Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

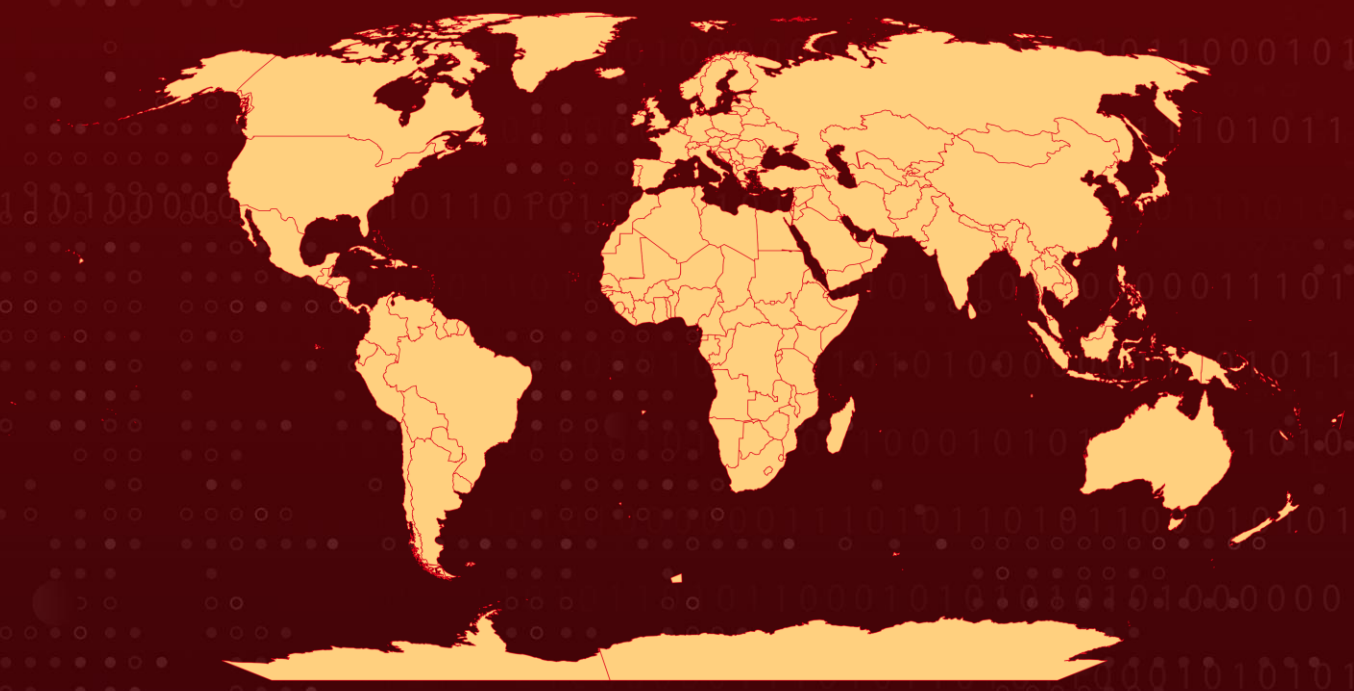
Deciphering Mirai's Next Chapter: the Strategies of the Latest Players

Date of Publication	Admiralty Code	TA Number
October 10, 2023	A1	TA2023405

Summary

Attack Began: September 2023
Malware: Mirai Botnet, hailBot, kiraiBot, and catDDoS
Attack Region: Worldwide
Targeted Industries: Financial, IoT platforms, and Trade Institutions
Attack: The realm of cybersecurity witnessed the rise of formidable botnet variants stemming from the notorious Mirai source code. Prominent among them are hailBot, kiraiBot, and catDDoS, showcasing heightened activity and a pervasive threat.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-17215	Huawei HG532 RCE Vulnerability	Huawei HG532 router: All versions	✓	✗	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office: 2007 - 2016	✗	✓	✓

Attack Details

#1 Novel iterations of botnet variants emerged in September 2023, drawing inspiration from the Mirai framework. Among them, hailBot, kiraiBot, and catDDoS have surfaced as particularly dynamic entities, rapidly proliferating and posing a substantial threat. In recent years, there has been a surge in the development of botnet Trojan horses rooted in Mirai, with numerous attackers engaging in secondary development based on its source code.

#2 One Mirai botnet variant, observed in attacks during **March** and **April 2023**, actively exploited vulnerabilities across various devices to create botnets and execute DDoS attacks. Around late January 2023, **Hinata Bot** surfaced, demonstrating a structure reminiscent of attempts to reconfigure the Mirai malware using the Go language.

#3 HailBot, derived from the Mirai source code and a modified live data packet, acquires its name from the output string 'hail china mainland' post-execution. This botnet propagates through a built-in vulnerability, CVE-2017-17215, coupled with weak password scanning and brute force. CVE-2017-17215 represents a remote code execution vulnerability in Huawei HG532 routers, previously exploited by Hinata Bot and **Zerobot**.

#4 HailBot's Command and Control (C&C) infrastructure had previously disseminated bait documents exploiting the six-year-old CVE-2017-11882 vulnerability. These documents contained files crafted to entice victims into triggering the vulnerability by opening them, resulting in the download and execution of various banking trojans oriented towards commercial espionage.

#5 CVE-2017-11882, identified as a Memory Corruption Vulnerability in Microsoft Office, had been previously employed in campaigns by **Agent Tesla** in August 2023, **NeedleDropper**, and threat actors such as **Tonto Team** and **Cloud Atlas**. KiraiBot, a recent addition to the Mirai botnet variant family, ensures persistence by configuring a self-starting script. Supporting six DDoS attack modes, kiraiBot spreads by breaching port 23 through weak password scanning.

#6 The catDDoS family innovates by introducing the ChaCha20 algorithm to encrypt and store crucial information, with its primary targets located in China and the United States, along with collateral impact in Japan, Singapore, France, and other nations. The act of repurposing code from existing malware remains a prevalent method for introducing novel variants into the threat landscape, and the Mirai source code is solidifying its legacy to enhance stealth and broaden the scope of potential targets.

Recommendations

Vulnerability Management: Regularly update and patch systems to mitigate vulnerabilities such as CVE-2017-17215 and CVE-2017-11882. Prioritize the patching of devices like Huawei HG532 routers to prevent exploitation by botnets like hailBot.

Network Monitoring and Intrusion Detection: Implement robust network monitoring and intrusion detection systems to promptly identify unusual activities indicative of botnet propagation. Specifically, monitor activities on port 23 to detect potential breaches by kiraiBot.

Network Segmentation: By implementing a strong network segmentation strategy and isolating critical systems, the lateral movement of malware is effectively restricted. This proactive approach significantly reduces the risk of malware spreading within the network, offering protection against threats like Agent Tesla.

File Integrity and Encrypted Traffic Monitoring: Implement file integrity monitoring to detect unauthorized changes to critical system files and configurations—a common tactic used by sophisticated botnets. Employ deep packet inspection for encrypted traffic to identify and block malicious payloads that may be concealed within encrypted communications.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**TA0040** Impact
T1590 Gather Victim Network Information	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1543** Create or Modify System Process
T1583.005 Botnet	**T1059** Command and Scripting Interpreter	**T1204** User Execution	**T1083** File and Directory Discovery

T1574 Hijack Execution Flow	**T1137** Office Application Startup	**T1505** Server Software Component	**T1068** Exploitation for Privilege Escalation
T1573 Encrypted Channel	**T1055** Process Injection	**T1211** Exploitation for Defense Evasion	**T1105** Ingress Tool Transfer
T1499 Endpoint Denial of Service			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	3f30a468b56c5761e346f3e709fd098e, 33ea03c6fdb4bcd826f99ca7ae8b5907, 12fe77575c11b698501e2068810823a4
SHA1	3a3f37333e298c3c6f2be18da4f5473454820d2d, 5e0f04554264dfc3eb0ed6a22a53ff8ae26a4162
SHA256	259b0c0c65f6836cc2ee8aa22da007415404231e178aabfbb4bfc11c7786f441, d619cefad993a0df9ad0ddb631159c50995f76dfd0f14b3fb334b04fce8095cd
IPv4	34.147.16[.]24, 34.165.70[.]211, 34.176.112[.]249, 34.64.52[.]239, 34.69.75[.]60, 34.92.28[.]223, 35.188.240[.]127, 5.181.80[.]115, 5.181.80[.]120, 5.181.80[.]70, 5.181.80[.]71, 179.43.155[.]231, 139.177.197[.]168, 212.118.43[.]167, 77.105.138[.]202, 84.54.47[.]93, 88.218.62[.]22, 88.218.62[.]221

Patch Link

http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

References

https://nsfocusglobal.com/mirai-botnets-new-wave-hailbot-kiraibot-catddos-and-their-fierce-onslaught/

https://www.hivepro.com/mirai-botnet-exploits-multiple-flaws-in-the-latest-campaign/

https://www.hivepro.com/tp-link-router-vulnerability-triggers-mirai-malware-infection/

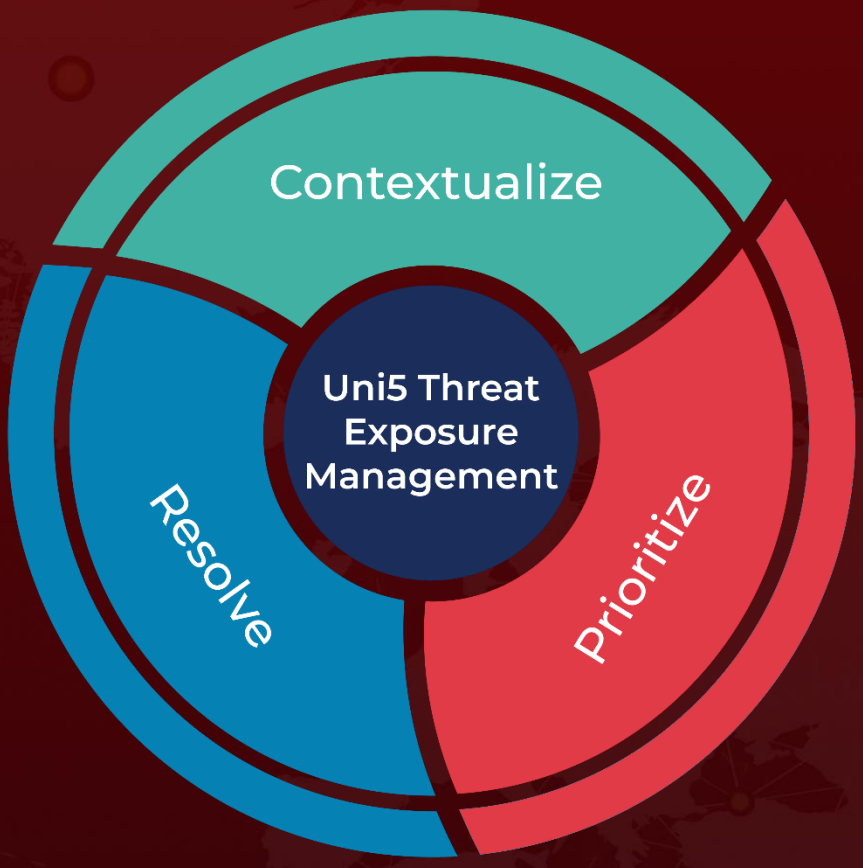
https://www.hivepro.com/new-hinatabot-go-based-botnet-with-ddos-capabilities-and-mirai-connection/

https://www.hivepro.com/new-botnet-named-zerobot-exploiting-multiple-vulnerabilities/

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

October 10, 2023 . 5:00 AM

More at www.hivepro.com