Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

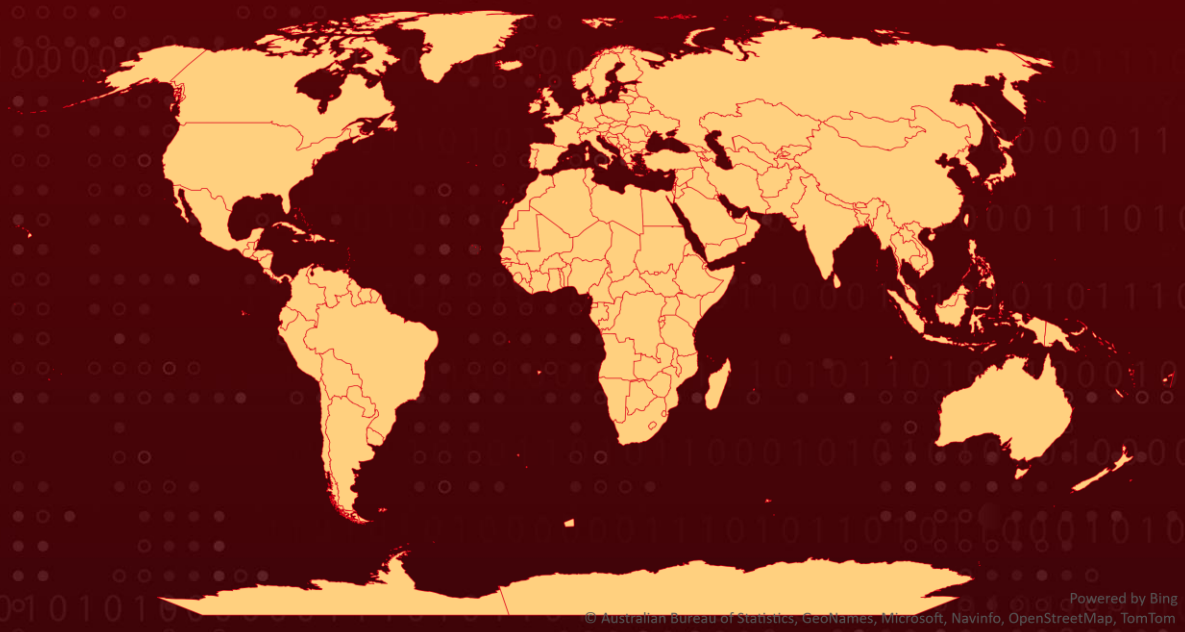
TP-Link Router Vulnerability Triggers Mirai Malware Infection

Date of Publication	Admiralty Code	TA Number
May 3, 2023	A1	TA2023208

Summary

Attack began: April 2023
Attack Regions: Worldwide
Malware: Mirai Botnet
Attack: The TP-Link router vulnerability allows attackers to execute commands and infect devices with the Mirai malware, which uses XOR encryption keys and imitates legitimate traffic to evade detection.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-1389	TP-Link Archer AX-21 Command Injection Vulnerability	TP-Link Archer AX21	✗	✓	✓

Attack Details

#1 The TP-Link router has a security flaw that lets attackers execute commands on it. Although the vulnerability was patched in March, attackers are already exploiting it with Mirai malware to control and infect devices. Attackers use a brute-force method to find the right payload for the targeted system architecture, which lets them execute code on the router and connect with the Mirai command and control servers.

#2 They make it harder to detect and stop the attack by encrypting strings with XOR keys of 0x00 and 0x22. The unencrypted strings reveal the Mirai bot attack functions, such as the TSource Engine Query attack functionality, User-Agent strings, and server headers like cloudflare-nginx and dosarrest. These allow the bot to imitate legitimate traffic.

Recommendations

- Update your TP-Link router's firmware to the latest version to ensure that the vulnerability has been patched and that your device is not exposed to the Mirai malware.
- Change the default password of your TP-Link router to a strong and unique one. This will help to prevent attackers from using a brute-force method to gain access to your router.
- Monitor your router's network activity and look out for any suspicious activity or connections to unknown IP addresses. If you suspect that your device has been compromised, reset your router to its factory settings and change your login credentials immediately.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1518 Software Discovery	T1518.001 Security Software Discovery
T1543 Create or Modify System Process	T1543.002 Systemd Service	T1070 Indicator Removal	T1070.004 File Deletion
T1564 Hide Artifacts	T1564.001 Hidden Files and Directories	T1082 System Information Discovery	T1571 Non-Standard Port

Indicators of Compromise (IOCs)

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

TYPE	VALUE
SHA256	aaf446e4e7bfc05a33c8d9e5acf56b1c7e95f2d919b98151ff2db327c333f089 4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b
URLs	http[://]185[.]225[.]74[.]251/armv4l http[://]185[.]225[.]74[.]251/armv5l http[://]185[.]225[.]74[.]251/armv6l http[://]185[.]225[.]74[.]251/armv7l http[://]185[.]225[.]74[.]251/mips http[://]185[.]225[.]74[.]251/mipsel http[://]185[.]225[.]74[.]251/sh4 http[://]185[.]225[.]74[.]251/x86_64 http[://]185[.]225[.]74[.]251/i686 http[://]185[.]225[.]74[.]251/i586 http[://]185[.]225[.]74[.]251/arc http[://]185[.]225[.]74[.]251/m68k http[://]185[.]225[.]74[.]251/sparc
Domain	zvub[.]us
IPV4	185[.]225[.]74[.]251

Patch Link

https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware

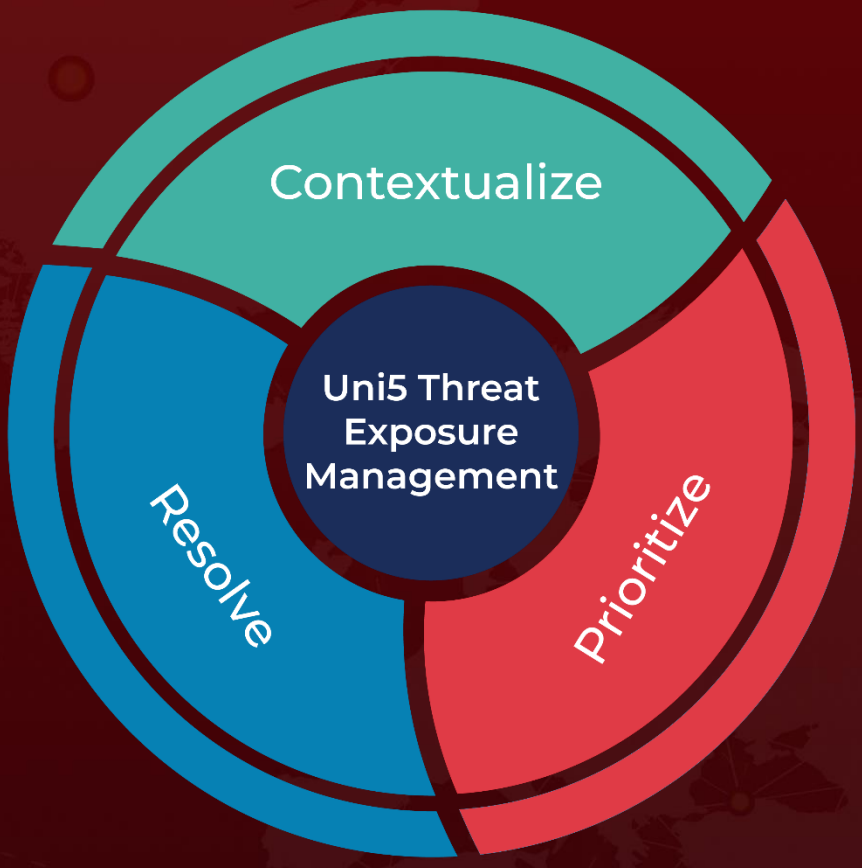
References

https://www.zerodayinitiative.com/blog/2023/4/21/tp-link-wan-side-vulnerability-cve-2023-1389-added-to-the-mirai-botnet-arsenal

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

May 3, 2023 • 6:45 AM

More at www.hivepro.com