Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

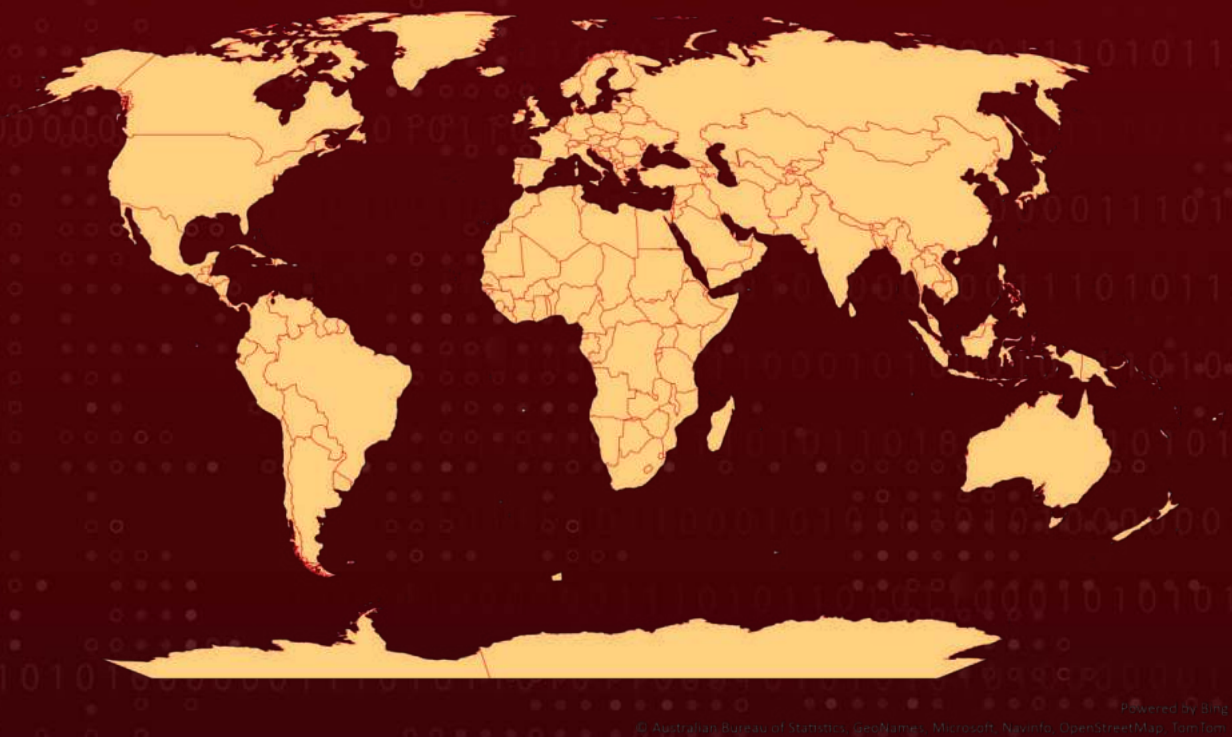
Mirai Botnet Exploits Multiple Flaws in the Latest Campaign

Date of Publication	Admiralty Code	TA Number
June 23, 2023	A1	TA2023276

Summary

Attack Began: March 2023
Malware: Mirai botnet
Attack Region: Worldwide
Attack: A new variant of the Mirai botnet is actively exploiting vulnerabilities in various devices, aiming to create botnets and launch DDoS attacks.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2019-12725	Zeroshell Remote Command Execution Vulnerability	Zeroshell versions: 3.9.0 - 3.9.0	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2019-17621	D-Link DIR-859 Remote Command Injection Vulnerability	D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01	✗	✗	✓
CVE-2019-20500	D-Link Remote Command Execution Vulnerability	D-Link DWL-2600AP 4.2.0.15	✗	✗	✓
CVE-2021-25296	Nagios OS Command Injection	Nagios XI version xi-5.7.5	✗	✓	✗
CVE-2021-46422	Telesquare Router Command Injection Vulnerability	Telesquare SDT-CW3B1 1.1.0	✗	✗	✗
CVE-2022-27002	Arris Remote Command Injection Vulnerability	Arris TR3300 v1.0.13	✗	✗	✗
CVE-2022-29303	SolarView Compact Command Injection Vulnerability	SolarView Compact version: 6.00	✗	✗	✗
CVE-2022-30023	Tenda Router Command Injection Vulnerability	Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1	✗	✗	✗
CVE-2022-30525	Zyxel Command Injection Vulnerability	Zyxel Multiple Firewalls	✗	✓	✓
CVE-2022-31499	Nortek Linear eMerge Command Injection Vulnerability	Nortek Linear eMerge E3-Series devices before 0.32-08f	✗	✗	✓
CVE-2022-37061	FLIR Unauthenticated OS Command Injection Vulnerability	All FLIR AX8 version up to and including 1.46.16	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-40005	Intelbras Command Injection Vulnerability	Intelbras WiFiber 120AC inMesh before 1-1-220826	✗	✗	✓
CVE-2022-45699	APsystems Remote Command Execution Vulnerability	APSystems ECU-R version 5203	✗	✗	✓
CVE-2023-1389	TP-Link Archer Command Injection Vulnerability	TP-Link Archer AX21	✗	✓	✓
CVE-2023-25280	D-link Command injection vulnerability	D-Link DIR820LA1_FW105B03	✗	✗	✓
CVE-2023-27240	Tenda Command Injection Vulnerability	Tenda AX3 Version: 16.03.12.11	✗	✗	✗

Attack Details

#1

Since March 2023, malicious actors have been exploiting various vulnerabilities in Internet of Things (IoT) devices to propagate a modified version of the Mirai botnet. They are exploiting multiple vulnerabilities in D-Link, Arris, Zyxel, TP-Link, Tenda, Netgear, MediaTek, and other I0T devices to gain control and use as a launchpad for distributed denial-of-service (DDoS) attacks.

#2

These threat actors take complete command over the compromised devices, turning into botnets and subsequently using them to carry out additional attacks, including DDoS attacks. The assault begins by exploiting one of the aforementioned vulnerabilities, laying the foundation for executing a shell script downloader that retrieves and executes the bot clients. These Bot Clients are platform agnostic and are capable of various Linux architectures.

#3

Compared to typical Mirai variants currently in circulation, this particular version directly accesses the encrypted strings within the .rodata section through an index. Instead of relying on a string table to acquire the configuration of the botnet client, this method bypasses the initialization of the encrypted string table. Consequently, the malware gains speed and stealthiness, making it less susceptible to detection by security tools.

#4

The TP-Link Archer Command Injection Vulnerability (CVE-2023-1389), which is also exploited by other malware like **Condi Malware**, is worth noting. It is important to mention that this Mirai variant does not possess the capability to forcefully guess telnet/SSH login credentials or exploit vulnerabilities. This implies that the sole method of spreading this variant is through manual attempts made by the botnet operator to exploit vulnerabilities.

Recommendations

- Mitigate the risk of infection by regularly updating device firmware to the latest version provided by the vendor, using strong and unique access credentials instead of default ones, and disabling remote admin panel access if not essential.
- Identify potential botnet malware infections on IoT devices by being vigilant for signs such as abnormal overheating, changes in settings or configuration, frequent disconnections, and a noticeable decline in overall performance. Promptly investigate and address any suspicious activity to prevent further damage.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**TA0040** Impact
T1543.002 Systemd Service	**T1070** Indicator Removal	**T1070.004** File Deletion	**T1543** Create or Modify System Process

T1564 Hide Artifacts	**T1564.001** Hidden Files and Directories	**T1082** System Information Discovery	**T1518** Software Discovery
T1518.001 Security Software Discovery	**T1571** Non-Standard Port	**T1584** Compromise Infrastructure	**T1584.005** Botnet
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1499** Endpoint Denial of Service	**T1059** Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	888f4a852642ce70197f77e213456ea2b3cfca4a592b94647827ca45adf2a5b8 b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c b45142a2d59d16991a38ea0a112078a6ce42c9e2ee28a74fb2ce7e1edf15dce3 366ddbaa36791cdb99cf7104b0914a258f0c373a94f6cf869f946c7799d5e2c6 413e977ae7d359e2ea7fe32db73fa007ee97ee1e9e3c3f0b4163b100b3ec87c2 2d0c8ab6c71743af8667c7318a6d8e16c144ace8df59a681a0a7d48affc05599 4cb8c90d1e1b2d725c2c1366700f11584f5697c9ef50d79e00f7dd2008e989a0 461f59a84ccb4805c4bbd37093df6e8791cdf1151b2746c46678dfe9f89ac79d aed078d3e65b5ff4dd4067ae30da5f3a96c87ec23ec5be44fc85b543c179b777 0d404a27c2f511ea7f4adb8aa150f787b2b1ff36c1b67923d6d1c90179033915 eca42235a41dbd60615d91d564c91933b9903af2ef3f8356ec4cfff2880a2f19 3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3eceec51018ef4d aaf446e4e7bfc05a33c8d9e5acf56b1c7e95f2d919b98151ff2db327c333f089 4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b

TYPE	VALUE
Domain	zvub[.]us
IPV4	185[.]225[.]74[.]251 185[.]44[.]81[.]114 193[.]32[.]162[.]189

Patch Links

https://www.zeroshell.org/download/

https://www.dlink.com/en/security-bulletin

https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls

https://na.niceforyou.com/solutions/access-control/

https://www.flir.com/products/ax8-automation/

https://seclists.org/fulldisclosure/2022/Dec/13

https://github.com/0xst4n/APSystems-ECU-R-RCE-Timezone

https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware,
https://www.fortiguard.com/encyclopedia/ips/52742

https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20Inject%20in%20pingV4Msg

References

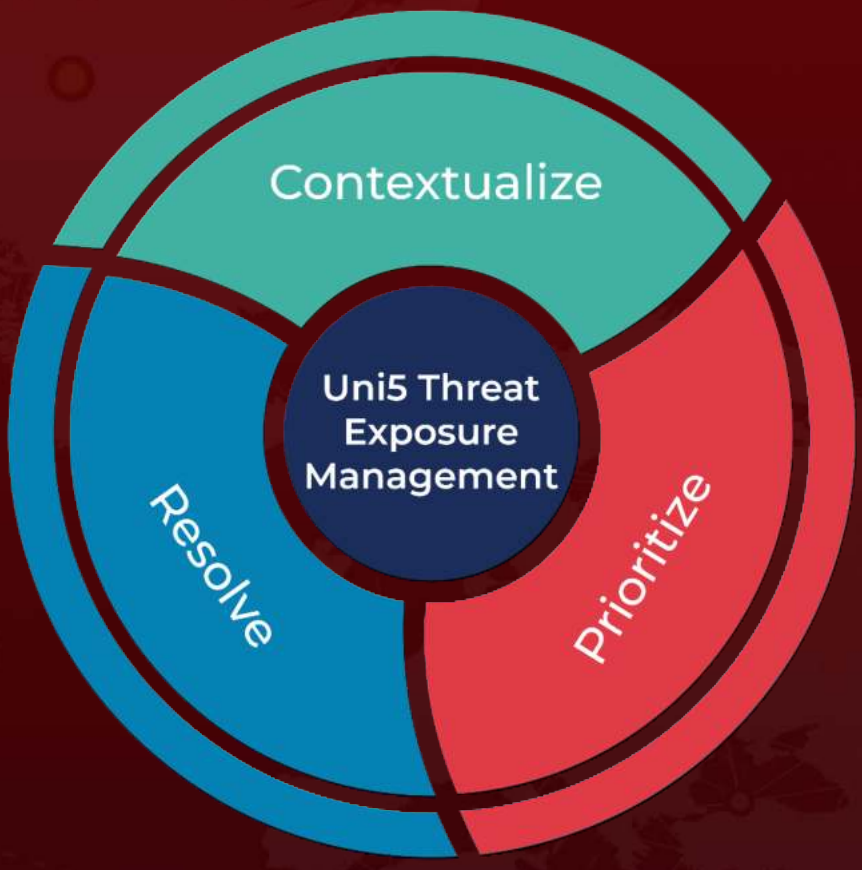
https://unit42.paloaltonetworks.com/mirai-variant-targets-iot-exploits/

https://www.hivepro.com/condi-malware-strikes-tp-link-routers-for-ddos-rampage/

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

June 23, 2023 • 8:00 AM

More at www.hivepro.com