzIWq+TT4ye09OmrZQlanOKIU3OkI635QcyLhIPko+QyKEJuPhfke955YVsZ5atNfzYtxB9aTeMWeYF2I4mwBTzyR3ZiEWjxMHInweZWXrP3ddC9/
jhryQLwb9d+t5jn1MyjmCf0UhMx05BkB+j4X4c430HG814vHa/ptqgokFkbIE24ImkPiJ6EeFnGPMy85Fjy/bXiUFuAcm/
8oU8V+IcLXiMHwlRyaDbSun9VjlE+wvtdpfdvQ0eJOtW4BnWGmerp2TFvX2EXyzMZVW8gR/XPhekCKIeGzSB0HtEyp9SLyWiHmMSgfzHM3nqbJP2BgJ034Rjqx3Brdi9ND/
au9f6LAWYS6eP+OjkhDp/H//Zk5TrkXofIDSmneRd6dThX3LTWz+a2xcYMB1NzEX3TxwHehE9RNRHhIhmJhicEHvlytK5TDhPM1ykRwMi+vlIrXEI6bifrwvmcmxDvWO8qH8b3wygmhniAvV71rwuY
```

Runs new process

PAVSHLD.DLL

- The malware creates the “klbtagt.exe” process.
- Inject decrypted payload INI files into the “klbtagt.exe” process.
- “klbtagt.exe” is also a module of Kaspersky.

Process Hollowing

- Create a new process in suspend form.
- Write payload into a newly created memory area.
- Change the execute pointer of the process in the newly created memory area.
- Continue executing the process.

```
if ( CreateProcess(p_Block, Ptr, 0, 0, 0,
  && (NtGetContextThread(ThreadHandle[1],
      (v5 = VirtualAllocEx(ThreadHandle[0], 0, Buffer.
{
  p_Buffer = &Buffer;
  if ( Buffer._Myres >= 0x10 )
    p_Buffer = (std_string *)Buffer.u._Ptr;
  Context.Eax = (DWORD)v5;
  NtWriteVirtualMemory(ThreadHandle[0], v5, p_Buffer,
  v7 = (int)ThreadHandle[2];
  NtSetContextThread(ThreadHandle[1], &Context);
  NtResumeThread(ThreadHandle[1], 0);
  CloseHandle(ThreadHandle[0]);
  CloseHandle(ThreadHandle[1]);
```

viettel security

PE Headless

- The payload is a PE file whose properties information is deleted.
- The malware needs to rebuild IAT for the payload
- RC4 and RTL_Decompess are used to rebuild PE's properties.

```
if ( first_entry_point->is_rc4_encrypted )
  decrypt_rc4(the_structure, first_entry_point->rc4_k
if ( _first_entry_point->is_rtl_decompress )
  v3 = RTL_Decompress(v3, _first_entry_point, v0, proc_addr);
mem = (struct_v2 *)allocate_memory(v3, v0, _first_entry_point)
create_section(v3, (int)mem, _first_entry_point);
relocation(mem, _first_entry_point);
fix_iat((int)mem, v6, v7, v8, _first_entry_point);
return jump_to_entry_point(_first_entry_point, (int)mem);
```

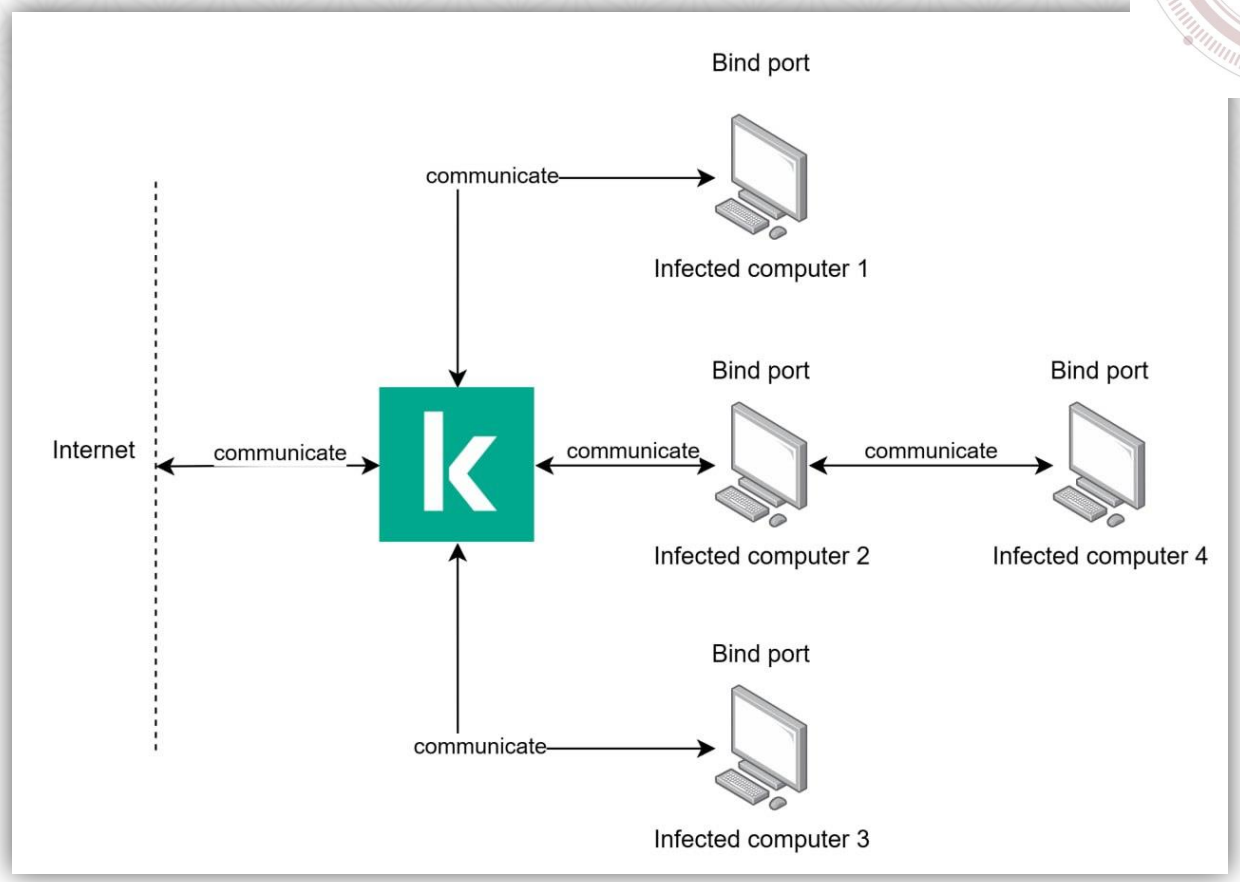
```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 2E 74 65 78 74 00 00 00 FA 6C 01 00 00 10 00  ..text...úl.....
00 00 6E 01 00 00 04 00 00 00 00 00 00 00 00 00  ..n.............
00 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00  ..... ..`.rdata.
00 C2 4B 00 00 00 80 01 00 00 4C 00 00 00 72 01  .ÂK...€...L...r.
00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00  .............@..
40 2E 64 61 74 61 00 00 00 6C 10 00 00 00 D0 01  @.data...l....Ð.
00 00 0A 00 00 00 BE 01 00 00 00 00 00 00 00 00  ......¾.........
00 00 00 00 00 40 00 00 C0 2E 72 73 72 63 00 00  .....@..À.rsrc..
00 E0 01 00 00 00 F0 01 00 00 02 00 00 00 C8 01  .à....ð.......È.
00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00  .............@..
```

viettel security

Malware utilizes AV's modules

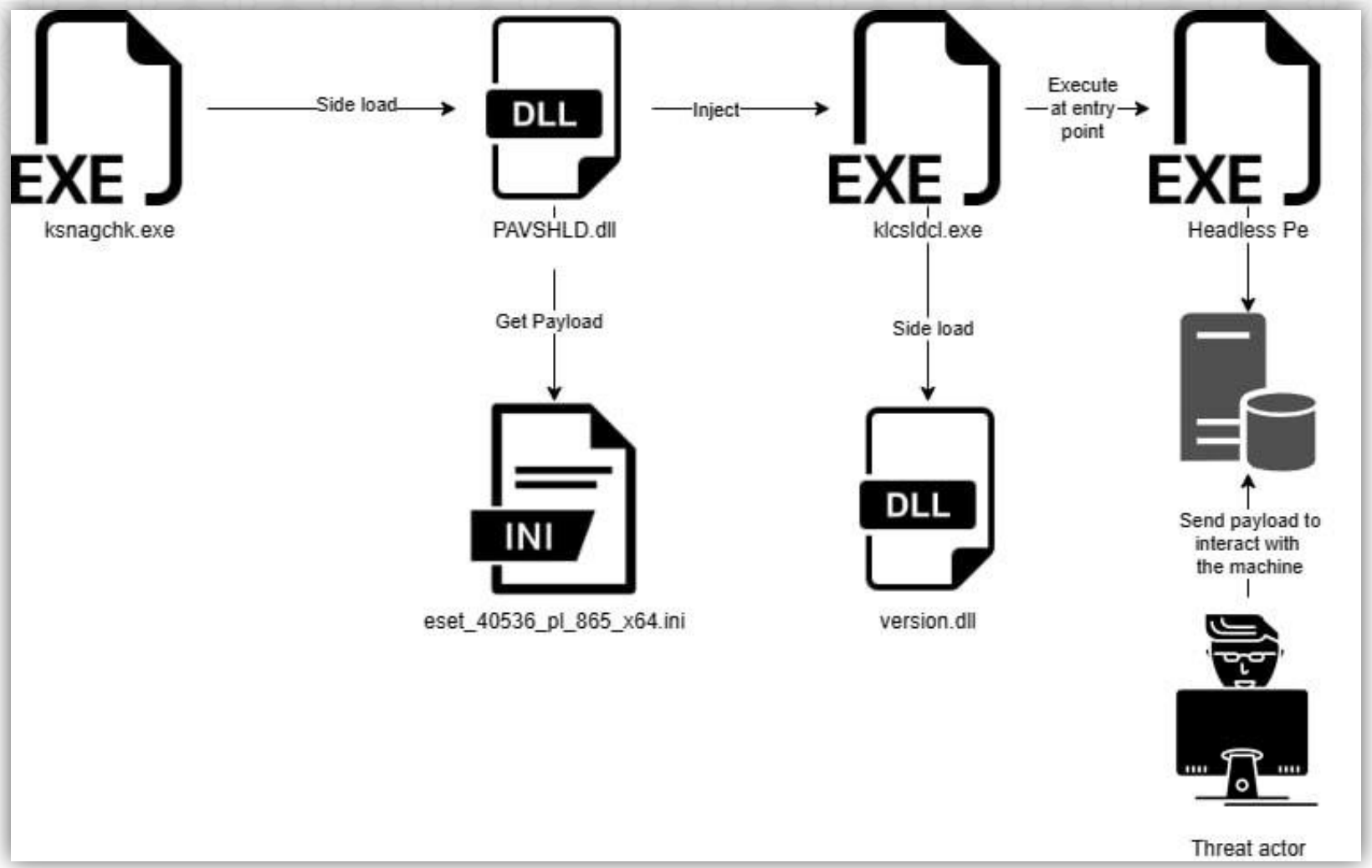
Create Server Bind to communicate within local network.

Port: 8090, 12345



viettel security

Attack scenario



viettel security

viettel security

4. RECOMMENDATION

Defense Solutions: Anti DLL SIDE-LOADING

- Sử dụng đường dẫn tuyệt đối hoặc hạn chế đường dẫn tương đối khi load dll
- Đảm bảo các hàm nhập hợp lệ hoặc dùng manifest để xác định file DLL hợp lệ
- Gọi hàm SetDllDirectory với tham số rỗng để loại bỏ thư mục hiện tại khi load dll

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity publicKeyToken="75e377300ab7b886" type="win32"
name="Test4Dir"
version="1.0.0.0" processorArchitecture="x86"/>
<file name="DirComp.dll" hash="35ca6f27b11ed948ac6e50b75566355f0991d5d9"
hashalg="SHA1">
<comClass clsid="{6C6CC20E-0F85-49C0-A14D-D09102BD7CDC}" progid="DirComp.
PathInfo"
threadingModel="apartment"/>
<typelibtlbid="{AA56D6B8-9ADB-415D-9E10-16DD68447319}" version="1.0"
helpdir=""/>
</file>
</assembly>
```

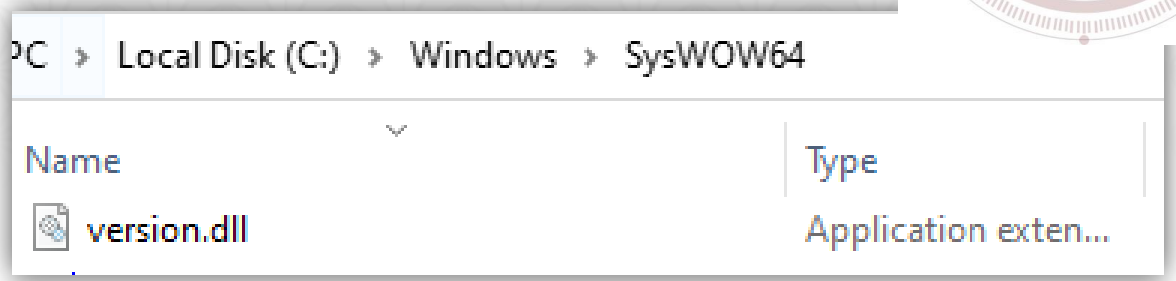
Source: https://www.mandiant.com/sites/default/files/2021-09/rpt-dll-sideloading.pdf

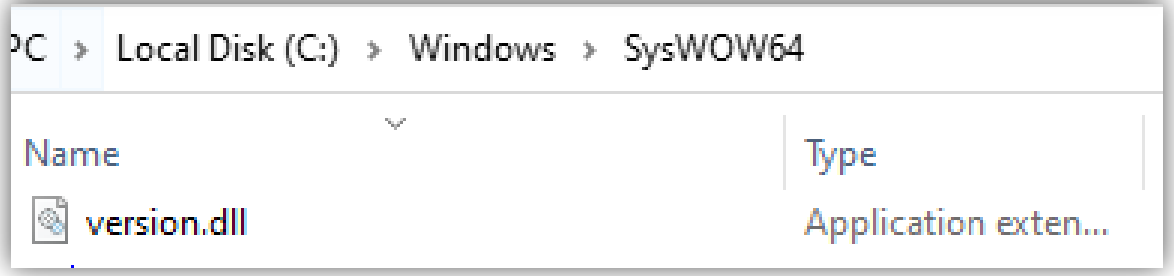
viettel security

DLL Sideloading detection guide (1)

For Persistent:

- DLL files do not have signature in the same folder.
- DLL files have the same name as the DLL file in the System32/Syswow64 folder (especially version.dll)
- DLL files have different MFT from other DLL files in the same folder.






```
orkAgent> gci * -include *.dll,*.exe | Get-AuthenticodeSignature | ?{$_.Status -ne "Valid"}

rkAgent\NetworkAgent

Status      Path
------      ----
NotSigned   PAVSHLD.dll
NotSigned   version.dll
```

viettel security

DLL Sideloading detection guide (2)

For Process:

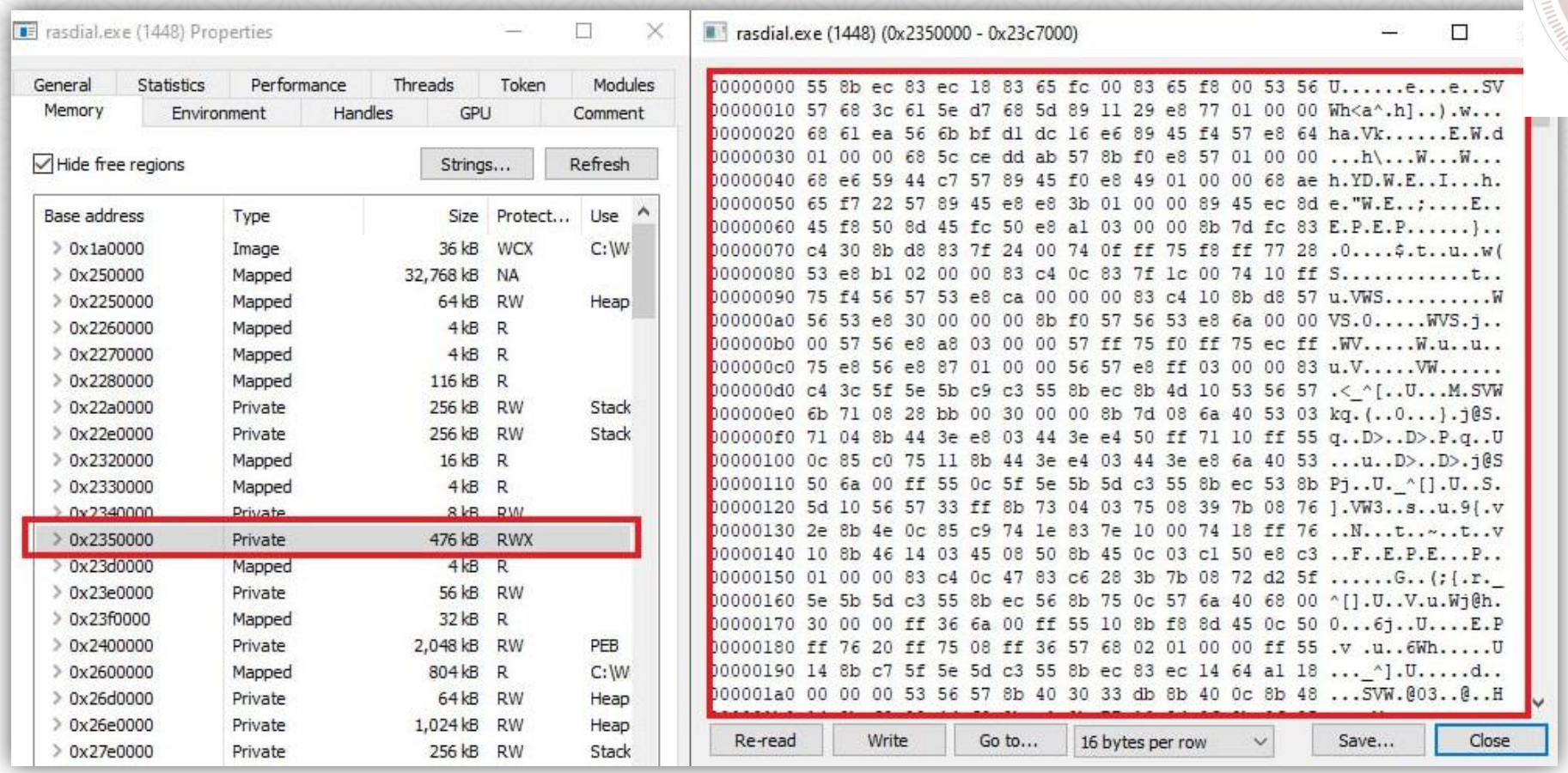
- Identify if the DLL file is loaded by process having the same path as exe files and different from the other DLL files.
- Check the signature and MFT of the DLL file to exe file or to other DLL files in the same folder.

ksnagchk.exe	User	C: NetworkAgent\ksnagchk.exe
pavshld.dll	User	C: NetworkAgent\PAVSHLD.dll
rasadhlp.dll	System	C:\Windows\SysWOW64\rasadhlp.dll
dnsapi.dll	System	C:\Windows\SysWOW64\dnsapi.dll
mswsock.dll	System	C:\Windows\SysWOW64\mswsock.dll
iphlpapi.dll	System	C:\Windows\SysWOW64\IPHLPAPI.DLL
cryptbase.dll	System	C:\Windows\SysWOW64\cryptbase.dll

klrbtagt.exe	User	C: NetworkAgent\klrbtagt.exe
version.dll	User	C: NetworkAgent\version.dll
dhcpcsvc.dll	System	C:\Windows\SysWOW64\dhcpcsvc.dll
msvcrt.dll	System	C:\Windows\SysWOW64\msvcrt.dll
rpcrt4.dll	System	C:\Windows\SysWOW64\rpcrt4.dll
shlwapi.dll	System	C:\Windows\SysWOW64\shlwapi.dll
msvcp_win.dll	System	C:\Windows\SysWOW64\msvcp_win.dll
kernelbase.dll	System	C:\Windows\SysWOW64\KernelBase.dll
gdi32.dll	System	C:\Windows\SysWOW64\gdi32.dll
win32u.dll	System	C:\Windows\SysWOW64\win32u.dll
imm32.dll	System	C:\Windows\SysWOW64\imm32.dll
sechost.dll	System	C:\Windows\SysWOW64\sechost.dll
user32.dll	System	C:\Windows\SysWOW64\user32.dll
kernel32.dll	System	C:\Windows\SysWOW64\kernel32.dll
advapi32.dll	System	C:\Windows\SysWOW64\advapi32.dll
ucrtbase.dll	System	C:\Windows\SysWOW64\ucrtbase.dll
gdi32full.dll	System	C:\Windows\SysWOW64\gdi32full.dll
ntdll.dll	System	C:\Windows\SysWOW64\ntdll.dll

viettel security

Process Injection detection guide (1)



viettel security

Process Injection detection guide (2)

Methods to detect Process Injection in Process Memory:

- Some featured Windows API usually used for process injection: (VirtualAllocEx, WriteProcessMemory, VirtualProtect, CreateRemoteThread, etc.).
- Memory area created by process injection techniques usually has these features: Type – Private, Protect – RWX/RX.
- Memory area contents usually are: Shellcode, PE file, PE file with deleted header.

Base address	Type	Size	Protect...	Use
0x1a0000	Image	36 kB	WCX	C:\W
0x250000	Mapped	32,768 kB	NA	
0x2250000	Mapped	64 kB	RW	Heap
0x2260000	Mapped	4 kB	R	
0x2270000	Mapped	4 kB	R	
0x2280000	Mapped	116 kB	R	
0x22a0000	Private	256 kB	RW	Stack
0x22e0000	Private	256 kB	RW	Stack
0x2320000	Mapped	16 kB	R	
0x2330000	Mapped	4 kB	R	
0x2340000	Private	8 kB	RW	
0x2350000	Private	476 kB	RWX	
0x23d0000	Mapped	4 kB	R	
0x23e0000	Private	56 kB	RW	
0x23f0000	Mapped	32 kB	R	
0x2400000	Private	2,048 kB	RW	PEB
0x2600000	Mapped	804 kB	R	C:\W
0x26d0000	Private	64 kB	RW	Heap

viettel security

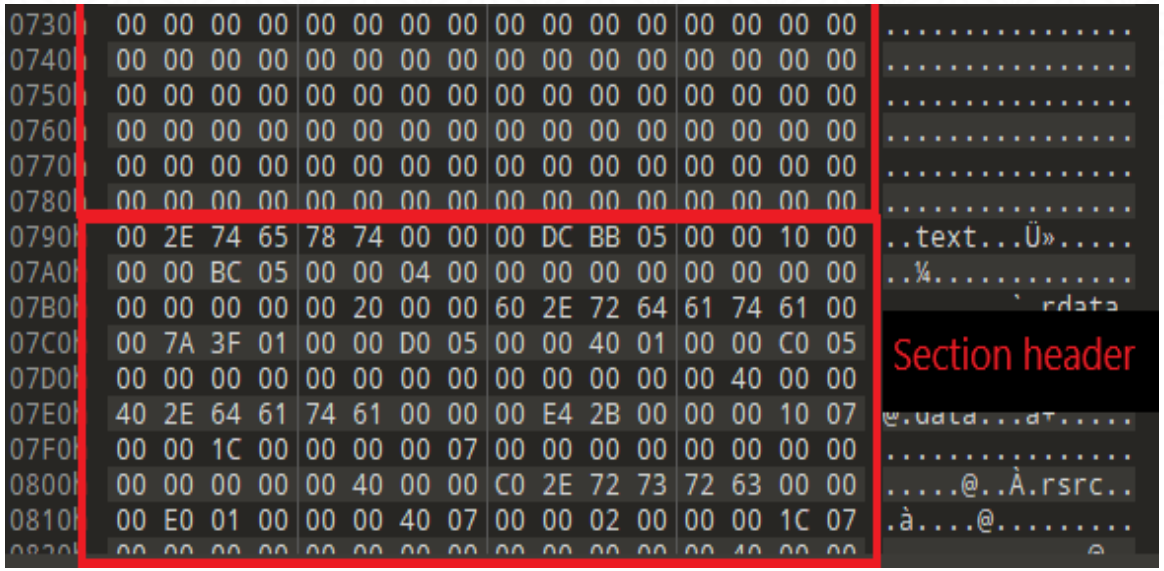
Process Injection detection guide (3)

Process Injection detection guide

- Use Hollows_hunter tool

(https://github.com/hasherezade/hollows_hunter)

- Tool help detect shellcode, pe file, pe file with deleted header in injected processes



viettel security

viettel security

#FIRSTCON24

THANK YOU!

Viettel Cyber Security Team