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

By Noah StoneFebruary 28, 2025

Archived: 2026-04-05 13:12:13 UTC

Update (5 March 2025): Key Clarifications on Eleven11bot

Further analysis has refined the understanding of the scale and nature of Eleven11bot. Key clarifications:

Likely a Mirai Variant

- Eleven11bot is likely not a distinct botnet, but rather a Mirai variant using a single new exploit targeting HiSilicon-based devices, particularly those running TVT-NVMS9000 software.

Overestimated Infection Numbers

- While reports estimated 86,400 infections globally, the actual number of compromised devices is likely fewer than 5,000.

Misidentified Tracking Signature

- The "head[...]1111" signature, initially associated with Eleven11bot, is not malware-related but rather part of the HiSilicon SDK protocol used for remote management across white-labeled devices.

Faulty Detection Method Inflated Infection Estimates

- The reported 86K+ infections appear to be based on a misidentification of normal HiSilicon device protocol traffic as botnet activity.

How GreyNoise Identified This Activity

GreyNoise analyzed a list of 1,400 IPs provided by Censys, identifying 1,042 of them engaging in scanning and exploitation attempts. These were primarily embedded systems that typically do not initiate outbound internet communication, reinforcing their likely compromise.

While initial infection estimates were high, the activity observed in GreyNoise suggests that a subset of these devices are actively participating in Mirai-related behavior. Because these IPs are unlikely to change dynamically

(e.g., through DHCP), they may continue to be involved in future Mirai botnet activity.

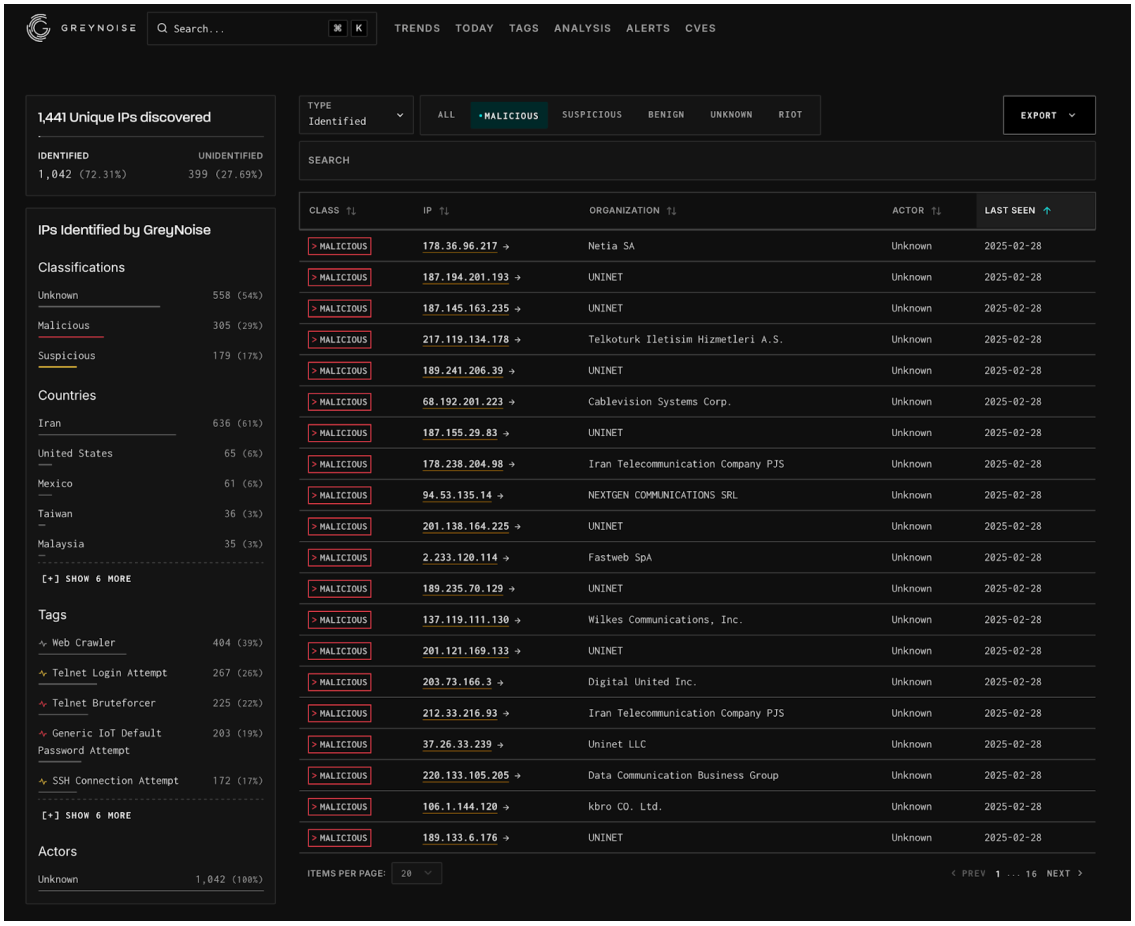
GreyNoise has developed an enhanced dynamic IP blocklist to help defenders take faster action on emerging threats. Click here to learn more about GreyNoise Block.

A newly discovered global cyber threat is rapidly expanding, infecting tens of thousands of internet-connected devices to launch powerful cyberattacks. Nokia Deepfield's Emergency Response Team (ERT) has identified a new botnet, tracked as Eleven11bot, which they estimated has compromised over 30,000 devices, primarily security cameras and network video recorders (NVRs).

According to DeepField, Eleven11bot has been used in distributed denial of service (DDoS) attacks against telecom providers and gaming platforms, with some attacks lasting multiple days and causing widespread disruptions. Jérôme Meyer, a security researcher tracking the botnet, described it as **"one of the largest known DDoS botnet campaigns observed since the invasion of Ukraine in February 2022."**

GreyNoise Observations on Eleven11bot

Following Deepfield's findings, Censys provided GreyNoise with a list of 1,400 IPs that appear to be linked to Eleven11bot due to the configuration of the endpoint devices and the banners matching what Deepfield identified in their research. **GreyNoise has observed 1,042 IPs actively hitting our sensors in the past 30 days.**



Key findings from our data:

- **96% of these IPs are non-spoofable**, meaning they originate from genuine, accessible devices.
- **61% of the 1,042 observed IPs (636) are traced to Iran.**
- **305 IPs are currently classified as malicious** by GreyNoise.

While GreyNoise does not speculate on attribution, this increase in botnet activity comes just two days after the U.S. administration reasserted its “maximum pressure” campaign on Iran, imposing new economic sanctions.

How the Botnet is Expanding

GreyNoise data indicates that the botnet is involved in malicious activities. Observations from GreyNoise show that the botnet is engaging in actions presumably aimed at expanding its operations, including:

- **Brute-force attacks** against login systems.
- **Exploitation of weak and default passwords** on IoT devices.
- **Targeting specific security camera brands**, such as VStarcam, using hardcoded credentials.
- **Network scanning for exposed Telnet and SSH ports** is often left unprotected on IoT hardware.

GreyNoise has identified 305 IP addresses actively carrying out malicious attacks linked to the botnet.

How to See the Botnet in Action

SOC teams, vulnerability management professionals, and threat hunters can **track the botnet's live activity using GreyNoise**:

1. Navigate to the Analysis feature.
2. Paste the list of botnet IPs (source: Censys) into the search bar.
3. Download the CSV of malicious IPs to **take immediate blocking actions**.

Censys-Provided IP List

A list of IPs associated with this botnet is available below:

How Organizations Can Defend Themselves

GreyNoise recommends the following steps to protect against the botnet and similar cyber threats:

- **Block traffic from known malicious IPs.** GreyNoise provides real-time data for defenders to block threats proactively.
- **Monitor network logs for unusual login attempts.** Attackers are brute-forcing weak Telnet and SSH credentials.
- **Secure IoT devices immediately.** Change default passwords, update firmware, and disable remote access where unnecessary.
- **Enable DDoS protection and rate-limiting.** The botnet is designed for high-intensity attacks, so organizations should harden their network defenses.

GreyNoise is Actively Monitoring Eleven11bot-Linked Activity

GreyNoise continues to track real-time scanning and attack activity from the botnet. We will provide further updates if new information arises.

Track the botnet in real time — see if your network is a target. **Navigate to the GreyNoise Analysis feature, paste the IPs above into the search bar, and download the CSV of malicious IPs for immediate blocking actions.**

— — —

Stone is Head of Content at GreyNoise Intelligence, where he leads strategic content initiatives that illuminate the complexities of internet noise and threat intelligence. In past roles, he led partnered research initiatives with Google and the U.S. Department of Homeland Security. With a background in finance, technology, and engagement with the United Nations on global topics, Stone brings a multidimensional perspective to cybersecurity. He is also affiliated with the Council on Foreign Relations.

This article is a summary of the full, in-depth version on the GreyNoise Labs blog.

Read the full report

Related content
