AL2025_06 Chinese cyberspies use new SSH backdoor in network device hacks (7th February 2025)

Description

A newly identified attack campaign by the Chinese cyber-espionage group Evasive Panda (DaggerFly) involves the hijacking of the SSH daemon on network appliances. The attack utilizes a sophisticated malware suite, named ELF/Sshdinjector.A!tr, to gain persistent access and conduct covert operations. This campaign has been active since mid-November 2024, targeting network devices for intelligence collection and espionage.

Attack Details

The attack begins with an initial compromise of network appliances, though the exact infiltration method remains undisclosed. Once a device is breached, a dropper component checks for existing infections and verifies if the system is running with root privileges. If these conditions are met, several binaries, including an SSH library (libssdh.so), are deployed to the target machine.

The injected SSH library serves as the primary backdoor, facilitating command and control (C2) communications and data exfiltration. Other components, such as mainpasteheader and selfrecoverheader, are used to maintain persistence on compromised devices.

The malware can execute fifteen different commands, including:

- System reconnaissance by collecting hostname and MAC address details
- Listing installed services from /etc/init.d
- Extracting sensitive user credentials from /etc/shadow
- Monitoring active processes
- Accessing system logs from /var/log/dmesg
- Reading potential sensitive data from /tmp/fcontr.xml
- Managing files on the system (uploading, downloading, renaming, and deleting)
- Establishing a remote shell for full command-line access
- Executing arbitrary commands remotely
- Removing itself from memory when required
- Notifying the attacker upon successful infection

Remediation

To mitigate the risk of infection from ELF/Sshdinjector.A!tr, organizations should take the following steps:

1. **Update Security Systems:** Ensure that security solutions, including antivirus and intrusion detection systems, are up to date. Fortinet customers are protected through the FortiGuard AntiVirus service.
2. **Monitor Network Traffic:** Watch for abnormal SSH traffic patterns, particularly unexpected outbound connections.

3. **Restrict SSH Access:** Limit SSH access to trusted users and implement multi-factor authentication.
4. **File Integrity Monitoring:** Regularly check for unauthorized modifications to SSH and system service files.
5. **Patch and Update Firmware:** Ensure network appliances and SSH services are updated to the latest security patches.
6. **Incident Response Readiness:** Organizations should prepare an incident response plan in case of suspected compromise, including forensic analysis and system isolation measures.

By implementing these defensive strategies, organizations can significantly reduce the risk posed by this advanced SSH backdoor attack.

References

- Onsite Computing, Inc. (2025, February 4). Chinese cyberspies use new SSH backdoor in network device hacks. Retrieved from Onsite Computing. https://www.onsitecomputing.net/2025/02/04/chinese-cyberspies-use-new-ssh-backdoor-in-network-device-hacks/
- Toulas, B. (2025, February 4). Chinese cyberspies use new SSH backdoor in network device hacks. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/chinese-cyberspies-use-new-ssh-backdoor-in-network-device-hacks/