PlushDaemon compromises network devices for adversary-in-the-middle attacks

By Facundo MuñozDávid Gábriš

Archived: 2026-04-05 18:35:01 UTC

ESET researchers provide insights into how PlushDaemon performs adversary-in-the-middle attacks using a previously undocumented network implant that we have named EdgeStepper, which redirects all DNS queries to an external, malicious hijacking node, effectively rerouting the traffic from legitimate infrastructure used for software updates to attacker-controlled infrastructure.

> **Key points in this blogpost:**
>
> - We analyzed the network implant EdgeStepper to understand how PlushDaemon attackers compromise their targets.
> - We provide an analysis of LittleDaemon and DaemonicLogistics, two downloaders that deploy the group's signature SlowStepper backdoor on Windows machines.

PlushDaemon profile

PlushDaemon is a China-aligned threat actor active since at least 2018 that engages in espionage operations against individuals and entities in China, Taiwan, Hong Kong, Cambodia, 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 through a network implant that we call EdgeStepper. Additionally, we have observed the group gaining access via vulnerabilities in web servers, and in 2023 it performed a supply-chain attack.

Overview

In 2024, while researching PlushDaemon's clusters of activity (including the supply-chain compromise of a South Korean VPN service), we noticed that an ELF file submitted to VirusTotal contained two subdomains from PlushDaemon's infrastructure. That file, called bioset, was previously hosted on a server likely compromised by multiple threat actors. Note that on the same day of the submission to VirusTotal, a researcher (@James_inthe_box) tweeted about an open directory on the server where bioset was hosted, so the sample was probably uploaded to VirusTotal by a researcher who was investigating the contents of the directory.

Internally named dns_cheat_v2 by its developers – and codenamed EdgeStepper by us – bioset is PlushDaemon's adversary-in-the-middle tool, which forwards DNS traffic from machines in a targeted network to a malicious DNS node. This allows the attackers to redirect the traffic from software updates to a hijacking node that serves instructions to the legitimate software to download a malicious update.

Victimology

Figure 1 presents the geographical distribution of victims of PlushDaemon that have been compromised through malicious updates, since 2019, according to ESET telemetry.

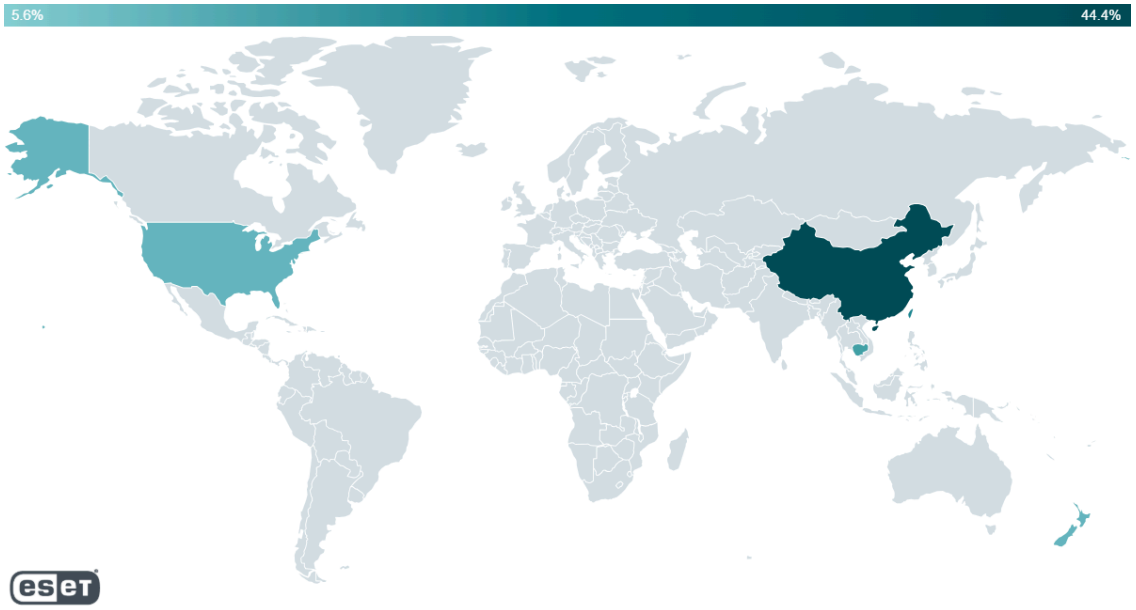

Figure 1. Geographical distribution of victims

PlushDaemon has compromised individuals and organizations located in the following regions:

- United States (2019)
- Taiwan (2021, 2024)
- China (2021–2024), including a university in Beijing and a Taiwanese company that manufactures electronics
- Hong Kong (2023)
- New Zealand (2023)
- Cambodia (2025), including a company in the automotive sector and a branch of a Japanese company in the manufacturing sector

Adversary-in-the-middle attack overview

First, PlushDaemon compromises a network device (for example, a router) to which their target might connect; the compromise is probably achieved by exploiting a vulnerability in the software running on the device or through weak and/or well-known default administrative credentials, enabling the attackers to deploy EdgeStepper (and possibly other tools).

EdgeStepper begins redirecting DNS queries to a malicious DNS node that verifies whether the domain (for example, info.pinyin.sogou.com from Sogou Pinyin) in the DNS query message is related to software updates, and if so, it replies with the IP address of the hijacking node. Alternatively, we have also observed that some servers are both the DNS node and the hijacking node; in those cases, the DNS node replies to DNS queries with its own IP address.

Note that since we have closely studied updates for Sogou Pinyin software being hijacked, we will continue to use that as an example from here on out. Many other popular Chinese software titles also have their updates hijacked

in similar ways by PlushDaemon via EdgeStepper.

Figure 2 illustrates the first stages of the deployment of PlushDaemon's capabilities.

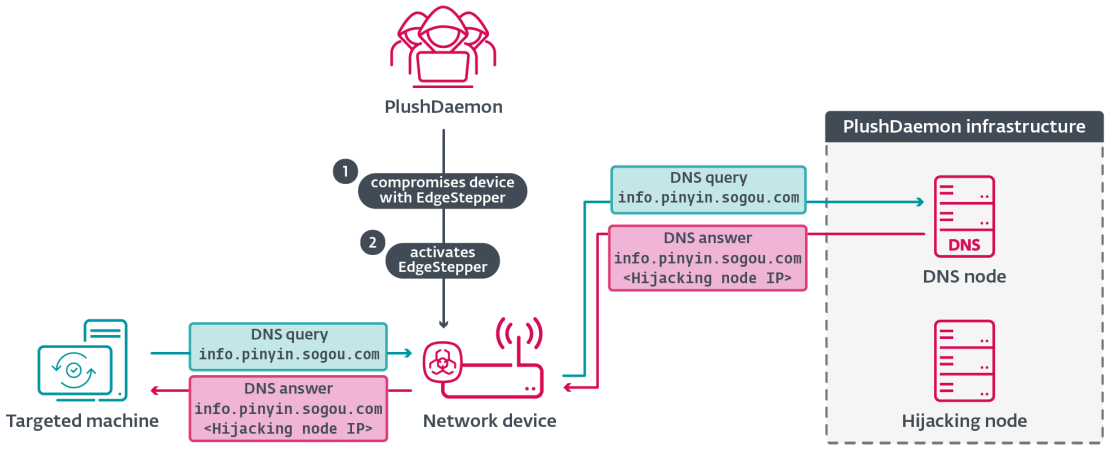

Figure 2. Illustration of the first stages of the attack

The updating software communicates via HTTP with the hijacking node instead of Sogou's legitimate infrastructure; the hijacking node replies with instructions to, for example, download a DLL file from http://ime.sogou.com/popup_4.2.0.2246.dll, as shown in Figure 3.

```
GET /version.txt?h=CA1B4767D0F6711581EF509EC7BCE5A6&v=9.3.0.2927&r=0000_sogou_pinyin_93c&ppversion=3.1.0.2113&lt=2019-9-26.17%3A57%3A8&uex=0 HTTP/1.1
Host: info.pinyin.sogou.com
Accept: */*
User-Agent: SogouIMEMiniSetup_imepopup


HTTP/1.1 200 OK
Content-Length: 133
Connection: close
Content-Type: text/plain; charset=utf-8
Pragma: no-cache
Server: nginx
X-Powered-By: PHP/5.3.3

[sogoupopup]
version=4.2.0.2246
url=http://ime.sogou.com/popup_4.2.0.2246.dll
filesize=79360
md5=004c77921bd1bb412225237c373d9d96
```

Figure 3. Traffic capture of the update hijacking process

The software sends an HTTP GET request to ime.sogou.com to try to obtain the DLL; however, the communication is again redirected to the hijacking node, which serves popup_4.2.0.2246.dll that, in reality, is the *LittleDaemon* DLL. The process is illustrated in Figure 4.

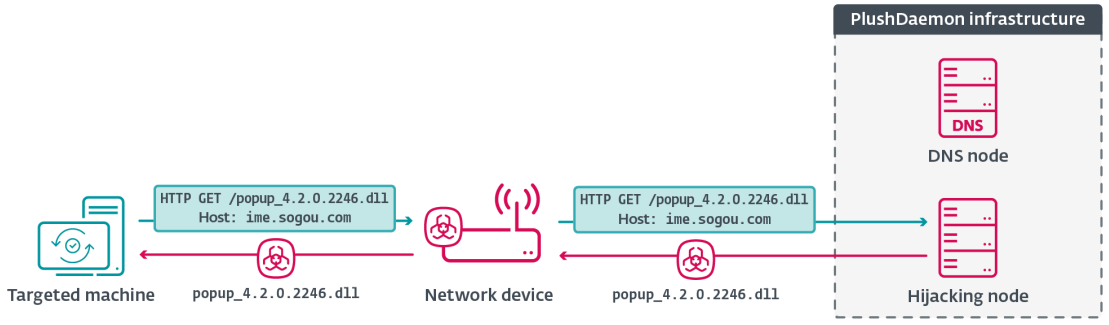

Figure 4. Illustration of the final stage of the update hijacking

Figure 5 shows the hijacking node serving LittleDaemon.

Figure 5. Traffic capture of the update hijacking process

EdgeStepper

According to the symbols in the binary, EdgeStepper was originally called dns_cheat_v2. It was developed in Go using the open-source GoFrame framework, and compiled as an ELF file for MIPS32 processors. It is important to note that it is unlikely that EdgeStepper is the only component deployed on the compromised network device. Unfortunately, we don't have samples of other components in the compromise chain.

EdgeStepper begins by obtaining and decrypting configuration data from /etc/bioset.conf. For decryption, it uses AES CBC with the key and IV being the string I Love Go Frame!, which is used as the default IV in the implementation by the GoFrame library.

The decrypted configuration reveals the data shown in Figure 6.

```
 [cheat]
toPort = 1090
host = "ds20221202.dsc.wcsset[.]com"
```

Figure 6. Decrypted configuration

The meaning of the parameters is as follows:

- toPort specifies the port where EdgeStepper will listen, and
- host specifies the domain that is resolved to obtain the IP address(es) of the DNS node to which the DNS query packets are forwarded.

Additionally, there is a configuration block (Figure 7) in the EdgeStepper binary, which appears to not be referenced anywhere in the code. The domain in the host field is test.dsc.wcsset[.]com, which resolved to 47.242.198[.]250. We observed that IP address from 2021 to 2022 as the source of the malicious update: the hijacking node. At the time of writing, the domain resolves to that IP address.

```
0043EEC3 aCheatToport109:.ascii "[cheat]\n"
0043EECB                  .ascii "toPort = 1090\n"
0043EED9                  .ascii "host = \"test.dsc.wcsset.com\"\n"
```

Figure 7. Unused configuration block in EdgeStepper

After loading its configuration, EdgeStepper initializes the *Distributor* system and the *Ruler* system.

Distributor

The distributor resolves the IP address(es) associated with the domain value in the host field of the configuration and invokes the Ruler system. The workflow of the distributor is illustrated in Figure 8.

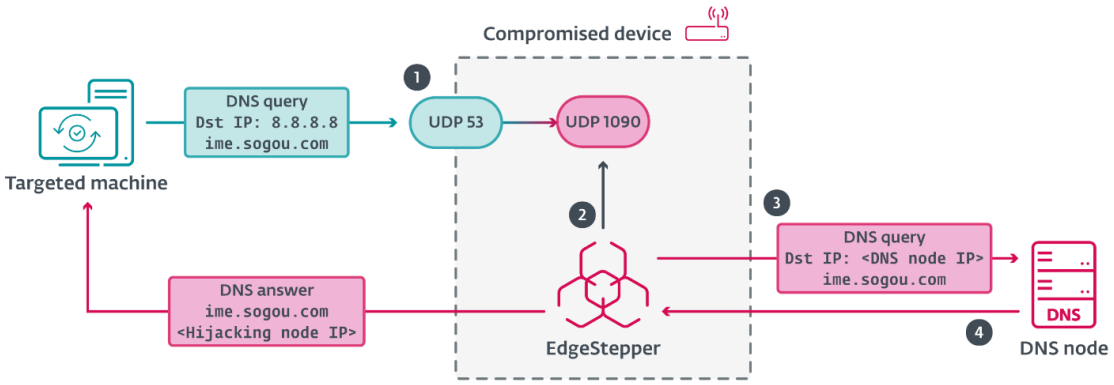

Figure 8. EdgeStepper workflow

1. Via the Ruler system, the distributor redirects traffic on port 53 to port 1090, establishing itself as a DNS proxy.
2. When a DNS message is received from a potential victim's device, it checks whether the message is RFC compliant (probably just to verify that the packet is really from the DNS protocol).
3. Then it forwards the packet to the malicious DNS node.
4. Finally, it forwards the reply from the DNS node to the device.

Ruler

The Ruler system uses the iptables command to issue new rules, and to remove them when concluding the attack. First, it issues a rule to redirect all UDP traffic on port 53 of the device to the port specified by toPort in the configuration:

iptables -t nat -I PREROUTING -p udp --dport 53 -j REDIRECT --to-port <value_from_toPort>

Then it issues a command to accept the packets on that port:

iptables -t filter -I INPUT -p udp --dport <value_from_toPort> -j ACCEPT

When terminating, it removes the previous rules it set up by issuing the commands:

iptables -t nat -D PREROUTING *

iptables -t filter -D INPUT -p udp –dport <value_from_toPort> -j ACCEPT

LittleDaemon

LittleDaemon is the first stage deployed on the victim's machine through hijacked updates. We have observed both DLL and executable versions, both of them 32-bit PEs. The main purpose of LittleDaemon is to communicate with the hijacking node to obtain the downloader that we call DaemonicLogistics. LittleDaemon does not establish persistence.

First, it verifies whether the SlowStepper backdoor is running on the system. If not, LittleDaemon downloads DaemonicLogistics by issuing an HTTP GET request to a server (typically, the hijacking node), decrypts it with a combination of XOR operations, and then executes it.

The request can be sent to two legitimate domains (ime.sogou.com or mobads.baidu.com) or the IP address 119.136.153.0. The resource path is /update/updateInfo.bzp for all three. In the case of the legitimate domains, it's expected that the traffic will be redirected to the hijacking node by EdgeStepper.

DaemonicLogistics

DaemonicLogistics is position-independent code downloaded and executed in memory by LittleDaemon. Its main purpose is to download and deploy the SlowStepper implant.

When DaemonicLogistics sends a request to the server (typically, the hijacking node), it replies with an HTTP status code, which DaemonicLogistics interprets as a command, and performs the actions listed in Table 1.

Table 1. Commands supported by DaemonicLogistics

Code	Action taken
200	Downloads SlowStepper without checking for the presence of a process named 360tray.exe (a component of the 360 Total Security antimalware solution).
205	
206	
208	
203	Downloads a file named plugin.exe and executes it (during our tests, the server did not request downloading this file).
207	Checks for the presence of a process named 360tray.exe and downloads SlowStepper if not present.
202–300	Default to execute command 200. These could be unimplemented commands.

The initial HTTP GET request is sent to:

ime.sogou.com/update/latest/new_version?tp=2&c=0&s=<OS_ID_number>&mac=<identifier>

The meaning of the parameters in the URL are as follows:

- The values tp and c are hardcoded by default to 2 and 0, respectively.

- The s field is one byte and is a number that identifies the operating system version.
- The mac field is six bytes and is the MAC address value from the machine's ethernet or Wi-Fi adapter, or randomly generated if it fails to obtain any; the value is probably used as an identifier by the server.

During our analysis we observed that the server replied with status code 207, to which DaemonicLogistics replied with another request to ime.sogou.com/update/latest/new_version?tp=1&g=15&c=0. In this case, the part of the URL tp=1&g=15&c=0 is hardcoded.

The server replied with status code 202. DaemonicLogistics proceeded to do two requests to download the SlowStepper payload files, first to ime.sogou.com/update/file6.bdat, and then to ime.sogou.com/update/file2.bdat.

The payload data in the first and second responses from the server began with a magic value:

- In response to the first request, the magic value in hex was 50 4B 03 04 0A 1B 2C 3D (PK\3\4\A\1B\2C\3C):

  ○ DaemonicLogistics actively checks that the first eight bytes of data received from the server match this magic value. If true, it writes the data to %PROGRAMDATA%\Tencent\QQUpdateMgr\UpdateFiles\logo.gif.

- In response to the second request, the magic value in hex was 47 49 46 38 39 61 10 10 (GIF89a\10\10)

  ○ DaemonicLogistics does not check this magic value specifically: when the check for the previous magic value does not match, it processes the data and decrypts it using a combination of XOR operations. The data contains files that are written to disk on paths specified in the decrypted data..

Conclusion

We analyzed the EdgeStepper network implant that enables PlushDaemon's adversary-in-the-middle capabilities to hijack updates from machines in a targeted network. We also analyzed LittleDaemon and DaemonicLogistics tools that together deploy the SlowStepper implant on Windows machines. These implants give PlushDaemon the capability to compromise targets anywhere in the world.

> *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	ESET detection name	Description
8F569641691ECB3888CD 4C11932A5B8E13F04B07	bioset	Linux/Agent.AEP	EdgeStepper.
06177810D61A69F34091 CC9689B813740D4C260F	bioset.conf	Win32/Rozena.BXX	EdgeStepper encrypted configuration.
69974455D8C13C5D57C1 EE91E147FF9AED49AEBC	popup_4.2.0.2246.dll	Win32/Agent.AGXK	LittleDaemon.
2857BC730952682D39F4 26D185769938E839A125	sogou_wubi_15.4. 0.2508_0000.exe	Win32/Agent.AFDT	LittleDaemon.

Network

IP	Domain	Hosting provider	First seen	Details
8.212.132[.]120	ds20221202.dsc. wcsset[.]com	Alibaba (US) Technology Co., Ltd.	2024-07-12	DNS/Hijacking node.
47.242.198[.]250	test.dsc.wcsset[.]com	Alibaba Cloud LLC	2024-07-12	DNS/Hijacking node.

MITRE ATT&CK techniques

This table was built using version 18 of the MITRE ATT&CK framework**.**

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	PlushDaemon uses EdgeStepper to redirect traffic to specific subdomains that are part of PlushDaemon's infrastructure on wcsset[.]com.
	T1583.002	Acquire Infrastructure: DNS Server	Part of the PlushDaemon infrastructure is used to host its malicious DNS nodes.
	T1583.004	Acquire Infrastructure: Server	PlushDaemon has acquired servers to host its DNS/hijacking nodes and C&C servers.
	T1608.001	Stage Capabilities: Upload Malware	PlushDaemon hosts its payloads on DNS/hijacking servers.

Tactic	ID	Name	Description
Initial Access	T1659	Content Injection	Hijacking nodes from PlushDaemon process hijacked traffic and reply to legitimate software with instructions to download malware such as LittleDaemon.
Execution	T1106	Native API	DaemonicLogistics executes the SlowStepper implant using the ShellExecute API.
Defense Evasion	T1070.004	Indicator Removal: File Deletion	Some variants of LittleDaemon can remove themselves.
	T1036.005	Masquerading: Match Legitimate Name or Location	DaemonicLogistics creates a subdirectory named Tencent, where it stores its files.
	T1036.008	Masquerading: Masquerade File Type	DaemonicLogistics and SlowStepper's loader can decrypt files that masquerade as ZIP and GIF files.
	T1027.009	Obfuscated Files or Information: Embedded Payloads	Files masquerading as ZIPs and GIF files contain embedded encrypted components.
	T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	Components of the SlowStepper implant are encrypted on disk.
Discovery	T1518.001	Software Discovery: Security Software Discovery	DaemonicLogistics checks for the presence of 360tray.exe – a component of 360 Total Security.
	T1016	System Network Configuration Discovery	DaemonicLogistics attempts to obtain the ethernet or Wi-Fi adapter's MAC address.
	T1057	Process Discovery	DaemonicLogistics lists processes.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	LittleDaemon and DaemonicLogistics use HTTP to communicate with their server.
	T1573	Encrypted Channel	LittleDaemon downloads via HTTP the encrypted DaemonicLogistics that downloads via HTTP the encrypted SlowStepper implant.

Tactic	ID	Name	Description
	T1665	Hide Infrastructure	LittleDaemon and DaemonicLogistics make downloads by sending HTTP requests to legitimate domains.

Source: https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-network-devices-for-adversary-in-the-middle-attacks/