Eleven11bot Botnet Expands to Over 86,000 Devices

Overview

A botnet, named Eleven11bot, has rapidly infected over 86,000 IoT devices, primarily security cameras and network video recorders (NVRs). The botnet has been observed launching DDoS attacks against telecom providers, gaming infrastructure, and other industries.

Researchers now believe Eleven11bot is a Mirai variant, exploiting a new vulnerability in HiSilicon-based devices running TVT-NVMS9000 software. There are conflicting estimates on the number of actively compromised devices, with GreyNoise revising its count to under 5,000. Nokia Deepfield reports at least 30,000 devices engaged in DDoS activity.

Mirai-based botnets have previously been linked to threat actors in China, Russia, and Eastern Europe, but Eleven11bot's new exploit for HiSilicon devices suggests a different operator may be involved. GreyNoise data shows a large number of compromised devices traced to Iran (over 60% of observed Ips).

Affected Products

- IoT devices, including **security cameras and network video recorders (NVRs)**
- Devices running **TVT-NVMS9000 software** on **HiSilicon chipsets**
- Systems using **default or weak credentials** for remote access

Eleven11bot spreads by brute-forcing weak or default credentials and scanning for exposed Telnet and SSH ports. Attackers gain control of devices using common login credentials, allowing them to deploy malware and launch DDoS attacks. The botnet appears to specifically target HiSilicon-based IoT devices, many of which use the TVT-NVMS9000 software platform.

Some early infection reports overestimated the botnet's size due to misidentified HiSilicon traffic, but researchers confirm that a significant number of devices remain compromised and actively participating in attacks. For more details, review GreyNoise's full analysis on Eleven11bot.

Aspire Protects

- Update Firmware – Apply the latest patches to IoT devices.
- Change Default Credentials – Use strong, unique passwords for all devices.

- Disable Remote Access – Turn off Telnet and SSH if not needed.
- Monitor for Suspicious Activity – Watch for unauthorized login attempts and unexpected network traffic.
- Enable DDoS Protections – Use rate-limiting, firewalls, and traffic filtering to reduce risk.
- Block Malicious IPs – Review the GreyNoise report for identified Eleven11bot-related addresses.

TTPs to Watch

Initial Access
- Brute Force [T1110] – The attacker may have accessed devices by guessing weak credentials.

Execution
- Command and Scripting Interpreter [T1059] – The attacker may have executed scripts to automate exploitation.

Persistence
- Valid Accounts [T1078] – The attacker may have maintained access using stolen or default credentials.

Impact
- Network Denial of Service [T1498] – The attacker launched large-scale DDoS attacks using compromised IoT devices.

IoCs

Find a complete list of known malicious IP addresses in the link below.

- Eleven11bot

Targeted Industries

Any organization using IoT devices with weak security is at risk of exploitation. The botnet may impact the following industries/sectors:
- Finance
- Telecommunications
- Gaming
- Cloud and Hosting Providers
- Retail and E-Commerce
- Manufacturing
- Healthcare

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

DDoS - Eleven11bot Activity - LevelBlue - Open Threat Exchange

New DDoS Botnet Discovered: Over 30,000 Hacked Devices, Majority of Observed Activity Traced to Iran