Research Threat intelligence Microsoft Defender IoT / OT threats
11 min read

IoT devices and Linux-based systems targeted by OpenSSH trojan campaign

By Microsoft Threat Intelligence

June 22, 2023

Microsoft Defender for Endpoint

Microsoft Defender for IoT

Microsoft Sentinel

Attacker techniques, tools, and infrastructure

Cryptojacking

Linux

Cryptojacking, the illicit use of computing resources to mine cryptocurrency, has become increasingly prevalent in recent years, with attackers building a cybercriminal economy around attack tools, infrastructure, and services to generate revenue from targeting a wide range of vulnerable systems, including Internet of Things (IoT) devices. Microsoft researchers have recently discovered an attack leveraging custom and open-source tools to target internet-facing Linux-based systems and IoT devices. The attack uses a patched version of OpenSSH to take control of impacted devices and install cryptomining malware.

Utilizing an established criminal infrastructure that has incorporated the use of a Southeast Asian financial institution's subdomain as a command and control (C2) server, the threat actors behind the attack use a backdoor that deploys a wide array of tools and components such as rootkits and an IRC bot to steal device resources for mining operations. The backdoor also installs a patched version of OpenSSH on affected devices, allowing threat actors to hijack SSH credentials, move laterally within the network, and conceal malicious SSH connections. The complexity and scope of this attack are indicative of the efforts attackers make to evade detection.

In this blog post, we present our analysis of the tools and techniques used in this attack and the efforts made by the threat actor to evade detection on affected devices. We also provide indicators of compromise and relevant Microsoft Defender for IoT and Microsoft Defender for Endpoint detections, as well as recommendations for defenders to protect devices and networks.

Attack chain

The threat actors initiate the attack by attempting to brute force various credentials on misconfigured internet-facing Linux devices. Upon compromising a target device, they disable shell history and retrieve a compromised OpenSSH archive named *openssh-8.0p1.tgz* from a remote server. The archive contains benign OpenSSH source code alongside several malicious files: the shell script *inst.sh*, backdoor binaries for multiple architectures (x86-64, arm4l, arm5l, i568, and i686), and an archive containing the shell script *vars.sh*, which holds embedded files for the backdoor's operation.

After installing the payload, the shell script *inst.sh* runs a backdoor binary that matches the target device's architecture. The backdoor is a shell script compiled using an open-source project called Shell Script Compiler (shc), and enables the threat actors to perform subsequent malicious activities and deploy additional tools on affected systems.

Figure 1. OpenSSH trojan attack chain.

Custom backdoor deploys open-source rootkits

Once running on a device, the shell script backdoor tests access to */proc* to determine whether the device is a honeypot. If it can't access */proc*, it determines the device is a honeypot and exits. Otherwise, it exfiltrates information about the device, including its operating system version, network configuration, and the contents of */etc/passwd* and */etc/shadow* over email to the hardcoded address *dotsysadmin[@]protonmail[.]com*, and to any email address provided by the threat actor as an argument to the script.

On supported systems, the backdoor downloads, compiles, and installs two open-source rootkits available on GitHub, Diamorphine and Reptile. The backdoor configures Reptile to connect to the C2 domain *rsh.sys-stat[.]download* on port 4444 and to hide its child processes, files, or their content. Microsoft researchers assess that the Diamorphine rootkit is used to hide processes as well.

Figure 2. Any content in a file that appears between __R_TAG, which is defined as "ubiqsys", will be hidden.

To ensure persistent SSH access to the device, the backdoor appends two public keys to the *authorized_keys* configuration files of all users on the system.

Figure 3. Adding SSH keys to all users to preserve SSH access.

The backdoor obscures its activity by removing records from Apache, nginx, httpd, and system logs that contain the IP and username specified as arguments to the script. Additionally, it has the capability to install an open-source utility called *logtamper* to clear the *utmp* and *wtmp* logs, which record information about user sign-in sessions and system events.

The backdoor eliminates cryptomining competition from other miners that may exist on the device by monopolizing device resources and preventing communication with a hardcoded list of hosts and IPs related to these activities. It accomplishes this by adding iptables rules to drop communication with the hosts and IPs and configuring */etc/hosts* to make the hosts resolve to the localhost address. It also identifies miner processes and files by their names and either terminates them or blocks access to them, and removes SSH access configured in *authorized_keys* by other adversaries.

Patching OpenSSH source code

The backdoor uses the Linux *patch* utility to apply the patch file *ss.patch*, which is embedded in *vars.sh*, to the OpenSSH source code files included in its package. Once the patches are applied, the backdoor compiles and installs the modified OpenSSH on the device.

The compromised OpenSSH grants the attackers persistent access to the device and to the SSH credentials the device handles. The patches install hooks that intercept the passwords and keys of the device's SSH connections, whether as a client or a server. The passwords and keys are then stored encrypted in a file on the disk. Moreover, the patches enable root login over SSH and conceal the intruder's presence by suppressing the logging of the threat actors' SSH sessions, which are distinguished by a special password.

The modified version of OpenSSH mimics the appearance and behavior of a legitimate OpenSSH server and may thus pose a greater challenge for detection than other malicious files. The patched OpenSSH could also enable the threat actors to access and compromise additional devices. This type of attack demonstrates the techniques and persistence of adversaries who seek to infiltrate and control exposed devices.

Figure 4. OpenSSH patch to save incoming SSH passwords (ss.patch)

Botnet operation

The backdoor runs a secondary payload embedded in the shell script *vars.sh*, which is a slightly modified version of ZiggyStarTux, an open-source IRC bot based on the Kaiten malware. Among its features is executing bash commands issued from the C2 and possessing distributed denial of service (DDoS) capabilities.

The backdoor employs various mechanisms to set up ZiggyStarTux's persistence on compromised systems. It copies the ZiggyStarTux binary to several locations on the disk and establishes *cron* jobs to invoke it at regular intervals. Moreover, it runs a bash script that registers ZiggyStarTux as a *systemd* service by creating and configuring the service file */etc/systemd/system/network-check.service*.

Figure 5. Registration of ZiggyStarTux as a systemd service

Analysis of ZiggyStarTux revealed that the threat actors stripped the binary of logging-related strings and incorporated a function that writes the bot's process ID to */var/run/sys_checker.pid*, allowing the backdoor to read that file and conceal that process ID using the installed rootkits.

The ZiggyStarTux bots communicate with the C2 via an IRC server hosted on various domains and IPs located in different geographical regions. Evidence indicates that the threat actors disguise their traffic by utilizing the subdomain of a Southeast Asian financial institution that is hosted on one of their own servers.

To receive commands, the ZiggyStarTux bots connect to the IRC server and join a hidden password-protected channel named *##..##*. The server was observed issuing bash commands that instruct bots to download and launch two shell scripts from a remote server. The first script, *lscan*, retrieves *lssh.tgz* from the server, an archive of scripts that scan each IP in the subnet for SSH access using a password list. The scripts record the results of each connection attempt in a log file.

The second script, *zaz*, fetches the compromised OpenSSH package with the embedded backdoor from the remote server. The installation is carried out using the email address *ancientgh0st@yahoo[.]com* as an argument to serve as an additional exfiltration point for device information. Additionally, *zaz* retrieves an archive called *hive-start.tgz* which contains mining malware crafted for Hiveon OS systems, a Linux-based open-source operating system designed for cryptomining.

Indications of criminal cooperation

Microsoft researchers have traced the campaign to a user named *asterzeu* on the hacking forum *cardingforum[.]cx*, who offered multiple tools for sale on the platform, including an SSH backdoor. The domain *madagent[.]tm* was registered in 2015 with an email address matching the username and shared numerous servers over a four-year period with *madagent[.]cc*, one of the C2 domains of ZiggyStarTux. Furthermore, the distribution of the shell script backdoor between threat actors has been identified, adding to the evidence of a network of tools and infrastructure shared or sold on the malware-as-a-service market.

Figure 6. Post on hacking forum where malicious tools are being sold by the user "asterzeu"

Mitigation and protection guidance

Microsoft recommends the following steps to protect devices and networks against this threat:

- Harden internet-facing devices against attacks
  - Ensure secure configurations for devices: Change the default password to a strong one, and block SSH from external access.
  - Maintain device health with updates: Make sure devices are up to date with the latest firmware and patches.
  - Use least-privileges access: Use a secure virtual private network (VPN) service for remote access and restrict remote access to the device.
  - When possible, update OpenSSH to the latest version.
- Adopt a comprehensive IoT security solution such as Microsoft Defender for IoT to allow visibility and monitoring of all IoT and OT devices, threat detection and response, and integration with SIEM/SOAR and XDR platforms such as Microsoft Sentinel and Microsoft 365 Defender.
- Use security solutions with cross-domain visibility and detection capabilities like Microsoft 365 Defender, which provides integrated defense across endpoints, identities, email, applications, and data.

Detections

Microsoft Defender for IoT

Microsoft Defender for IoT uses detection rules and signatures to identify malicious behavior. Microsoft Defender for IoT has alerts for the use of open-source tools and exploits that may be tied to this attack.

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects this threat as the following malware:

- Trojan:Linux/SamDust!MTB
- Trojan:Linux/SamDust.D!MTB
- Trojan:Linux/SamDust.B!MTB
- Trojan:Linux/SamDust.A!MTB
- Trojan:Linux/SamDust.N!MTB
- Trojan:Linux/Reptile.A
- Trojan:Linux/Reptile.B
- Trojan:Linux/Reptile.C
- Trojan:Linux/Reptile.D
- Trojan:Linux/Diamorphine.A!MTB

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate associated threat activity:

- Unusual number of failed sign-in attempts

The following alerts might also indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- Suspicious file property modification occurred
- Suspicious termination of security tool
- Suspicious service launched
- Suspicious Linux service created
- File masquerading

Hunting queries

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy.

In addition, customers can use the SSH Brute force detection template in the Syslog solution package to monitor for brute force attempts against their exposed SSH endpoints.

Indicators of Compromise

Indicator	Type
asterzeu[@]yahoo[.]com	Email address
dotsysadmin[@]protonmail[.]com	Email address
185.161.208[.]234	C2

139.180.185[.]24	C2
199.247.30[.]230	C2
149.28.239[.]146	C2
209.250.234[.]77	C2
70.34.220[.]100	C2
irc[.]socialfreedom[.]party	C2
singapore[.]sg[.]socialfreedom[.]party	C2
amsterdam[.]nl[.]socialfreedom[.]party	C2
frankfurt[.]de[.]socialfreedom[.]party	C2
sidney[.]au[.]socialfreedom[.]party	C2
losangeles[.]us[.]socialfreedom[.]party	C2
mumbaitravelers[.]org	C2
sh[.]madagent[.]tm	C2
ssh[.]madagent[.]tm	C2
dumpx[.]madagent[.]tm	C2
reg[.]madagent[.]tm	C2
sshm[.]madagent[.]tm	C2
z[.]madagent[.]tm	C2
ssho[.]madagent[.]tm	C2
sshr[.]madagent[.]tm	C2
sshu[.]madagent[.]tm	C2
user[.]madagent[.]tm	C2
madagent[.]cc	C2
cler[.]madagent[.]cc	C2
dumpx[.]madagent[.]cc	C2
mh[.]madagent[.]cc	C2
ns1[.]madagent[.]cc	C2

ns2[.]madagent[.]cc	C2
ns3[.]madagent[.]cc	C2
ns4[.]madagent[.]cc	C2
reg[.]madagent[.]cc	C2
ssh[.]madagent[.]cc	C2
sshm[.]madagent[.]cc	C2
ssho[.]madagent[.]cc	C2
sshr[.]madagent[.]cc	C2
sshu[.]madagent[.]cc	C2
user[.]madagent[.]cc	C2
www[.]madagent[.]cc	C2
rsh[.]sys-stat[.]download	C2
sh[.]sys-stat[.]download	C2
sh[.]rawdot[.]net	C2
ssho[.]rawdot[.]net	C2
donate[.]xmr[.]rawdot[.]net	C2
pool[.]rawdot[.]net	C2
2018[.]rawdot[.]net	C2
blog[.]rawdot[.]net	C2
clients[.]rawdot[.]net	C2
ftp[.]rawdot[.]net	C2
psql01[.]rawdot[.]net	C2
www[.]rawdot[.]net	C2
sh[.]0xbadc0de[.]stream	C2
ss[.]0xbadc0de[.]stream	C2
a26631dcc1aef92a92d2d37476fb1e9becae54541e0411224a441d3afc20b02a	Script to launch ZiggyStarTux

6e9b692b401a57db306bd6c95409042aa6ed075088a40a6ceb74f96895116b62	ZiggyStarTux
5e11731e570fc79ad07da4f137e103e0ebfa45530fabd8fa9a9fece4e497bce0	ZiggyStarTux
22c2115becd1d0ff9dfe70d14a52ab0354e420f4bfe0df70ca0d55d3c557c6b3	ZiggyStarTux
d335c83c0dd5bc9a078e796016f9a9f845ff89ee434c63c7a2e7b360e8be3e95	ZiggyStarTux
336928c813f3c0ab9aaad5a9853ed96b3f82e7b2b6d96139a7ebb146337dd248	ZiggyStarTux
1f6a52ce5ee017f88bd5f9028e3741e69837437cc48444d31d50ef28f1ed03f4	ZiggyStarTux
b72f21077f9f4d85d555cc6c18677e285b61f980ca99d0495d52f0cbbe66517a	Malicious OpenSSH
8e7c6cbbb17ffe5ea98986dd36c3e979bc348626637ff9bfd55cb08414f3494c	Malicious OpenSSH
39b640f62c0046139c41bccd0f98f96165597d50c4823ed88154160c0cae6bd1	Malicious OpenSSH
b77f991a9e0533a7bb39480ba7e96c29a1c1c9e2e212497cfbf6221751a196a2	Malicious OpenSSH
1782930bc2d46da541c980c09b13811f504b743e485a2befb0df1e5865a95847	Malicious OpenSSH
7ea1db1581afb977ec6d4abadf98660526205f23c366f7ba6aa04061762b5a7e	Malicious OpenSSH
4b23d2126a6aec79396630dc10bdf279d9dafc71358145ab0b726cdf0a90dedf	Malicious OpenSSH
081ad11e67af3fd98cb34cae89a5d26699f132a7ada62b1409eb85eaa4431437	Malicious OpenSSH
8ff06c7f0c105301397d15b1be3f6fe3ba081bbe042136c5b0fa4478ab59650d	Backdoor
28616594b320b492c04429ab2f569d22d56bd9a047903f214d8b0eacab9b9c14	Backdoor
e22148ae0cb1a5cc7743351909cd0ae99ba6a84e181dded1cfa9fa0ed9e4f0e2	Backdoor
6101fcda212f2ee2340e85eaac071ffa95507166ba253d555a69c9ab6c16b148	Backdoor

52fb0dcd929d57e32c8383873897963dd671b626d7e31dd98d2b092a9b57be43	Backdoor
78701d6cafb3e477a033d63b99d480c2d7647079133ecabdcb54cd7a520e46de	Backdoor
2eb5a4766dd7b90674f16eea62ba4e9c33dac8023e1692ed67c917bca448d14f	Backdoor
c775964fe1207b6a6f9faf818c63874b2bf5612581e3c3b2d9f6eeee969229d8	Backdoor
75385bb1548c567c4814ad5c13fde6bf64e47694c244e1c26e903abc4523c667	Backdoor
bc1e444ab92bb40e41e08846f3e485ffa17ab98563f2ed2129ef1b02c3d5a878	Backdoor
8cb1df542bc60eb187066c136ae413540b33dd28c856ee472dd073affb96a84b	Backdoor
55448d04183a253c939a6463c8992cbc007be237c80de92ff31e3f6606ebd470	Backdoor
9967921339799ed6f510c8a567f8bd69129d75d113f5c63612ceef0d5c4bf019	Backdoor
0a565ebae65fb5fbb34801c2948d35a0b7b5762a9ce51bd55a43181f46bc9723	Backdoor
fdfed7c2bf55d0f2440f623e265ab8b8006987f94d23982688914feffb3c549e	Backdoor
32aa3e5fd9b79dcfd9ebe590b6784527cb17217cdeb61a1791bd4a5f721f0099	vars.sh archive
30d456d6dbd492923972d5f3ceb72c0f7e80d1f6391d6f9c0f5e889b6f71be66	vars.sh archive
74f4b030529435a8872c3e10d3341a1988d4fdbba89d9afd876458980f6f7a49	vars.sh archive
3033bb18554ce62f2f96338af682efb647c98d126734bb20426da8ec49ec1cdd	Decode utility used by the backdoor
58b9622960e1bb189a403da6cd73e6ec2cb446680a18092351e5a9fa1a205cbc	ss.patch
0027edb4a3c33f3d0cb5cc6fc85b58a8f7c70b8e57a2d28bed53f11c5f649848	inst.sh
7ca66932d9015bf14b89b8650408e39a65c96f59f9273feaede28cabca8a3bbc	hive-start.tgz

9564172445e66f0d3cb64c42f2298f14093c342b95b023bc b82408b6f2a66cd3	lssh.tgz
722b1970caa804154d85fb3dba88cf192bf3eedd2fea40c8c 49c98130797649d	File from lssh.tgz
85877eb8f60c903ccb256e776c3e077295cf10eccff8d8ce4 400edc699e8021f	File from lssh.tgz
635b3dfadeab6b3c2574b1689607b776518d42c2b9fdb89 5e25c04a8ae9dee92	File from lssh.tgz
3ba302f533fcf065fe3f80b4bbea4653e86a5a8c1c752e479 8a64a6be3d06e5d	File from lssh.tgz
b8a360e7094e27857c7daacf624f2d9916e002201caf8a88 c5aa3bd37f7bc264	File from lssh.tgz

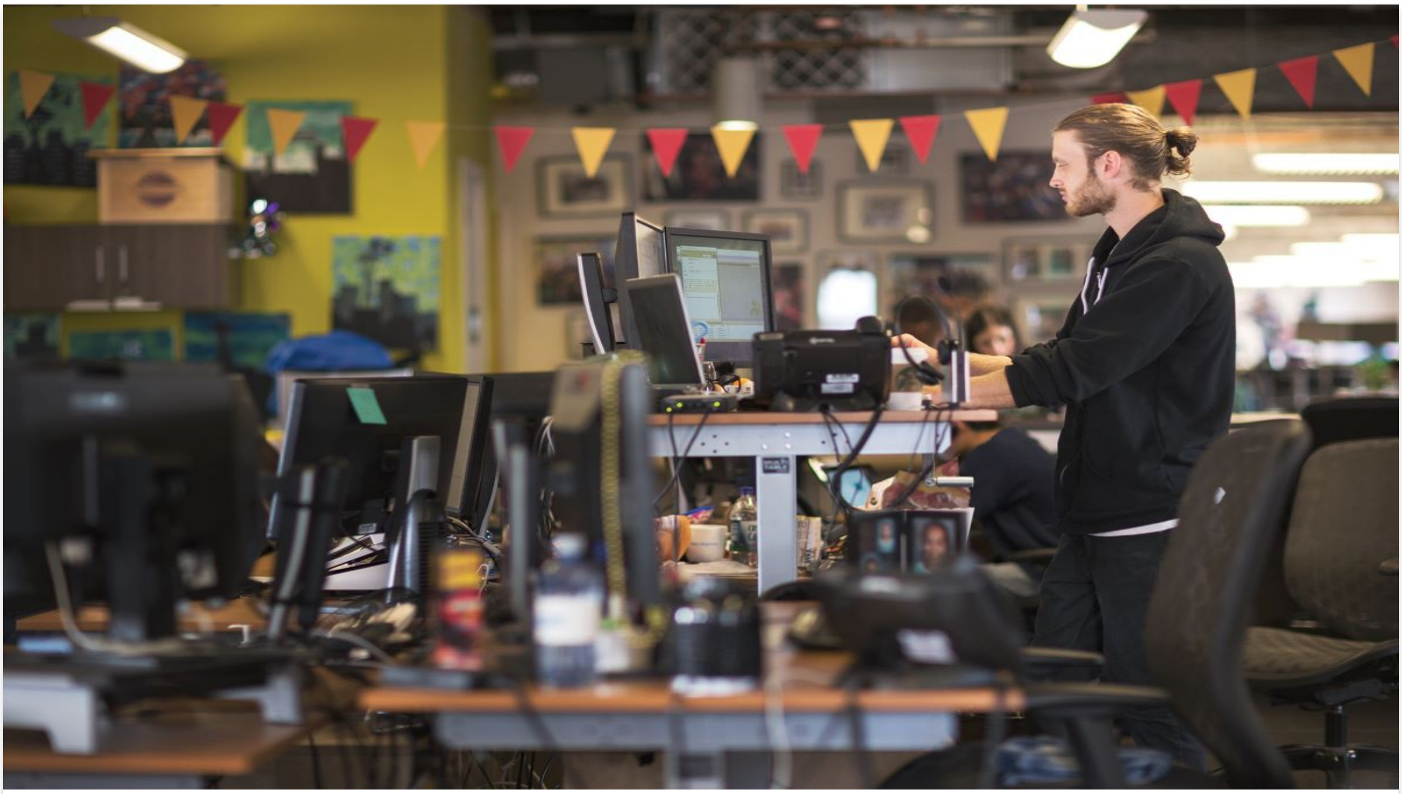
***Rotem Sde-Or**, Microsoft Threat Intelligence Community*

Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

Related Posts



[Research](#)
[Threat intelligence](#)
[IoT / OT threats](#)

Dec 21
12 min read

Microsoft research uncovers new Zerobot capabilities

The Microsoft Defender for IoT research team details information on the recent distribution of a Go-based botnet, known as Zerobot, that spreads primarily through IoT and web-application vulnerabilities.

[Research](#)
[Threat intelligence](#)
[Microsoft Defender](#)
[IoT / OT threats](#)

Dec 15
9 min read

MCCrash: Cross-platform DDoS botnet targets private Minecraft servers

The Microsoft Defender for IoT research team analyzed a cross-platform botnet that infects both Windows and Linux systems from PCs to IoT devices, to launch distributed denial of service (DDoS) attacks against private Minecraft servers.

[Research](#)
[Threat intelligence](#)
[Microsoft Defender](#)
[Supply chain attacks](#)

Nov 22
6 min read

Vulnerable SDK components lead to supply chain risks in IoT and OT environments

As vulnerabilities in network components, architecture files, and developer tools have become an increasingly popular attack vector to leverage access into secure networks and devices, Microsoft identified such a vulnerable component and found evidence of a supply chain risk that might affect millions of organizations and devices.

[Research](#)
[Threat intelligence](#)
[Microsoft Defender](#)
[IoT / OT threats](#)

Oct 21
4 min read

Securing IoT devices against attacks that target critical infrastructure

South Staffordshire PLC, a company that supplies water to over one million customers in the United Kingdom, notified its customers in August of being a target of a criminal cyberattack. This incident highlights the sophisticated threats that critical industries face today. According to South Staffordshire, the breach did not appear to have caused damage to [...]