Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

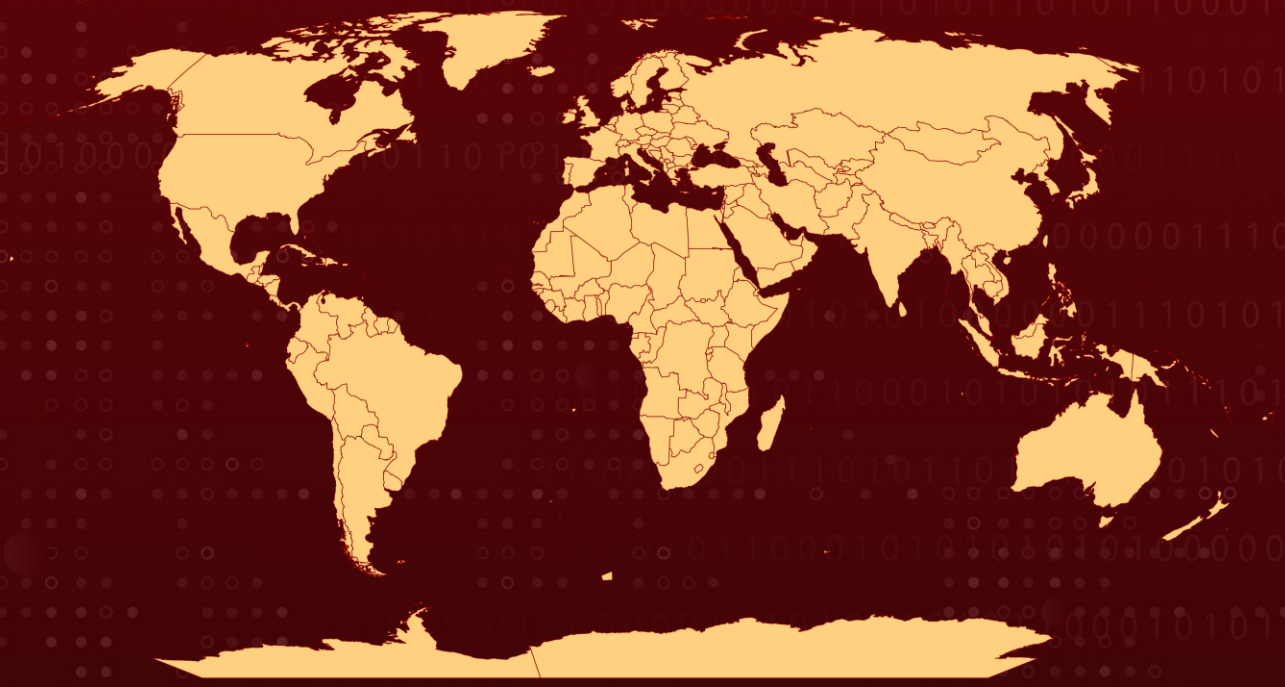
New HinataBot Go-Based Botnet with DDoS Capabilities and Mirai Connection

Date of Publication	Admiralty Code	TA Number
March 21, 2023	A1	TA2023147

Summary

First appeared: January 2023
Attack Region: Worldwide
Malware: HinataBot, Mirai
Attack: HinataBot is a newly discovered Go-based botnet that spreads through old vulnerabilities and weak credentials. It carries out DDoS flooding attacks and has a connection with the Mirai malware family.

Attack Regions



CVEs

CVE	NAME	PATCH	CISA KEV
CVE-2017-17215	Remote Code Execution Vulnerability in Huawei HG532 routers	✗	✗
CVE-2014-8361	Remote Code Execution Vulnerability in Realtek SDK	✗	✗

Attack Details

#1

HinataBot is a new Go-based botnet that was discovered by Akamai's Security Intelligence Response Team (SIRT) during the first three months of 2023. The malware appears to have been named after a character from the anime series Naruto. HinataBot has been observed being distributed through old vulnerabilities and weak credentials, and it employs various methods of communication, including both dialing out and listening for incoming connections.

#2

The botnet has been observed with distributed denial-of-service (DDoS) flooding attacks that utilize protocols such as HTTP, UDP, TCP, and ICMP to send traffic. HinataBot's infection campaigns involve a mix of infection scripts and full payloads using two primary vulnerabilities: a Hadoop YARN RCE and exploitation of a vulnerability in the miniigd SOAP service within Realtek SDK devices (CVE-2014-8361).

#3

The attackers have used multiple versions of infector scripts, which were updated over time, and have employed brute-force tactics in SSH honeypots. The HinataBot malware was distributed as Go binaries designed to run on various architectures and operating systems. The attackers behind HinataBot have been active since at least December 2022, but only began developing their own malware in mid-January 2023.

#4

HinataBot appears to follow a similar structure to some attempts to rewrite the well-known malware family Mirai in Go. The actors behind HinataBot originally distributed Mirai binaries, and the IP most recently associated with HinataBot was resolving for the domain "hihi.mirailovers.pw" as recently as February 2023.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0001 Initial Access
TA0011 Command and Control	T1021 Remote Services	T1059 Command and Scripting Interpreter	T1021.004 SSH
T1110 Brute Force	T1203 Exploitation for Client Execution	T1584 Compromise Infrastructure	T1584.005 Botnet
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1588 Obtain Capabilities	T1588.005 Exploits
T1588.006 Vulnerabilities	T1499 Endpoint Denial of Service	T1190 Exploit Public-Facing Application	T1205 Traffic Signaling

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	77[.]73[.]131[.]247 156[.]236[.]16[.]237 185[.]112[.]83[.]254
SHA256	01422e34b2114c68cdb6ce685cd2e5673bbe5652259a0c4b862d5de2824a9375 1b958fd718f1419700c53fed10807e873e8399c354877b0a3dfceac7a8581456 8a84dc2a9a06b1fae0dd16765509f88f6f54559c36d4353fd040d02d4563f703 4aba67fdd694219ff0dff07ebd444ed154edacc00c3a61f9b661eabe811a0446 71154ad6bd1a8a79fc674c793bb82b8e7d1371eca0f909c6e4a98ef8e7f5d1da c6a7e25290677cc7b9331343166b140f2c320764a815b241747e6913b1a386d9

TYPE	VALUE
SHA256	92adfbe6aae06d7c99469aeb6551db8eee964b589f2b8774e29d987cfbd0e0d6 8eda08ce362c09b5f45772467f94d5370068c1798f78c5316f15647ac898c621 ff7638c0c893c021c3a059a21a71600249881afd84dc0d751d99db1c8edd3cac a3fac6fea9201c3c3eaae47bd95e0be93e91298e48df755409588834f9e75ac4d 9875bb9dd6d159a3b327de80e151ef7f3831c0d6833ae781490d68e426b73680 6ec35ef48ffdf9a92aa8845c336b327c280e1f20d7130ba0856540aed3233bbc C0aa34dd8dbf654d5230d4ef1db61f9befc89a0ea16cb7757edbf8a8090c9146 5643bf01e113de246575a9ec39ea12a85f9babb6ac069132ad8d1a7bfa56ed1b 845134ee7335f07b23e081f024cad5cbfc9ef453d6e2adc7970d6543292e5bcc 995681f388f5e0a405c282ae9ce22dc41f2249f0f5208254e1eec6e302d7ad7d 07326cce5325eabbe1caa2b3f8a4ab78e7913b65703c0afc3bab808441c30688 61181b4b7b7040ce4ab9c489a2b857f5a7fe8407c422327fff798f3b55e0cbe3 75c050580725279a6592eecc2b02b6fa78f5469c2f08fb1d0e2fe616beb8bf0d E3427838132b6161f10e77d0beca1beac90c63a8ccc4aabd523041aec25aab67

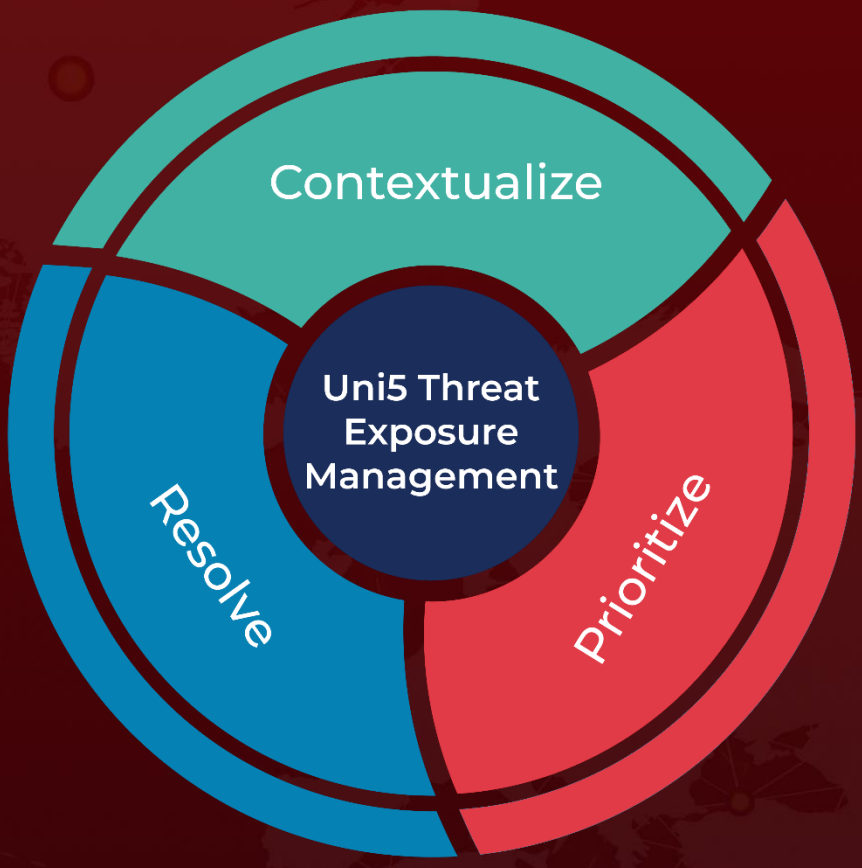
References

https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 21, 2023 • 1:30 AM

More at www.hivepro.com