Threat Intelligence Report

Threats Posed by Compromised Network Devices

Threat actors can exploit vulnerabilities in network devices to obfuscate malicious activity, bypass network defenses, and create large-scale networks of hijacked devices. Almost all organizational network traffic passes through these devices, making the devices ideal targets for threat actors looking to steal proprietary or otherwise sensitive information from targeted organizations. Vulnerable network devices may still be compromised even if device owners themselves are not targets of the malicious activity. Taking advantage of the opportunity to conceal signs of compromise amongst normal network traffic, threat actors may target and hijack unpatched or end-of-life routers, particularly small office/home office (SOHO) routers, to use as covert global infrastructure. This infrastructure is used to extend the reach, impact, and effectiveness of their cyber-enabled campaigns.

THREAT ACTIVITY

- In December 2023, researchers detailed an extensive SOHO router botnet serving as a covert data transfer network for threat actors, including Volt Typhoon.
- In November 2023, a large U.S. retailer had more than 1,000 network devices compromised in a cyber attack, preventing customers from placing online orders and leading to some franchise owners experiencing follow-up phishing attacks.
- In September 2023, several government agencies – including the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) – released a joint advisory detailing a state-sponsored threat actor capable of modifying router firmware without detection, allowing the actors to disable logging and abuse trusted domain relationships to access the intended target.
- In July 2023, researchers uncovered a covert network of more than 70,000 infected SOHO routers that had gone undetected for more than two years, and was used to enable a range of malicious activities including password spraying and digital advertising fraud.

THREAT ASSESSMENT

- We expect threat actors will increase their reliance on compromised networks while conducting malicious activity due to the level of obfuscation they provide. Intrusions leveraging compromised routers will be more difficult for network defenders to identify and mitigate, further increasing their appeal to threat actors.
- Organizations will likely need to allocate additional resources for securing network devices. Anomalous activity on network devices can be difficult to detect, as there is often no disruption of service or bandwidth and the devices can exist outside traditional security perimeters.
- Compromised network devices are used by both nation-state threat actors for intelligence collection or espionage, and cyber criminals as an initial network entry point or infrastructure for deploying malware or engaging in other nefarious activities.

RECOMMENDED ACTION

- Always install the latest updates and patches on network devices to protect against known vulnerabilities.
- Replace network devices once they have reached end-of-life.
- Harden devices for operation by reconfiguring default settings, resetting default passwords, and disabling unnecessary functions.
- Implement virtual segmentation of networks using tools like Virtual Local Area Networks (VLANs) and Virtual Private Networks (VPNs) to improve network security controls and ensure that a threat actor cannot access an entire organizational network through a single entry point.
- Limit internal access to network devices by implementing multi-factor authentication (MFA), managing privileged access, regularly updating administrative credentials, and improving security surrounding physical network devices.
- Do not ignore suspicious activity originating from residential IP addresses.

SOURCES

Sources include open-source information from public and private indusry reporting.

- Dark Reading: Ace Hardware Still Reeling From Weeklong Cyberattack
- CISA: People's Republic of China-Linked Cyber Actors Hide in Router Firmware
- Lumen: Routers From The Underground: Exposing AVrecon
- NCSC: APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers
- CISA: Securing Network Infrastructure Devices

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

Americas

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)