مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

IoT Botnet Targets Global Organizations with Large-Scale DDoS Attacks

Tracking #:432316769

Date:21-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a large-scale Distributed Denial-of-Service (DDoS) campaign, orchestrated by an IoT botnet, has been ongoing since the end of 2024.

TECHNICAL DETAILS:

A large-scale Distributed Denial-of-Service (DDoS) campaign, orchestrated by an IoT botnet, has been ongoing since the end of 2024. This botnet, comprising malware variants derived from Mirai and Bashlite, targets IoT devices—specifically wireless routers and IP cameras—by exploiting remote code execution (RCE) vulnerabilities and weak device credentials. The botnet's C&C (command-and-control) servers issue commands to infected devices, allowing attackers to manipulate the devices for further exploits.
Organizations worldwide, particularly in the information, communication, and finance sectors, have been affected. The attackers' ability to hijack IoT devices via default credentials and security weaknesses underscores the critical need for stronger security measures across IoT ecosystems.

Details:
Technical Analysis
Initial Infection:

- The botnet infects IoT devices by exploiting Remote Code Execution (RCE) vulnerabilities or weak passwords.
- The infection process involves downloading and executing a second-stage executable file (loader) that connects to the Command-and-Control (C&C) server for attack commands.
- The malware deactivates the watchdog timer to prevent the device from restarting during high loads.

Commands:

- The botnet uses various commands for DDoS attacks, including socket, handshake, stomp, syn, ack, udph, tonudp, gre, update, exec, kill, socks, and udpfwd.
- Commands are text messages with a message length of two bytes added at the beginning, using a specific structure.

Use of iptables:

- The malware abuses the iptables command in Linux systems to delay the discovery of the infection and manipulate the packets used in DDoS attacks.
- It sets rules to allow TCP connection requests from the LAN side, deny TCP connection requests from the WAN side, and allow communication with the C&C server.

Analysis of DDoS Attack Targets

- The attacks target various regions, including Asia, North America, South America, and Europe.
- Differences in command usage exist between domestic (Japan) and international targets, with varied impact on different industry sectors.

Botnet Trends

- The majority of the devices used in the attack were wireless routers (80%) and IP cameras (15%).
- TP-Link and Zyxel wireless routers accounted for 52% and 20% respectively, while Hikvision IP cameras accounted for 12%.

Countermeasures Against Specific Types of DDoS Attacks

UDP Flood:

- Use a firewall or router to block specific IP addresses or protocols and restrict traffic.
- Collaborate with communication service providers to filter DDoS traffic at the backbone or edge of the network.
- Strengthen router hardware to increase the number of packets that can be processed.
- Perform real-time monitoring and block IP addresses with high communication traffic.

TCP SYN Flood, TCP ACK Flood, STOMP Flood, GRE Flood, socket, handshake:

- Use a CDN provider to distribute and mitigate the load of the attack.
- Limit the number of requests that can be sent by a specific IP address within a certain period of time.
- Use third-party services to separate attack traffic and process clean traffic.
- Perform real-time monitoring and block IP addresses with a high number of connections.
- Detect and block abnormal traffic with IDS/IPS.
- Cut off clients that have been connected for a long time but have not sent packets via behavioral analysis.
- Strengthen server hardware to increase the number of packets that can be processed.
- Increase the upper limit of server connections to improve availability.
- Shorten timeout periods to quickly reuse server resources.

Indicators of Compromise:

SHA256	Detection Name
be2d34d170e8fc4956464f36c36c93dbeaa2957c0ed4139e1d06a5693c3f8b25	TROJ_FRS.VSNTA525
63e91c3ddf7c808008b2bdef26d56b110b6b4b0b23c6e470045564864c44143e	Trojan.Win32.FRS.VSNW1CL24
405491255ff73ddfb1dd2a1859347dd00a3ce05bc681693fc7cd95fc11717a5a	Trojan.Linux.MIRAI.AU
620636c1b8ecdde20b33a572bc79b2f2b9a212e063bf17a61e9e294adc5eb857	Backdoor.Linux.MIRAI.VSNTLS24
0cffa89872b6fda2dd813bde128763c77280e663a8f73b3c1c5fb76bc7355cd1	TROJ_FRS.VSNTLS24
d1585e0acc839200b095c76833d0c85fdc95df3894a18662b508f734075b5297	Backdoor.Linux.MIRAI.VSNTA525
371204521df08047c17cc2934c50c0ffec48b4cde93dd19a4495dcfc671a3060	TROJ_FRS.VSNTA525
548d1c8de71f5444228e2c1f031c540b0e08781e332f46a5d21e564180c81b6d	Backdoor.Linux.MIRAI.VSNTA525
32bc52b263c6d40077eeaf4e2c105c91fdfb3eb859b1d11470b5a2087a39bcee	TROJ_FRS.VSNTLS24
1bba9d9ca796b61828ff9866f0c7a8326e5d34eda6bd20d790fab846091e5d07	Trojan.Win32.FRS.VSNW05A25
aebe831a4ab5dee97209ecc80a3a9728dae38dd8eb0cdc744bf26ff51baa6998	Trojan.Linux.MIRAI.AU
C&C servers	
92[.]249[.]48[.]205	
156[.]253[.]250[.]201	
194[.]50[.]16[.]15	

RECOMMENDATIONS:

1. **Change Default Credentials**: Immediately change the default username and password to secure and difficult-to-brute-force credentials after purchasing the device.
2. **Regular Updates**: Regularly apply the latest firmware and software provided by the manufacturer to prevent attackers from exploiting known vulnerabilities.
3. **Disable Unused Functions**: Consider disabling remote access or port forwarding functions that are not in use.

4. **Network Segmentation**: Separate IoT devices into a dedicated network to reduce risks to other systems.
5. **Review Router Settings**: Review the settings of home routers and avoid opening unnecessary ports.
6. **Proper Asset Management**: Properly manage and configure machines and other assets, including IoT devices, to eliminate situations where devices are running without being recognized and to prevent leaving unnecessary devices unused.
7. **Restrict Access**: If it is necessary to use the management function from the internet, restrict the access source to the minimum necessary to prevent abuse.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.trendmicro.com/en_us/research/25/a/iot-botnet-linked-to-ddos-attacks.html?&web_view=true