

Ministry of Industry and Information Technology: Risk Tips on Preventing PolarEdge Botnets - Security Insider

 secrss.com/articles/86101



Ministry of Industry and Information Technology: Tips on Preventing PolarEdge Botnets

[Virus Trojan Network Security Threat and Vulnerability Information Sharing Platform](#) 2025-12-16

The attackers used security vulnerabilities in company router-related products such as Cisco, Asus, QNAP and Qunhui to deploy PolarEdge backdoors, hijack control devices, steal sensitive data, and form a botnet.

Recently, the Ministry of Industry and Information Technology's network security threat and vulnerability information sharing platform (CSTIS) monitoring found that the attackers used Cisco, Asus, Unicom and Qunhui and other company router-related products to deploy PolarEdge backdoor procedures, hijack control devices, steal sensitive data, and form a botnet.

The attacker hacked the target device through security vulnerabilities in company router-related devices such as Cisco, ASUS, QNAP, and Qunhui, forcing the victim device to download Shell scripts from a remote FTP server. The script will be downloaded and started immediately after the script is run and the PolarEdge backdoor is launched. Once implanted, PolarEdge performs environmental cleanup first, removes wgets, and renames curl to block competitive attacks. PolarEdge then starts the process occult, disguises it as a legitimate system process such as igmp proxy, and binds to a reserved PID path (such as /proc/1) to hide process metadata via mount-bind. At the same time, PolarEdge implements process navigation by creating a watchdog child process, checks the parent process status every 30 seconds and restarts automatically when it is abnormal. After the completion of the door deployment, PolarEdge will start hidden communication, use self-signed PolarSSL certificates and magic tokens to build a TLS encryption channel, combined with PRESENT packet password dynamic decryption key code segments, imitation password (AffineCipher) confusing sensitive string data. PolarEdge will then deliver malicious payloads to /tmp/.qnx.sh in reconnect mode for remote dynamic control.

It is recommended that relevant units and users immediately organize inspections, verify the digital signature of firmware, block malicious implants; update the security version of the device in time, and replace the discontinued and stop-duty equipment. Or by disabling high-risk service

components, turning off non-essential Internet exposure services (such as UPnP, PhotoStation, remote management ports), and regularly offline backup of sensitive data to prevent the risk of attacks.

IOC information for PolarEdge backdoor samples

SHA256: a3e2826090f009691442ff1585d07118c73c95e40088c47f0a16c8a59c9d9082

SHA1: ff1b0a492dd42fc01e1b894b577040927890b3bb3b

MD5:191be2f2f31efe4a64da54.ed9d0e25

Statement: This article is from the network security threat and vulnerability information sharing platform, copyright is owned by the author. The content of the article only represents the independent views of the author, does not represent the security insider position, and the purpose of reprinting is to pass on more information. If there is an infringement, please contact anquanneican@163.com.

[Virus Trojan Regulatory](#)

Related information

- **[Ministry of National Security: Catching the "Fox Tail" of Trojan Virus Stealing Secrets](#)**

[Virus Trojan Ministry of National Security](#) 2025-12-10

[Some people with ulterior motives will disguise it as a file containing a secretive virus, which will easily make the relevant unit personnel relax their vigilance, and once clicked, it will cause harm to the security of information data.](#)

- **[At least \\$14.8 billion! In the past three years, the amount of ransomware ransom paid by the injured enterprises has reached a record high.](#)**

[Financial insurance Security Intravenor](#) 2025-12-08

[According to statistics from the U.S. Treasury Department, between 2022 and 2024, victims paid at least \\$14.8 billion in ransomware organizations through U.S. financial institutions alone, a record high.](#)

- **[The Hidden Value of Remote Denial of Service Attack Vulnerability on Android](#)**

[Virus Trojan Blackbird](#) 2025-12-02

[There are indications that CVE-2025-48633 and CVE-2025-48572 may be being targeted for limited exploitation.](#)