Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

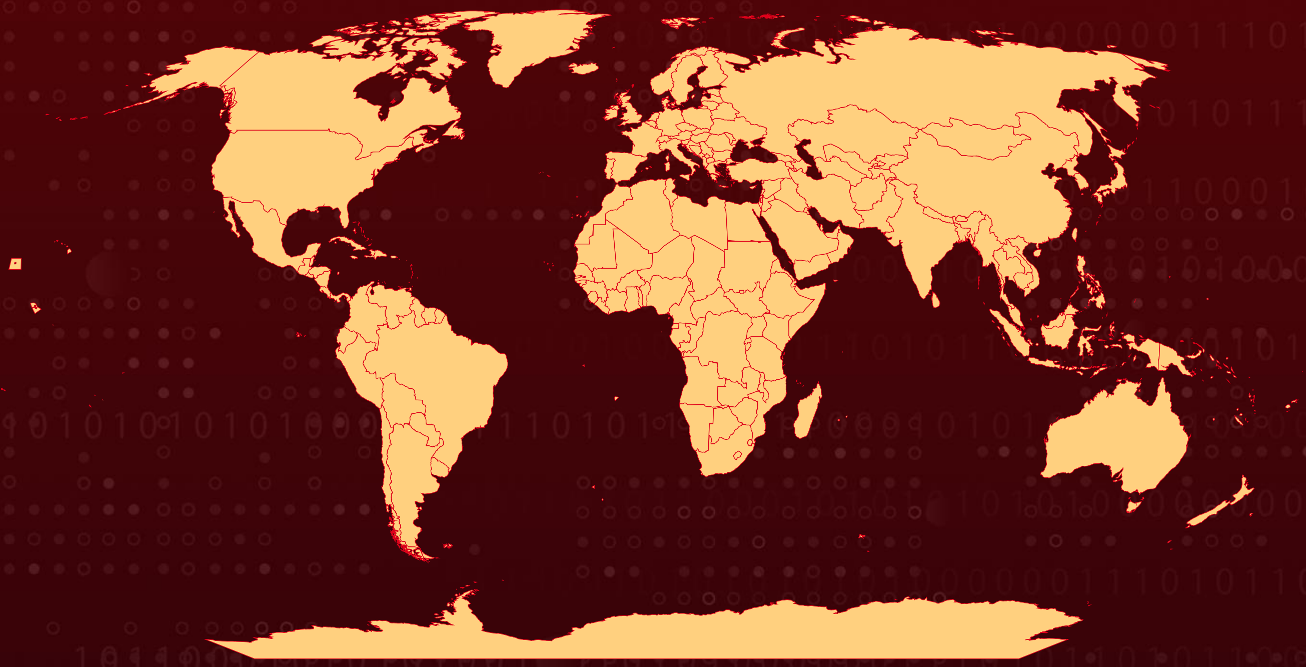
FICORA and CAPSAICIN Botnets Target Unpatched D-Link Devices

Date of Publication	Admiralty Code	TA Number
December 31, 2024	A1	TA2024478

Summary

Attack Began: October 2024
Malware: FICORA and CAPSAICIN
Targeted Countries: Worldwide
Affected Products: Multiple D-Link Routers
Attack: Recent botnet activity, particularly from FICORA (a Mirai variant) and CAPSAICIN (a Kaiten variant), targets vulnerabilities in D-Link routers via the Home Network Administration Protocol (HNAP). These botnets exploit known vulnerabilities to execute remote commands and conduct DDoS attacks. FICORA uses brute-force methods with hard-coded credentials, while CAPSAICIN focuses on East Asian countries and can eliminate competing malware. Regular firmware updates and network monitoring are crucial for mitigating these threats.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2015-2051	D-Link DIR-645 Router Remote Code Execution Vulnerability	D-Link DIR-645 Router	✗	✓	✓
CVE-2019-10891	D-Link DIR-806 Router Command Injection Vulnerability	D-Link DIR-806 Router	✗	✗	✗
CVE-2022-37056	D-Link Go-RT-AC750 Command Injection Vulnerability	D-Link Go-RT-AC750 Router	✗	✗	✗
CVE-2024-33112	D-Link DIR-845L router Command Injection Vulnerability	D-Link DIR-845L router	✗	✗	✗

Attack Details

#1

The ongoing threat of botnets exploiting outdated vulnerabilities in D-Link routers persists. These attacks primarily target routers with unpatched firmware, exploiting weaknesses in the Home Network Administration Protocol (HNAP). Two botnets, "FICORA" (a Mirai variant) and "CAPSAICIN" (a Kaiten variant), have been actively using these vulnerabilities to compromise devices globally.

#2

FICORA has demonstrated a widespread geographic impact. This botnet utilizes a shell script named "multi" to download and execute its payload through various methods, including wget, curl, ftpget, and tftp. It also incorporates brute-force capabilities with hard-coded credentials to infiltrate additional Linux-based systems. FICORA is capable of conducting distributed denial-of-service (DDoS) attacks using techniques such as UDP flooding, TCP flooding, and DNS amplification.

#3

On the other hand, CAPSAICIN exhibited a more concentrated attack pattern, primarily targeting East Asian countries during a brief but intense activity period on October 21 and 22, 2024. This botnet employs a downloader script called "bins.sh" to fetch its payload and establish a connection with its command-and-control (C2) server. Once compromised, CAPSAICIN can send system information back to the C2 server and await commands to execute various functions, including DDoS attacks.

#4

Despite these vulnerabilities being known for nearly a decade, and many having received patches, these attacks continue to pose significant risks due to the prevalence of unpatched legacy devices in use. By prioritizing regular updates and robust protection strategies, users can significantly reduce their risk of falling victim to botnet campaigns.

Recommendations

Update Firmware Regularly: Ensure your router's firmware is up-to-date to protect against known vulnerabilities. Regular updates provide critical security patches that can prevent unauthorized access. Refer to D-Link's official support page for guidance on updating your specific router model.

Enable WPA2 or WPA3 Encryption: Configure your router to use WPA2 or WPA3 encryption for wireless connections. These protocols offer robust security compared to older methods like WEP. For detailed instructions, consult D-Link's guidelines on securing wireless signals.

Disable Unused Services and Features: Turn off unnecessary services such as remote management, Universal Plug and Play (UPnP), and WPS to reduce potential attack vectors. Disabling unused features minimizes the risk of exploitation.

Monitor Network Activity: Regularly review connected devices and network traffic for any unusual activity. Early detection of unauthorized access can prevent potential security breaches.

Consider Router Replacement: If your router is an older model no longer receiving firmware updates, consider upgrading to a newer device with ongoing support. D-Link has issued warnings recommending the replacement of outdated routers to maintain network security.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0010 Exfiltration	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0003 Persistence	TA0004 Privilege Escalation	TA0011 Command and Control
TA0040 Impact	T1071.004 DNS	T1041 Exfiltration Over C2 Channel	T1027 Obfuscated Files or Information
T1059 Command and Scripting Interpreter	T1046 Network Service Discovery	T1110 Brute Force	T1095 Non-Application Layer Protocol
T1562.001 Disable or Modify Tools	T1562 Impair Defenses	T1190 Exploit Public-Facing Application	T1078 Valid Accounts
T1203 Exploitation for Client Execution	T1068 Exploitation for Privilege Escalation	T1071.001 Web Protocols	T1071 Application Layer Protocol
T1498 Network Denial of Service			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[://]103[.]149[.]87[.]69/multi, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arc, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm5, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm6, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm7, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]m68k,

TYPE	VALUE
URLs	hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]mips, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]mipsel, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]powerpc, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]sh4, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]sparc, hxxp[://]87[.]11[.]174[.]141/bins[.]sh, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]yak[.]sh, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]arm5, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]arm6, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]arm7, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]i586, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]i686, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]m68k, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]mips, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]mipsel, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]ppc, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]sparc, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]x86, hxxp[://]87[.]10[.]220[.]221/bins[.]sh, hxxp[://]87[.]10[.]220[.]221/yakuza[.]sh, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm4, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm5, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm6, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm7, hxxp[://]87[.]10[.]220[.]221/yakuza[.]i586, hxxp[://]87[.]10[.]220[.]221/yakuza[.]i686, hxxp[://]87[.]10[.]220[.]221/yakuza[.]m68k, hxxp[://]87[.]10[.]220[.]221/yakuza[.]mips, hxxp[://]87[.]10[.]220[.]221/yakuza[.]mipsel, hxxp[://]87[.]10[.]220[.]221/yakuza[.]ppc, hxxp[://]87[.]10[.]220[.]221/yakuza[.]sparc, hxxp[://]87[.]10[.]220[.]221/yakuza[.]x86
Domains	ru[.]coziest[.]lol, f[.]codingdrunk[.]cc, www[.]codingdrunk[.]in, eighteen[.]pirate, nineteen[.]libre, 75cents[.]libre, 2joints[.]libre, fortyfivehundred[.]dyn, 21savage[.]dyn, imaverygoodbadboy[.]libre, le[.]codingdrunk[.]in, pirati[.]abuser[.]eu
IPv4	87[.]11[.]174[.]141, 103[.]149[.]87[.]69, 87[.]10[.]220[.]221, 45[.]86[.]86[.]60, 194[.]110[.]247[.]46

TYPE	VALUE
SHA256	f71dc58cc969e79cb0fdfe5163fbb9ed4fee5e13cc9407a11d231601ee4c6e23, ea83411bd7b6e5a7364f7b8b9018f0f17f7084aeb58a47736dd80c99cfeac7f1, 48a04c7c33a787ef72f1a61aec9fad87d6bd9c49542f52af7e029ac83475f45d, 18c92006951f93a77df14eca6430f32389080838d97c9e47364bf82f6c21a907, 9b161a32d89f9b19d40cd4c21d436c1daf208b5d159ffe1df7ad5fd1a57610e5, faeea9d5091384195e87caae9dd88010c9a2b3b2c88ae9cac8d79fd94f250e9f, 10d7aedc963ea77302b967aad100d7dd90d95abcdb099c5a0a2df309c52c32b8, 7f6912de8bef9ced5b9018401452278570b4264bb1e935292575f2c3a0616ec4, a06fd0b8936f5b2370db5f7ec933d53bd8a1bf5042cdc5c052390d1ecc7c0e07, 764a03bf28f9eec50a1bd994308e977a64201fbe5d41337bdcc942c74861bcd3, df176fb8cfbc7512c77673f862e73833641ebb0d43213492c168f99302dcd5e3, ac2df391ede03df27bcf238077d2dddcde24cd86f16202c5c51ecd31b7596a68, ca3f6dce945ccad5a50ea01262b2d42171f893632fc5c5b8ce4499990e978e5b, afee245b6f999f6b9d0dd997436df5f2abfb3c8d2a8811ff57e3c21637207d62, ec508df7cb142a639b0c33f710d5e49c29a5a578521b6306bee28012aadde4a8, 8349ba17f028b6a17aaa09cd17f1107409611a0734e06e6047ccc33e8ff669b0, b3ad8409d82500e790e6599337abe4d6edf5bd4c6737f8357d19edd82c88b064, ec87dc841af77ec2987f3e8ae316143218e9557e281ca13fb954536aa9f9caf1, 784c9711eadceb7fedf022b7d7f00cff7a75d05c18ff726e257602e3a3ccccc1, bde6ef047e0880ac7ef02e56eb87d5bc39116e98ef97a5b1960e9a55cea5082b, c7be8d1b8948e1cb095d46376ced64367718ed2d9270c2fc99c7052a9d1ffed7, 4600703535e35b464f0198a1fa95e3668a0c956ab68ce7b719c28031d69b86ff, 6e3ef9404817e168c974000205b27723bc93abd7fbf0581c16bb5d2e1c5c6e4a, 32e66b87f47245a892b102b7141d3845540b270c278e221f502807758a4e5dee,

TYPE	VALUE
SHA256	540c00e6c0b53332128b605b0d5e0926db0560a541bb13448d094764844763df, b74dbd02b7ebb51700f3c5900283e46570fe497f9b415d25a029623118073519, 148f6b990fc1f1903287cd5c20276664b332dd3ba8d58f2bf8c26334c93c3af5, 464e2f1faab2a40db44f118f7c3d1f9b300297fe6ced83fabe87563fc82efe95, b699cd64b9895cdcc325d7dd96c9eca623d3ec0247d20f39323547132c8fa63b, 1007f5613a91a5d4170f28e24bfa704c8a63d95a2b4d033ff2bff7e2fe3dcffe, 7a815d4ca3771de8a71cde2bdacf951bf48ea5854eb0a2af5db7d13ad51c44ab, d6a2a22000d68d79caeae482d8cf092c2d84d55dccee05e179a961c72f77b1ba, 7ab36a93f009058e60c8a45b900c1c7ae38c96005a43a39e45be9dc7af9d6da8, 803abfe19cdc6c0c41acfeb210a2361cab96d5926b2c43e5eb3b589a6ed189ad, 7b29053306f194ca75021952f97f894d8eae6d2e1d02939df37b62d3845bfdb7, 59704cf55b9fa439d6f7a36821a50178e9d73ddc5407ff340460c054d7defc54, aaa49b7b4f1e71623c42bc77bb7aa40534bcb7312da511b041799bf0e1a63ee7, 1ca1d5a53c4379c3015c74af2b18c1d9285ac1a48d515f9b7827e4f900a61bde

Patch Details

The vulnerabilities CVE-2019-10891, CVE-2022-37056, and CVE-2024-33112 affect D-Link devices that have reached End of Life (EOL) or End of Service Life (EOS); as a result, D-Link no longer provides firmware updates or security patches for these products.

Patch Link for CVE-2015-2051:
http://securityadvisories.dlink.com/security/publication.aspx?name=SAP10051

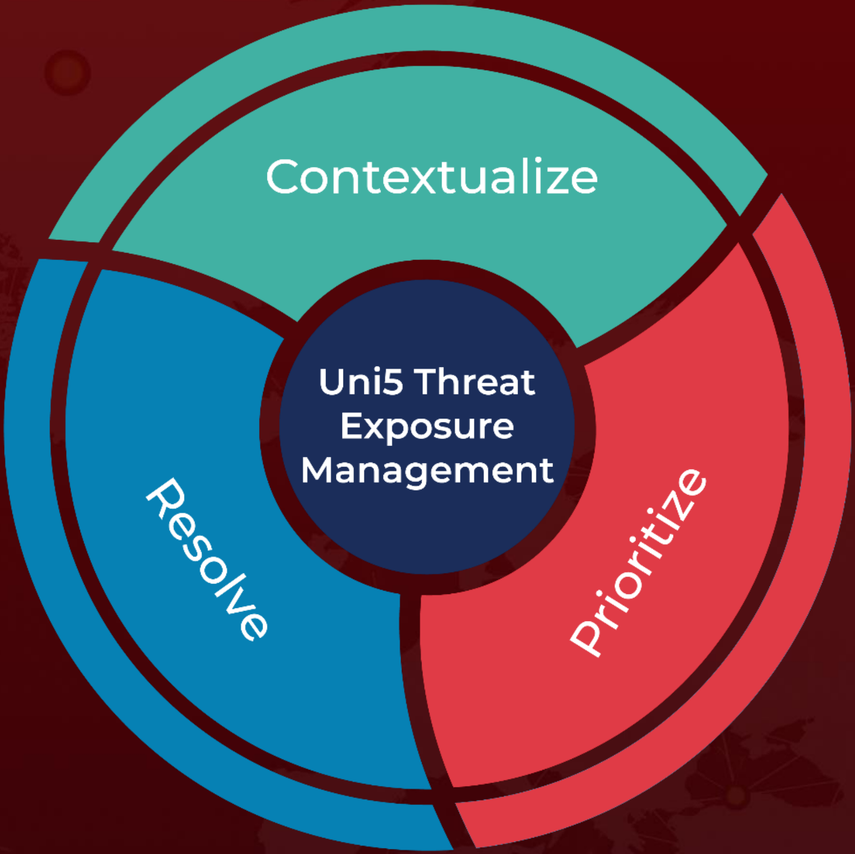
References

https://www.fortinet.com/blog/threat-research/botnets-continue-to-target-aging-d-link-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

Decmber 31, 2024 • 07:00 AM

More at www.hivepro.com