PlushDaemon compromises supply chain of Korean VPN service

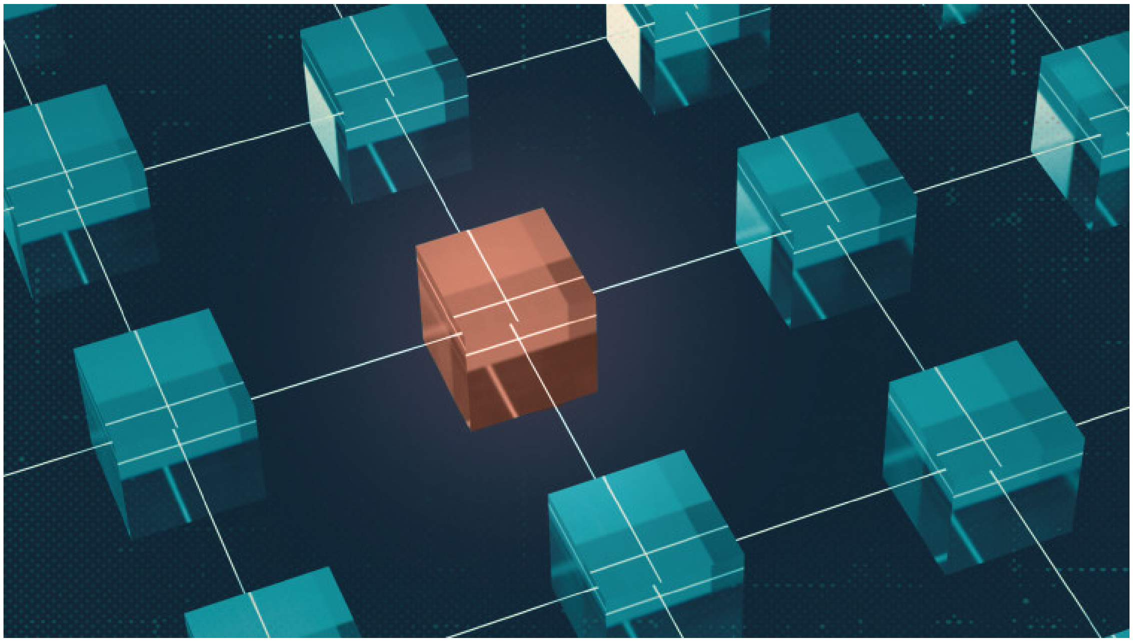
welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/

ESET Research

ESET researchers have discovered a supply-chain attack against a VPN provider in South Korea by a new China-aligned APT group we have named PlushDaemon

Facundo Muñoz

22 Jan 2025 , 20 min. read



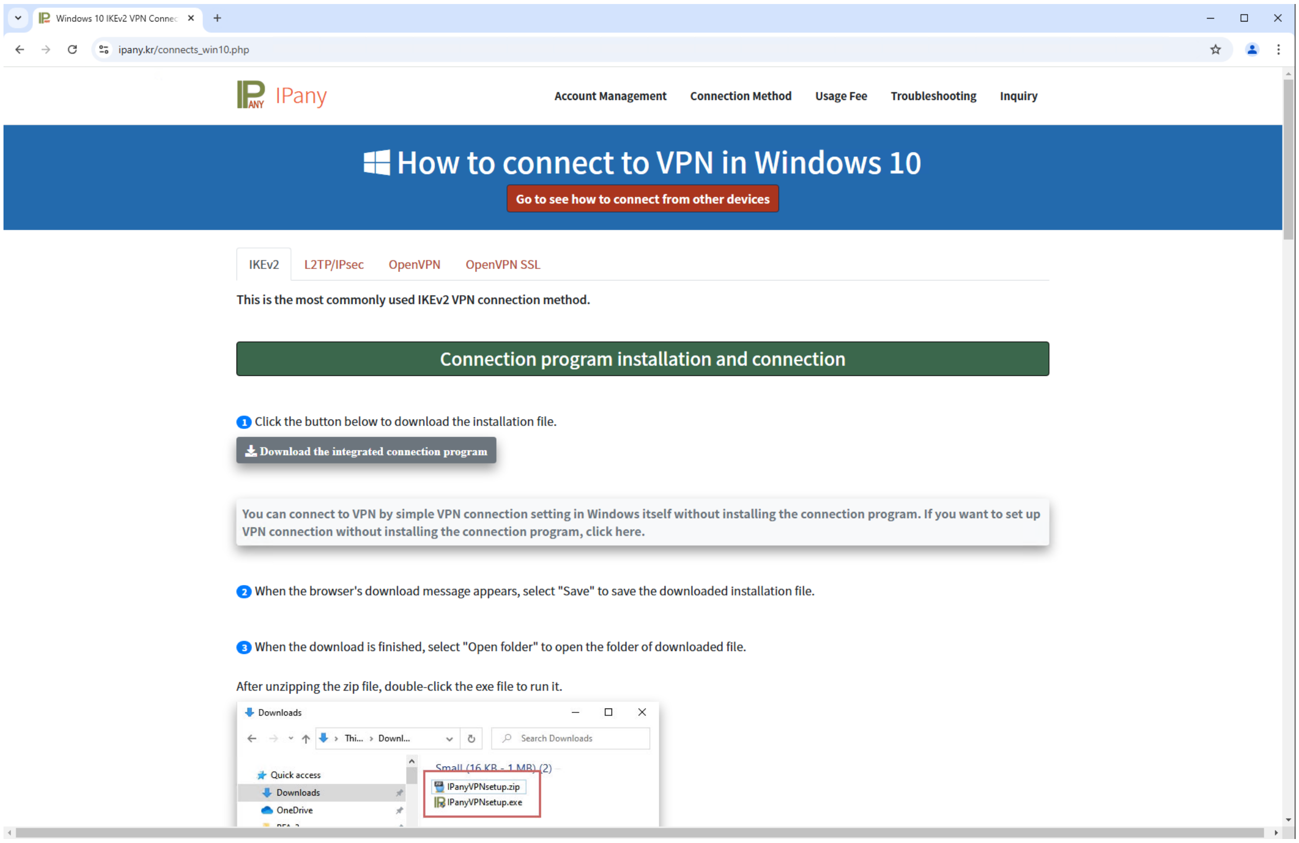
ESET researchers provide details on a previously undisclosed China-aligned APT group that we track as PlushDaemon and one of its cyberespionage operations: the supply-chain compromise in 2023 of VPN software developed by a South Korean company, where the attackers replaced the legitimate installer with one that also deployed the group's signature implant that we have named SlowStepper – a feature-rich backdoor with a toolkit of more than 30 components.

> **Key points of this blogpost:**
> - PlushDaemon is a China-aligned threat group, engaged in cyberespionage operations.
> - PlushDaemon's main initial access vector is hijacking legitimate updates of Chinese applications, but we have also uncovered a supply-chain attack against a South Korean VPN developer.
> - We believe PlushDaemon is the exclusive user of several implants, including SlowStepper for Windows.
> - SlowStepper has a large toolkit composed of around 30 modules, programmed in C++, Python, and Go.

Overview

In May 2024, we noticed detections of malicious code in an NSIS installer for Windows that users from South Korea had downloaded from the website of the legitimate VPN software IPany (https://ipany.kr/; see Figure 1), which is developed by a South Korean company. Upon further analysis, we discovered that the installer was deploying both the legitimate software and the backdoor that we've named SlowStepper. We contacted the VPN software developer to inform them of the compromise, and the malicious installer was removed from their website.

We attribute this operation to PlushDaemon – 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, and New Zealand. PlushDaemon uses a custom backdoor that we track as SlowStepper, and its main initial access technique is to hijack legitimate updates by redirecting traffic to attacker-controlled servers. Additionally, we have observed the group gaining access via vulnerabilities in legitimate web servers.



How to connect to VPN in Windows 10

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.

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.

Figure 1. Page at IPany website from which the malicious installer could be downloaded

The victims appear to have manually downloaded a ZIP archive containing a malicious NSIS installer from the URL https://ipany[.]kr/download/IPanyVPNsetup.zip. We found no suspicious code on the download page (shown in Figure 1) to produce targeted downloads, for example by geofencing to specific targeted regions or IP ranges; therefore, we believe that anyone using the IPany VPN might have been a valid target.

Via ESET telemetry, we found that several users attempted to install the trojanized software in the network of a semiconductor company and an unidentified software development company in South Korea. The two oldest cases registered in our telemetry were a victim from Japan in November 2023, and a victim from China in December 2023.

Technical analysis

As illustrated in Figure 2, when the malicious IPanyVPNsetup.exe installer is executed, it creates several directories and deploys both legitimate and malicious files.

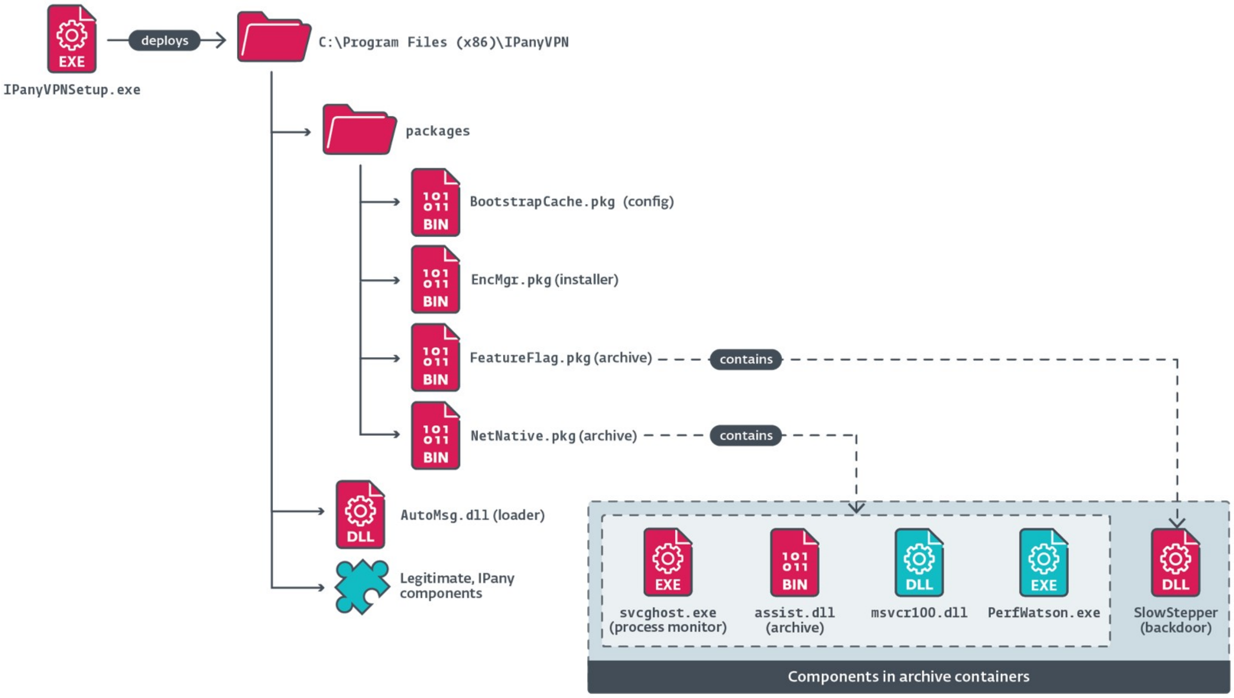


Figure 2. Deployment of both legitimate and malicious files

Additionally, the installer establishes persistence for SlowStepper by adding an entry named IPanyVPN to a Run key, with the value %PUBLIC%\Documents\WPSDocuments\WPSManager\svcghost.exe, so that the malicious component svcghost.exe (later extracted and deployed by the loader in EncMgr.pkg) is launched when the operating system starts.

The first malicious component that is loaded by the installer is the AutoMsg.dll loader. Figure 3 illustrates the major steps taken during the execution of this component.

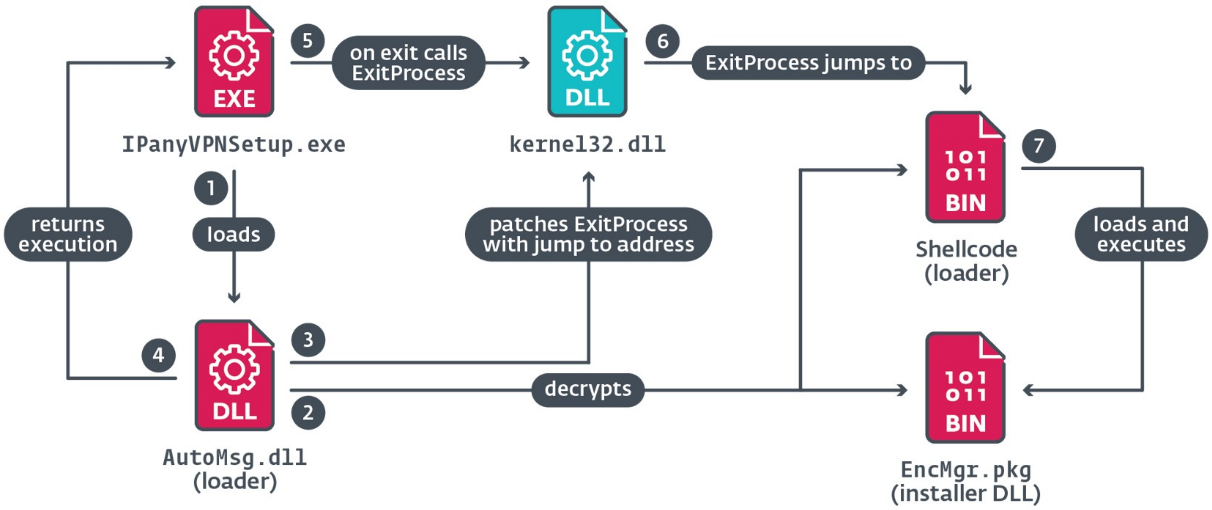


Figure 3. Loading chain initiated when IPanyVPNSetup.exe *loads* AutoMsg.dll

When IPanyVPNSetup.exe calls ExitProcess, the patched bytes redirect execution to the shellcode that loads EncMgr.pkg into memory and executes it.

EncMgr.pkg creates two directories – WPSDocuments and WPSManager – in %PUBLIC%\Documents and the deployment begins by extracting components from the custom archives NetNative.pkg and FeatureFlag.pkg. The components are dropped to disk and moved to other locations with new filenames. The sequence and actions taken are as follows:

1. Extracts the files from NetNative.pkg to:

a. %PUBLIC%\Documents\WPSDocuments\WPSManager\assist.dll,

b. %PUBLIC%\Documents\WPSDocuments\WPSManager\msvcr100.dll,

c. %PUBLIC%\Documents\WPSDocuments\WPSManager\PerfWatson.exe, and

d. %PUBLIC%\Documents\WPSDocuments\WPSManager\svcghost.exe.

2. Deletes NetNative.pkg.

3. Moves FeatureFlag.pkg to C:\ProgramData\Microsoft Shared\Filters\SystemInfo\winlogin.gif.

4. Moves assist.dll to C:\ProgramData\Microsoft Shared\Filters\SystemInfo\Winse.gif.

5. Extracts file from Winse.gif to %PUBLIC%\Documents\WPSDocuments\WPSManager\lregdll.dll.

6. Copies data from BootstrapCache.pkg to %PUBLIC%\Documents\WPSDocuments\WPSManager\Qmea.dat.

Its last actions are to execute svcghost.exe using the ShellExecute API and then exit.

The svcghost.exe component performs monitoring of the PerfWatson.exe process, where the backdoor is loaded, ensuring that it is always running. If the processes are not running, it executes PerfWatson.exe (originally a legitimate command line utility named regcap.exe, included in Visual Studio), which the attackers abuse to side-load lregdll.dll. The DLL’s goal is to load the SlowStepper backdoor from the winlogin.gif file.

On a new thread, it creates a nameless window that ignores all messages except WM_CLOSE, WM_QUERYENDSESSION, and WM_ENDSESSION. When any of these three messages is received, the thread attempts to establish persistence in the Windows registry, depending on the permissions of the current process; see Table 1.

Table 1. Registry keys targeted for persistence

Requires	Registry key	Entry	Value
Administrator	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Userinit	Current path of svcghost.exe.
User	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows	load	

The SlowStepper backdoor

SlowStepper is a backdoor developed in C++ with extensive use of object-oriented programming in the C&C communications code. Although the code contains hundreds of functions, the particular variant used in the supply-chain compromise of the IPany VPN software appears to be version 0.2.10 Lite, according to the backdoor’s code. The so-called “Lite” version indeed contains fewer features than other previous and newer versions.

The oldest version of the SlowStepper backdoor that we know of is 0.1.7, compiled on 2019-01-31 according to its PE timestamps; the newest one is 0.2.12, compiled on 2024-06-13, and is the full version of the backdoor.

Both the full and Lite versions make use of an array of tools programmed in Python and Go, which include capabilities for extensive collection of data, and spying through recording of audio and videos. The tools were stored in a remote code repository hosted on the Chinese platform GitCode, under the LetMeGo22 account; at the time of writing, the profile was private (Figure 4).

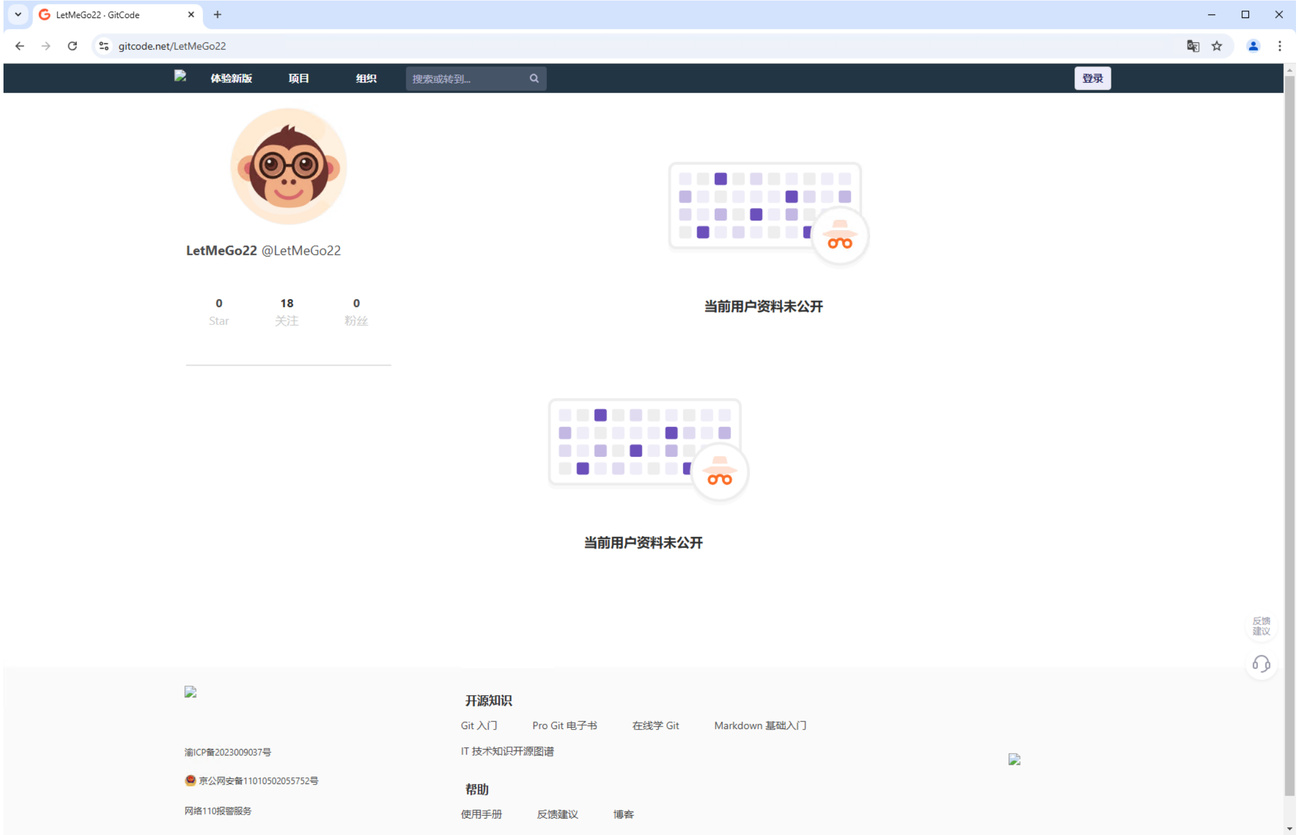


Figure 4. LetMeGo22 account at GitCode

C&C communications

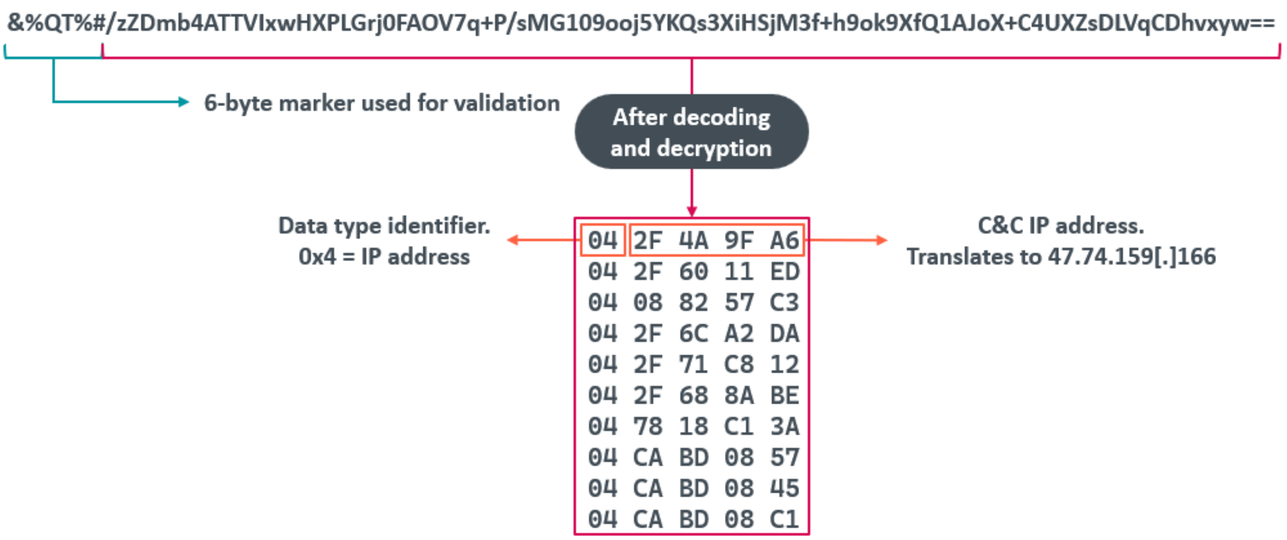
SlowStepper does not carry the C&C IP address in its configuration; instead, it crafts a DNS query to obtain a TXT record for the domain 7051.gsm.360safe[.]company. The query is sent to one of three legitimate, public DNS servers:

- 8.8.8.8 – Google Public DNS,
- 114.114.114.114 – 114dns.com, or
- 223.5.5.5 – Alibaba Public DNS.

We obtained four such records associated with that domain:

- &%QT%#/zZDmb4ATTVIxwHXPLGrj0FAOV7q+P/sMG109ooj5YLnVZBs3R/eZcuQximtgLkf
- &%QT%#/zZDmb4ATTVIxwHXPLGrj0FAOV7q+P/sMG109ooj5YKQs3XiHSjM3f+h9ok9XfQ1AjoX+C4UXZsDLVqCDhvxyw==
- &%QT%#aT1sAjOFTcwzQ7hwc0iyfygP/ooo8pkIRyaNKWcqBz+QRGYBV/2v8HrVg28+aZXhfXvgDxS1vXAuhdcN2dEKxw==
- &%QT%#aT1sAjOFTcwzQ7hwc0iyfySJBEDM0z6na7BiogG0hDJqdKlUqkrb9ppOjg8epeQ6I6cUXWLKyZGZCkJwFyKD4Q==

The format of the data in the query is shown in Figure 5. The code checks whether the first six bytes of the TXT record match &%QT%# and if so, it extracts the rest of the string, which is a base64-encoded AES-encrypted blob containing an array of 10 IP addresses to be used as C&C servers. The key used for decryption is sQi9&*2Uhy3Fg7se and the IV is Qhsy&7y@bsG9st#g.



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

```
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
```

6-byte marker used for validation
After decoding and decryption
Data type identifier. 0x4 = IP address
C&C IP address. Translates to 47.74.159[.]166

Figure 5. DNS TXT record obtained of malicious domains

When parsing the decrypted data, the code can extract at least four data identifiers, described in Table 2.

Table 2. Data types processed by the backdoor's code

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.

One of the IP addresses is chosen and SlowStepper connects to the C&C server via TCP to begin its communication protocol. If, after a number of attempts, it fails to establish a connection to the server, it uses the gethostbyname API on the domain st.360safe[.]company to obtain the IP address mapped to that domain and uses the obtained IP as its fallback C&C server.

Once communication is established, SlowStepper can process the commands listed in Table 3.

Table 3. Basic commands supported by SlowStepper

Command ID	Action performed

Command ID	Action performed
0x32	Collects the following information from the compromised machine and sends it to the server: · brand of the CPU, using the CPUID instruction, · HDDs connected to the computer and their serial numbers, · computer name, · local host name, · public IP address, by querying multiple services, · list of running processes, · list of installed applications, · network interface information, · additional information about the computer's drives, such as volume name and free space, · system memory, · current username, · persistence type used, · whether cameras are connected, · whether microphones are connected, · whether the operating system is running as a virtual machine, · system uptime, · HTTP proxy configuration, and · whether queries to the DNS server at 114.114.114.114:53 to resolve the addresses of two legitimate domains, cf.duba.net (Kingston) and f.360.cn (360 Qihoo), failed or succeeded. It is unclear to us what the purpose of this information is.
0x38	Executes a Python module from its toolkit; the output and any files created by the module are sent to the server. The procedure is very similar to what is used in the shell mode.
0x39	Deletes the specified file.
0x3A	This command can process other commands sent by the operator in SlowStepper's shell mode, which we explain in more detail below. Alternatively, it can also: · Run a command via cmd.exe and send the output back to the server. · Run a command via cmd.exe without sending the output to the server.
0x3C	Uninstalls SlowStepper by removing its persistence mechanism and removing its files.
0x3F	Lists files in the specified directory, and lists drives.
0x5A	Downloads and executes the specified file.

SlowStepper has a rather unusual feature: the developers implemented a custom shell, or command line interface, on top of its communication protocol. While the backdoor accepts and handles commands in the traditional way, the 0x3A command activates the interpretation of operator-written commands (Table 4).

Table 4. Commands supported in shell mode

Command	Parameters	Description
cd	Path to a directory.	Checks whether a directory exists.
gcall	Module name and other unknown parameter(s).	This function can perform two tasks: · Download a module from the remote code repository and execute it. The module is supposed to be a console application. · Send a file from the compromised machine to the operator.
pycall	Tool name to be executed.	This command is explained in detail in the ***Execution of tools via SlowStepper's pycall shell command*** section.
restart	self	Restarts SlowStepper by rerunning the host process and calling the ExitProcess API. Returns the message The mode of NSP doesn't support restart self. when SlowStepper is running in a process via a persistence technique that abuses Winsock namespace providers; however, it is not included in this variant of SlowStepper.
update	N/A	Downloads a module from the remote code repository, replacing a previous existing version.

Command	Parameters	Description
gconfig	show	Displays the value of ServerIP (the C&C IP address).
	set	Changes the value of ServerIP. The console suggests the following to the operator: If you want make the Configuration effective immediately, please command “gconfig reload”.
	reload	Reloads the configuration.
	getname	Returns the name of the current process in which SlowStepper is running.
	getdll	Returns the name of the SlowStepper DLL in the current process.
	getpid	Returns the process ID of the current process in which SlowStepper is running.
	getsid	Returns the Remote Desktop Services session ID of the current process. This suggests that SlowStepper might also be intended to compromise machines running Windows Server.
	getpwd	Downloads getcode.mod from the remote code repository and executes it using rundll32.exe. The module generates a file, named psf.bin, that contains the collected data.
gcmd	query	Creates a complete report of information about the specified file or directory.
	delete	Deletes the specified file, directory, or all files in a directory.
	set	Sets configuration parameters.
	terminate	Terminates the specified process.
	cancel	Creates a file with the .delete extension.

Execution of tools via SlowStepper’s pycall shell command

Figure 6 illustrates the execution chain, starting when the operator issues a pycall command to request the execution of a Python module on the compromised machine; here, as an example, the module CollectInfo.

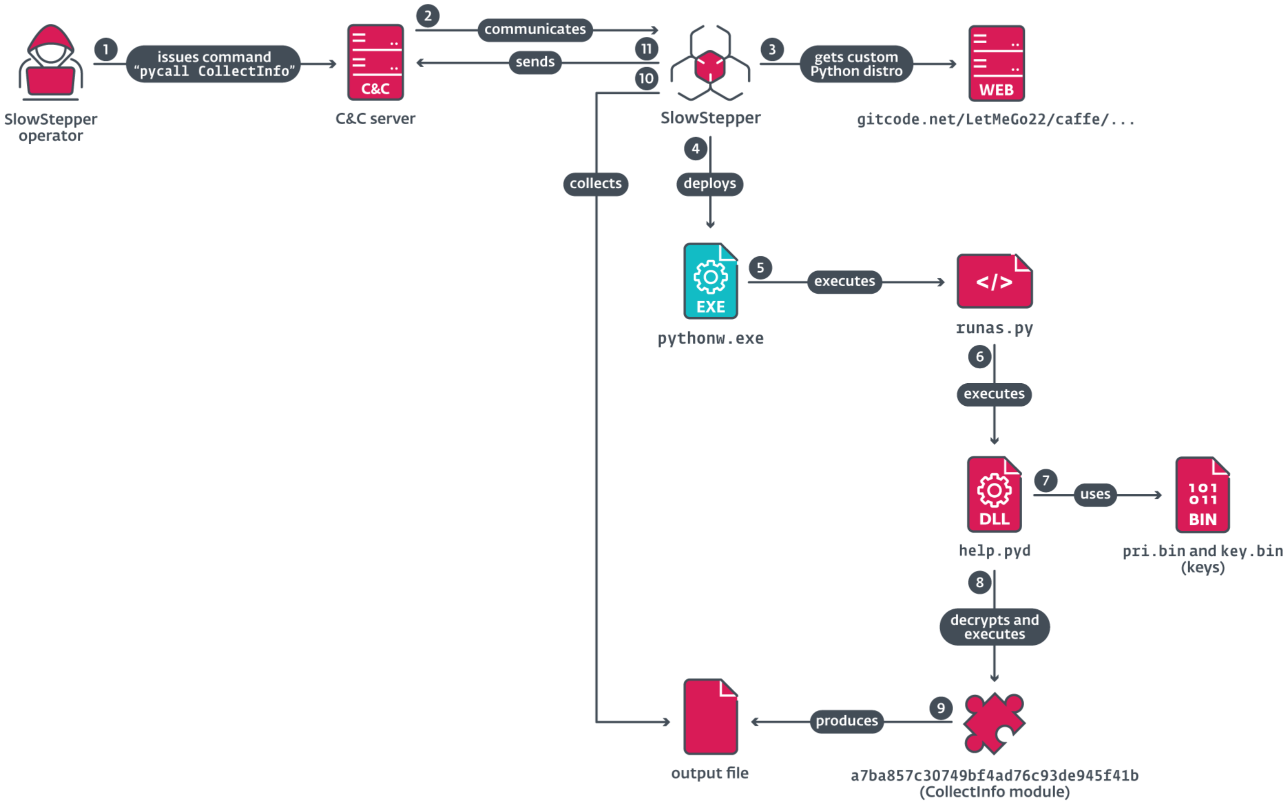


Figure 6. Execution flow of the pycall *command*

From the remote repository, the pycall command downloads a ZIP archive that contains the Python interpreter and its supporting libraries. One of three possible customized distributions is downloaded, as outlined in Table 5.

Table 5. List of customized Python distributions and the conditions under which they are downloaded

Condition	**Archive name**	**Description**
Windows operating system is XP.	winxppy.org	Python 3.4
All required Windows API set (stub) DLLs and the Microsoft C runtime are present.	winpy_no_rundll.org	Python 3.7
Neither of the preceding conditions are met.	win7py.org	Python 3.7; includes Windows API set (stub) DLLs and the Microsoft C runtime library.

Figure 7 shows the directory structure of the decompressed archive containing the Python distribution, listing only the malicious files that are included within.

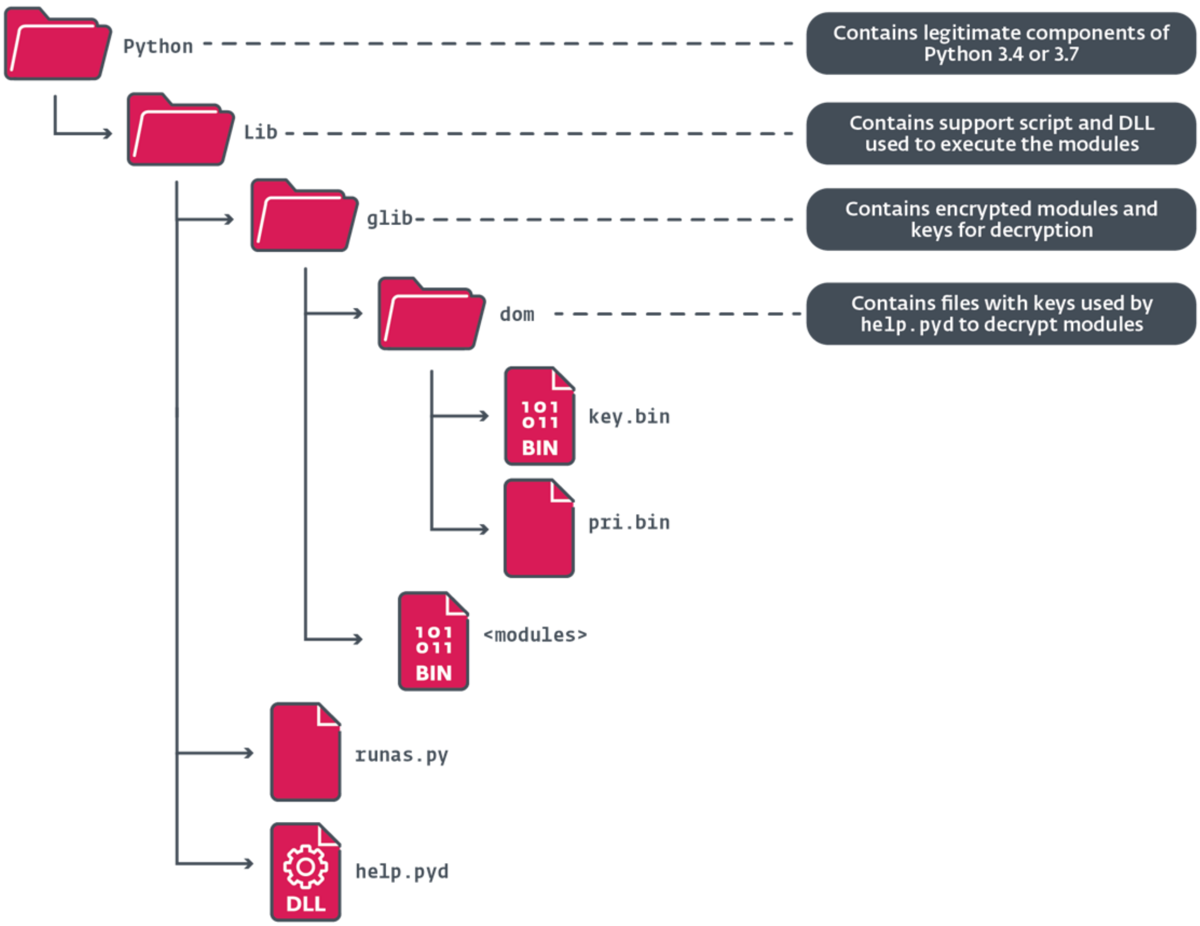
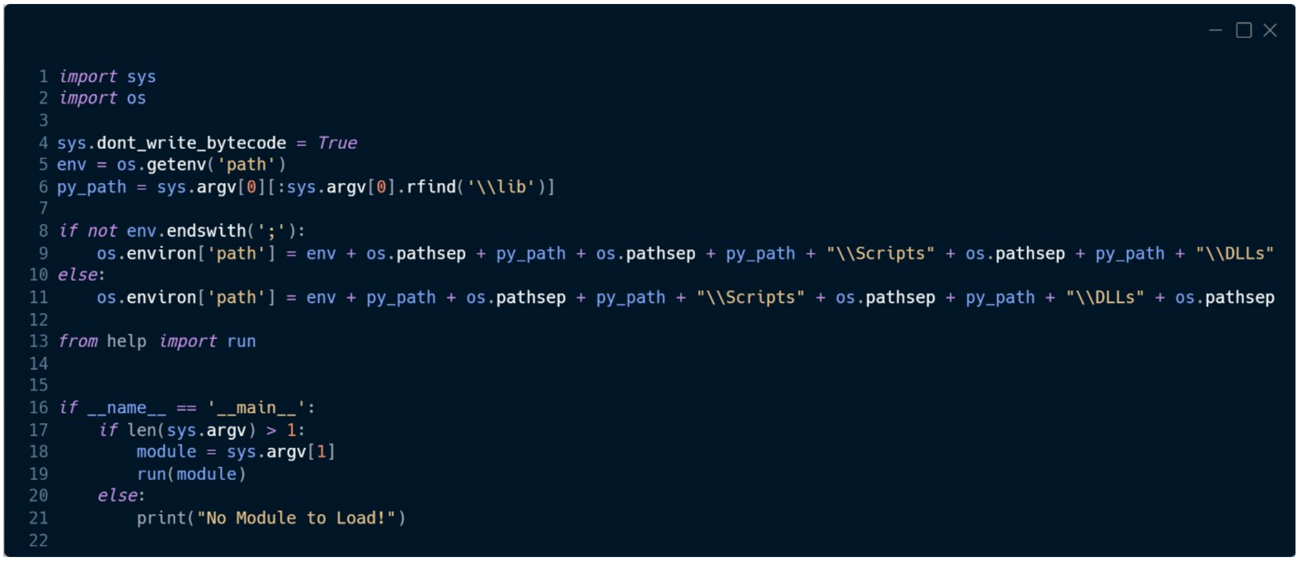

Python
Contains legitimate components of Python 3.4 or 3.7
Lib
Contains support script and DLL used to execute the modules
glib
Contains encrypted modules and keys for decryption
dom
Contains files with keys used by help.pyd to decrypt modules
101 011 BIN
key.bin
pri.bin
101 011 BIN
<modules>
runas.py
DLL
help.pyd

Figure 7. Directory structure of the customized Python distribution and malicious files

SlowStepper runs the Python interpreter using the following command line:

%PUBLIC%\Documents\WPSDocuments\WPSManager\Python\Pythonw.exe -m runas <module_name>

The module named runas is a custom Python script (Figure 8) that loads another custom Python module named help from which it uses the function named run to decrypt the module and execute it.



```
import sys
import os

sys.dont_write_bytecode = True
env = os.getenv('path')
py_path = sys.argv[0][:sys.argv[0].rfind('\\lib')]

if not env.endswith(';'):
    os.environ['path'] = env + os.pathsep + py_path + os.pathsep + py_path + "\\Scripts" + os.pathsep + py_path + "\\DLLs"
else:
    os.environ['path'] = env + py_path + os.pathsep + py_path + "\\Scripts" + os.pathsep + py_path + "\\DLLs" + os.pathsep

from help import run


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

```

Figure 8. Code of runas.py

Table 6 lists the modules that we recovered from the remote repository during the time it was available.

Table 6. List of Python modules and their purpose

Filename on disk	Original module name	Purpose
900150983cd24fb0d6963f7d28e17f72	abc	Test module that prints hello world.
ef15fd2f45e6bb5ce57587895ba64f93	Browser	Collects a wide range of data from web browsers: Google Chrome, Microsoft Edge, Opera, Brave, Vivaldi, Cốc Cốc browser, UC Browser, 360 Browser, and Mozilla Firefox.
967d35e40f3f95b1f538bd248640bf3b	Camera	If the computer has a camera connected, it takes photos.
a7ba857c30749bf4ad76c93de945f41b	CollectInfo	Scans the disk for files with extensions .txt, .doc, .docx, .xls, .xlsx, .ppt, and .pptx. Collects information from several software titles, including: LetsVPN, Tencent QQ, WeChat, Kingsoft WPS, e2eSoft VCam, KuGou, Oray Sunlogin, and ToDesk.
6002396e8a3e3aa796237f6469eb84f8	Decode	Downloads a module from the remote repository and decrypts it.
9348a97af6e8a2f482d5dbee402c8c6f	DingTalk	Collects a wide range of data from DingTalk (a corporate management tool developed in China), including chat messages, audio, video, contact information, and groups the user has joined.
801ab24683a4a8c433c6eb40c48bcd9d	Download	Downloads (non-malicious) Python packages.
16654b501ac48e4675c9eb0cf2b018f6	FileScanner	Scans the disk for files, using the same code as CollectInfo.
7d3b40764db47a45e9bc3f1169a47fe2	FileScannerAllDisk	
3582f6ebaf9b612940011f98b110b315	getOperaCookie	Gets cookies from the Opera browser.
10ae9fc7d453b0dd525d0edf2ede7961	list	Lists modules with a .py extension.
ce5bf551379459c1c61d2a204061c455	Location	Obtains the IP address of the computer and the GPS coordinates, using online services.
68e36962b09c99d6675d6267e81909ad	Location1	
5e0a529f8acc19b42e45d97423df2eb4	LocationByIP	
c84fcb037b480bd25ff9aaaebce5367e	PackDir	Creates a ZIP archive of the specified file.
4518dc0ae0ff517b428cda94280019fa	qpass	This script appears to be unfinished. It obtains and decrypts passwords from Tencent QQ Browser. Probably replaced by the qqpass module.
5fbf04644f45bb2be1afffe43f5fbb57	qqpass	Obtains and decrypts passwords from Google Chrome, Mozilla Firefox, Tencent QQ Browser, 360 Chrome, and UC Browser.
874f5aaef6ec4af83c250ccc212d33dd	ScreenRecord	Records the screen, saving the result as an AVI file inside a ZIP archive.
c915683f3ec888b8edcc7b06bd1428ec	Telegram	Collects account information from the Telegram desktop application.
104be797a980bcbd1fa97eeacfd7f161	Webpass	Similar to the qqpass module.

Filename on disk	Original module name	Purpose
e5b152ed6b4609e94678665e9a972cbc	WeChat	One of the largest modules, it collects a wide range of data from WeChat.
6d07a4ebf4dff8e5d4fdb61f1844cc12	Wechat_all_file	Collects data from WeChat.
17cf4a6dd339a1312959fd344fe92308	Wechat_src	
8326cef49f458c94817a853674422379	Wechat1	Similar to WeChat.
427f01be70f46f02ef0d18fcbbfaf01d	WechatFile	
72704d83b916fa1f7004e0fdef4b77ae	WirelessKey	Collects wireless network information and passwords, and output from the ipconfig /all command.

In addition to the Python toolkit, we found, stored in the remote code repository other tools (Table 7) that are not encrypted; some of these were programmed in C/C++ and others in Go, as noted below.

Table 7. Tools and their function

Tool filename	Description
agent.mod	Reverse proxy programmed in Go.
getcode.mod getcode64.mod	Mimikatz. This tool is a DLL downloaded by the getpwd command.
InitPython.mod	Old downloader to install the customized Python distribution on the compromised machine. This tool is a DLL.
Remote.mod	RealVNC server that allows the attackers to remotely control the compromised machine. This tool is a DLL.
soc.mod	Reverse proxy programmed in Go. Signed with a certificate from a Chinese company called Hangzhou Fuyang Qisheng Information Technology Service Department. We were unable to find any information about the company.
stoll.mod	Tool used to perform downloads, written in Go. Signed with a certificate from the Chinese company Zhoushan Xiaowen Software Development Studio. We were unable to find any information about the company.

Conclusion

In this blogpost, we have analyzed a supply-chain attack against a Korean VPN provider, targeting users in East Asia, as evident through the specific software targeted for information collection and confirmed via ESET telemetry. We also documented the SlowStepper backdoor, used exclusively by PlushDaemon. This backdoor is notable for its multistage C&C protocol using DNS, and its ability to download and execute dozens of additional Python modules with espionage capabilities.

The numerous components in the PlushDaemon toolset, and its rich version history, show that, while previously unknown, this China-aligned APT group has been operating diligently to develop a wide array of tools, making it a significant threat to watch for.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

A comprehensive list of indicators of compromise and samples can be found in our GitHub repository.

Files

SHA-1	Filename	Detection	Description
A8AE42884A8EDFA17E9D67AE5BEBE7D196C3A7BF	AutoMsg.dll	Win32/ShellcodeRunner.GZ	Initial loader DLL.
2DB60F0ADEF14F4AB3573F8309E6FB135F67ED7D	lregdll.dll	Win32/Agent.AGUU	Loader DLL for the SlowStepper backdoor.
846C025F696DA1F6808B9101757C005109F3CF3D	OldLJM.dll	Win32/Agent.AGXL	Installer DLL, internally named OldLJM.dll. It is extracted from EncMgr.pkg and executed in memory.
AD4F0428FC9290791D550EEDDF171AFF046C4C2C	svcghost.exe	Win32/Agent.AGUU	Process monitor component that launches PerfWatson.exe or RuntimeSvc.exe to side-load lregdll.dll.
401571851A7CF71783A4CB902DB81084F0A97F85	main.dll	Win32/Agent.AEIJ	Decrypted SlowStepper backdoor component.
068FD2D209C0BBB0C6FC14E88D63F92441163233	IPanyVPNsetup.exe	Win32/ShellcodeRunner.GZ	Malicious IPany installer. Contains the SlowStepper implant and the legitimate IPany VPN software.

Network

IP	Domain	Hosting provider	First seen	Details
202.189.8[.]72	reverse.wcsset[.]com	Shandong eshinton Network Technology Co., Ltd.	2024-10-14	Server used by the (reverse proxy) soc.mod tool.
47.96.17[.]237	agt.wcsset[.]com	Hangzhou Alibaba Advertising Co.,Ltd.	2024-10-14	Server used by agent.mod tool.
N/A	7051.gsm.360safe[.]company	N/A	2020-09-29	SlowStepper queries this domain to obtain its associated DNS TXT record.
202.105.1[.]187	st.360safe[.]company	IRT-CHINANET-CN	2021-03-11	Fallback C&C server contacted by SlowStepper.
47.74.159[.]166	N/A	Alibaba (US) Technology Co., Ltd.	2020-09-29	SlowStepper C&C server.
8.130.87[.]195	N/A	Hangzhou Alibaba Advertising Co.,Ltd.	2020-09-29	SlowStepper C&C server.
47.108.162[.]218	N/A	Hangzhou Alibaba Advertising Co.,Ltd.	2020-09-29	SlowStepper C&C server.
47.113.200[.]18	N/A	Hangzhou Alibaba Advertising Co.,Ltd.	2020-09-29	SlowStepper C&C server.
47.104.138[.]190	N/A	Guowei Pan	2020-09-29	SlowStepper C&C server.
120.24.193[.]58	N/A	Hangzhou Alibaba Advertising Co.,Ltd.	2020-09-29	SlowStepper C&C server.
202.189.8[.]87	N/A	Shandong eshinton Network Technology Co., Ltd.	2020-09-29	SlowStepper C&C server.
202.189.8[.]69	N/A	Shandong eshinton Network Technology Co., Ltd.	2020-09-29	SlowStepper C&C server.

IP	Domain	Hosting provider	First seen	Details
202.189.8[.]193	N/A	Shandong eshinton Network Technology Co., Ltd.	2020-09-29	SlowStepper C&C server.
47.92.6[.]64	N/A	Hangzhou Alibaba Advertising Co.,Ltd.	2020-09-29	SlowStepper C&C server.

MITRE ATT&CK techniques

This table was built using version 16 of the MITRE ATT&CK framework**.**

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	PlushDaemon has acquired domain names for its C&C infrastructure.
	T1583.004	Acquire Infrastructure: Server	PlushDaemon has acquired servers to be used as C&C servers.
	T1608.001	Stage Capabilities: Upload Malware	PlushDaemon has staged its toolkit in the code repository website GitCode.
	T1608.002	Stage Capabilities: Upload Tool	PlushDaemon has staged its toolkit in the code repository website GitCode.
	T1588.001	Obtain Capabilities: Malware	PlushDaemon has access to SlowStepper.
	T1588.002	Obtain Capabilities: Tool	PlushDaemon tools getcode.mod and getcode64.mod use Mimikatz.
	T1588.003	Obtain Capabilities: Code Signing Certificates	PlushDaemon tools soc.mod and stoll.mod are signed.
	T1588.005	Obtain Capabilities: Exploits	PlushDaemon has used an unidentified exploit for Apache HTTP server.
Initial Access	T1659	Content Injection	PlushDaemon can intercept network traffic to hijack update protocols and deliver its SlowStepper implant.
	T1190	Exploit Public-Facing Application	PlushDaemon exploited an unidentified vulnerability in Apache HTTP Server.
	T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	PlushDaemon has compromised the supply chain of a VPN developer and replaced the original installer with a trojanized one containing the SlowStepper implant.
Execution	T1059.003	Command-Line Interface: Windows Command Shell	SlowStepper uses cmd.exe to execute commands on a compromised machine.
	T1059.006	Command-Line Interface: Python	SlowStepper for Windows can use the Python console to execute the Python components of its toolkit.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	The SlowStepper installer establishes persistence by adding an entry in HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

Tactic	ID	Name	Description
	T1547.004	Boot or Logon Autostart Execution: Winlogon Helper DLL	The SlowStepper process monitor component can establish persistence by adding an entry in HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit or HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\load.
	T1574.002	Hijack Execution Flow: DLL Side-Loading	PlushDaemon has abused a legitimate command line utility included in Visual Studio called regcap.exe to side-load a malicious DLL named lregdll.dll.
Defense Evasion	T1222.001	File Permissions Modification: Windows File and Directory Permissions Modification	SlowStepper modifies the access rights of the directory where its components are stored on disk.
	T1070.004	Indicator Removal: File Deletion	SlowStepper can remove its own files.
	T1036.005	Masquerading: Match Legitimate Name or Location	SlowStepper uses folder names and filenames from legitimate software.
	T1112	Modify Registry	SlowStepper can modify the registry.
	T1027.007	Obfuscated Files or Information: Dynamic API Resolution	SlowStepper dynamically resolves Windows API functions.
	T1027.009	Obfuscated Files or Information: Embedded Payloads	SlowStepper loader DLLs contain embedded, position-independent code, executed in memory, to load components.
	T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	SlowStepper components are stored encrypted on disk.
	T1553.002	Subvert Trust Controls: Code Signing	PlushDaemon tools soc.mod and stoll.mod are signed.
Discovery	T1217	Browser Bookmark Discovery	SlowStepper’s Browser tool collects information from browsers.
	T1083	File and Directory Discovery	SlowStepper and its tools can search for files with specific extensions, or enumerate files in directories.
	T1120	Peripheral Device Discovery	SlowStepper and its toolkit can discover devices connected to the compromised machine.
	T1057	Process Discovery	SlowStepper can create a list of running processes.
	T1012	Query Registry	SlowStepper can query the registry.
	T1518	Software Discovery	SlowStepper can create a list of software installed on the compromised machine.
	T1082	System Information Discovery	SlowStepper can collect system information.
	T1614	System Location Discovery	SlowStepper’s Location tool attempts to discover the possible geolocation of the compromised machine by querying several online services.

Tactic	ID	Name	Description
	T1016	System Network Configuration Discovery	SlowStepper collects information from the network adapters.
	T1016.002	System Network Configuration Discovery: Wi-Fi Discovery	SlowStepper’s Wireless tool and its variants collects a wide range of information from the Wi-Fi network.
	T1033	System Owner/User Discovery	SlowStepper obtains the username.
Collection	T1560.002	Archive Collected Data: Archive via Library	SlowStepper tools can compress the collected data in ZIP archives.
	T1123	Audio Capture	SlowStepper can capture audio if the compromised machine has a microphone.
	T1005	Data from Local System	SlowStepper and its tools collect a wide range of data from the compromised system.
	T1074.001	Data Staged: Local Data Staging	SlowStepper and its tools stage data locally before exfiltrating it to the C&C server.
	T1113	Screen Capture	SlowStepper’s ScreenRecord tool can take screenshots.
	T1125	Video Capture	SlowStepper’s Camera tool can record videos if the compromised machine has a camera.
Command and Control	T1071.004	Standard Application Layer Protocol: DNS	SlowStepper retrieves a DNS TXT record that contains an AES-encrypted list of C&C servers.
	T1132.001	Data Encoding: Standard Encoding	SlowStepper retrieves a DNS TXT record that contains an AES-encrypted list of C&C servers. The record is base64 encoded.
	T1573.001	Encrypted Channel: Symmetric Cryptography	SlowStepper’s communication protocol with its C&C is encrypted with AES.
	T1008	Fallback Channels	SlowStepper gets a fallback C&C server IP address by resolving an alternative domain controlled by the attackers.
	T1105	Remote File Copy	SlowStepper downloads additional tools from a remote code repository at GitCode.
	T1104	Multi-Stage Channels	SlowStepper obtains a list of C&C servers by querying the DNS TXT record from a domain controlled by the attackers; if no communication can be established with the servers, it resolves the IP address of another domain controlled by the attackers to obtain a backup server. SlowStepper tools use different servers from PlushDaemon infrastructure.
	T1095	Standard Non-Application Layer Protocol	SlowStepper communicates with its C&C via TCP.
	T1090	Connection Proxy	SlowStepper tools agent.mod and soc.mod are reverse proxies.
	T1219	Remote Access Tools	SlowStepper tool Remote.mod allows its operator to remotely control the compromised machine via VNC.
Exfiltration	T1020	Automated Exfiltration	SlowStepper can exfiltrate staged data.
	T1041	Exfiltration Over C2 Channel	SlowStepper exfiltrates collected data when connected to one of its C&C servers.

eset
THREAT
INTELLIGENCE
FIND OUT MORE