Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

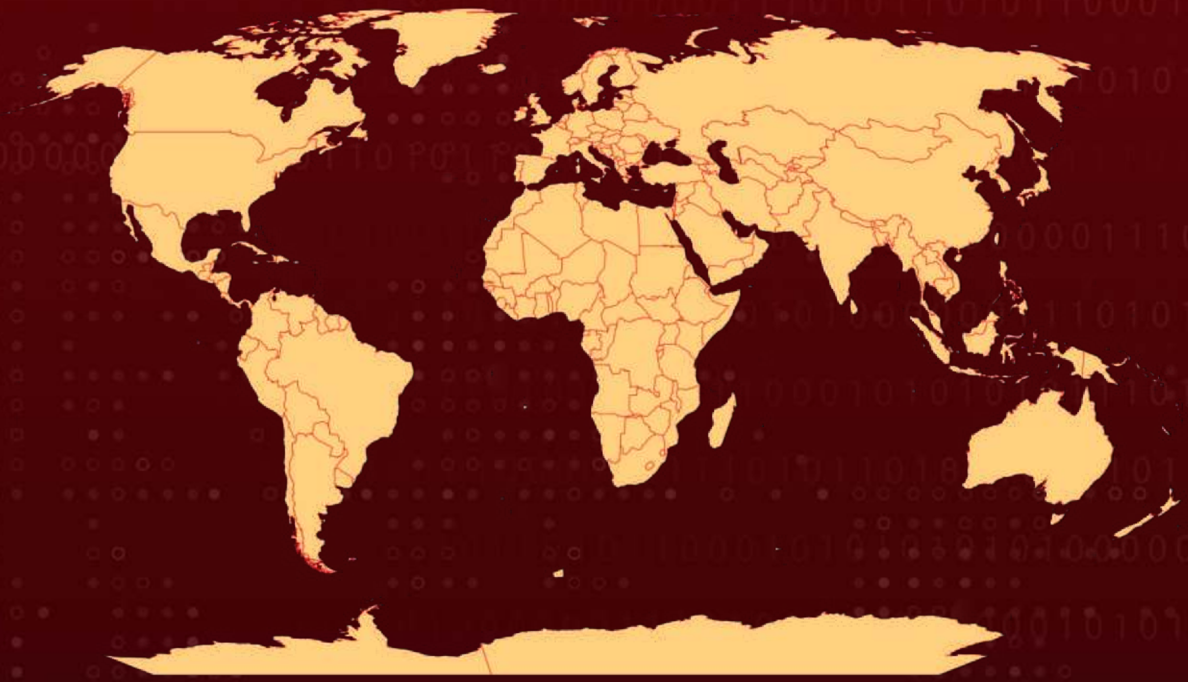
Condi Malware Strikes TP-Link Routers for DDoS Rampage

Date of Publication	Admiralty Code	TA Number
June 21, 2023	A1	TA2023273

Summary

First appeared: May 2023
Malware: Condi Botnet
Attack Region: Worldwide
Targeted Platforms: IoT, Routers
Attack: Condi, a recently discovered malware, utilizes a security vulnerability within TP-Link Archer Wi-Fi routers to ensnare these devices into a botnet specifically designed for launching distributed denial-of-service (DDoS) attacks.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

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 versions before 1.1.4 Build 20230219	✗	✓	✓

Attack Details

#1

A recently emerged distributed denial of service (DDoS) botnet, known as Condi, is leveraging the vulnerabilities present in TP-Link Archer AX21 (AX1800) routers. It specifically focuses on exploiting the (CVE-2023-1389) Command Injection Vulnerability. Condi botnet's primary objective is to recruit additional devices, thereby establishing a powerful DDoS botnet available for rent to initiate attacks on diverse websites and services.

#2

Moreover, Condi possesses the capability to neutralize rival botnets operating on the same host. However, it lacks a persistence mechanism, which renders the program incapable of surviving a system reboot. To circumvent this limitation, the malware efficiently eradicates multiple binaries employed for system shutdown or reboot functions.

#3

Condi represents the second wave of targeted DDoS botnets exploiting the mentioned vulnerability, following **Mirai's footsteps**, which capitalized on it towards the end of April. In contrast to most DDoS botnets, Condi does not rely on the trial-and-error approach of credential testing for propagation. Instead, it utilizes a modified and straightforward scanner derived from Mirai's original Telnet scanner.

#4

This scanner actively searches for public IP addresses with open ports 80 or 8080 and proceeds to dispatch a pre-programmed exploitation request. This request aims to download and execute a remote shell script, thereby infecting vulnerable TP-Link Archer AX21 devices with Condi. The binary protocol employed by Condi to establish communication with its command-and-control (C2) server is a customized iteration of the protocol initially introduced by Mirai.

#5

The mastermind behind Condi operates under the online alias zxcr9999 on Telegram and manages a Telegram channel called Condi Network, actively promoting the Condi botnet. It is worth noting that an earlier version of Condi possesses the capability to scan for devices with an exposed Android Debug Bridge (ADB) port (TCP/5555). Hence, it is possible that the botnet is spreading through this method.

Recommendations

Implement immediate firmware updates and security patches for TP-Link Archer AX21 (AX1800) routers to mitigate the vulnerabilities targeted by Condi and protect against potential DDoS attacks.

Strengthen the security of vulnerable TP-Link routers by securing ports 80 and 8080, utilizing robust firewall configurations to prevent the malware from propagating and infecting new devices.

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
T1518 Software Discovery	T1518.001 Security Software Discovery	T1059 Command and Scripting Interpreter	T1053 Scheduled Task/Job
T1574 Hijack Execution Flow	T1543 Create or Modify System Process	T1543.002 Systemd Service	T1499 Endpoint Denial of Service
T1584 Compromise Infrastructure	T1055 Process Injection	T1057 Process Discovery	T1595 Active Scanning
T1584.005 Botnet	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	admin[.]duc3k[.]com cdn2[.]duc3k[.]com

TYPE	VALUE
SHA256	091d1aca4fcd399102610265a57f5a6016f06b1947f86382a2bf2a668912554f,291e6383284d38f958fb90d56780536b03bcc321f1177713d3834495f64a3144,449ad6e25b703b85fb0849a234cbb62770653e6518cf1584a94a52cca31b1190,4e3fa5fa2dcc6328c71fed84c9d18dfdbd34f8688c6bee1526fd22ee1d749e5a,509f5bb6bcc0f2da762847364f7c433d1179fb2b2f4828eefb30828c485a3084,593e75b5809591469dbf57a7f76f93cb256471d89267c3800f855cabefe49315,5e841db73f5faefe97e38c131433689cb2df6f024466081f26c07c4901fdf612,cbff9c7b5eea051188cfd0c47bd7f5fe51983fba0b237f400522f22ab91d2772,ccda8a68a412eb1bc468e82dda12eb9a7c9d186fabf0bbdc3f24cd0fb20458cc,e7a4aae413d4742d9c0e25066997153b844789a1409fd0aecce8cc6868729a15,f7fb5f3dc06aebcb56f7a9550b005c2c4fc6b2e2a50430d64389914f882d67cf
URLs	hxxp://85[.]217[.]144[.]35/arm hxxp://85[.]217[.]144[.]35/arm5 hxxp://85[.]217[.]144[.]35/arm6 hxxp://85[.]217[.]144[.]35/arm7 hxxp://85[.]217[.]144[.]35/m68k hxxp://85[.]217[.]144[.]35/mips hxxp://85[.]217[.]144[.]35/mpsl hxxp://85[.]217[.]144[.]35/ppc hxxp://85[.]217[.]144[.]35/sh4 hxxp://85[.]217[.]144[.]35/x86 hxxp://85[.]217[.]144[.]35/x86_64 hxxp://85[.]217[.]144[.]35/abc3.sh hxxp://cdn2[.]duc3k[.]com/t
IPV4	85[.]217[.]144[.]35

Patch Links

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

References

https://www.fortinet.com/blog/threat-research/condi-ddos-botnet-spreads-via-tp-links-cve-2023-1389

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

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.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

June 21, 2023 • 6:22 AM

More at www.hivepro.com