Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

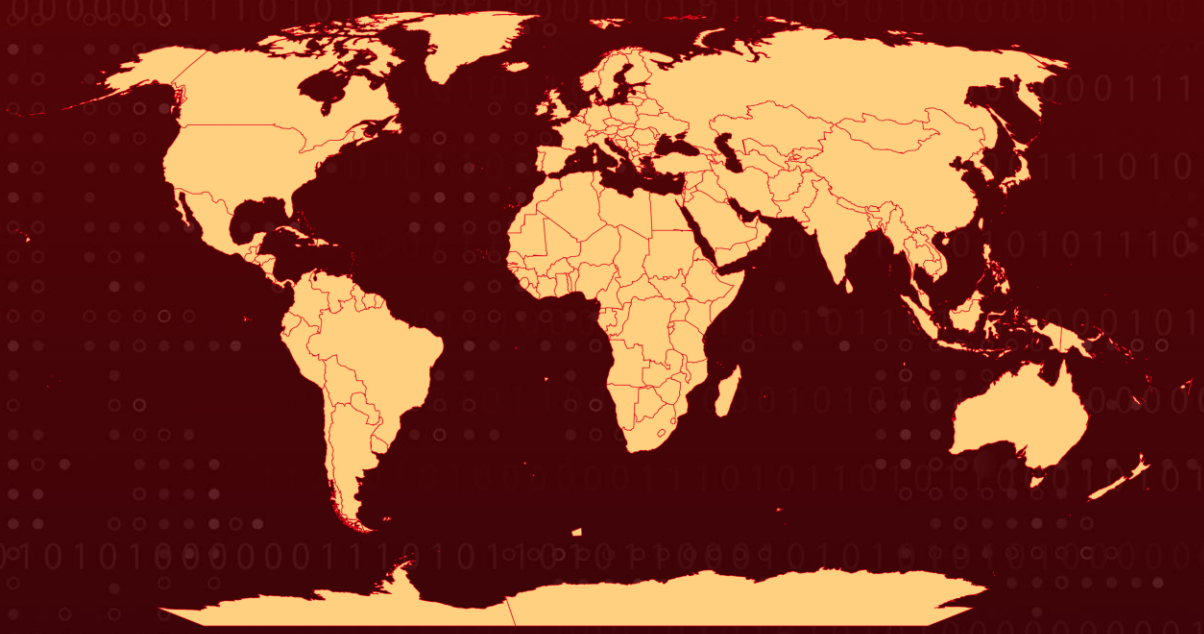
Goldoon Botnet Exploits Longstanding D-Link Vulnerability

Date of Publication	Admiralty Code	TA Number
May 2, 2024	A1	TA2024170

Summary

Attack Commenced: April 2024
Malware: Goldoon Botnet
Attack Region: Worldwide
Attack: A recently surfaced Goldoon botnet is exploiting a vulnerability in D-Link systems dating back a decade, identified as CVE-2015-2051. This flaw empowers remote attackers to execute arbitrary commands, granting them control over compromised devices. Consequently, they can extract system information and establish communication with a central server, thereby facilitating additional attacks such as DDoS.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2015-2051	D-Link DIR-645 Router Remote Code Execution Vulnerability	Dir-645: All versions	✗	✓	✓

Attack Details

#1 A new Goldoon botnet has been identified as exploiting a long-standing vulnerability in D-Link systems, specifically CVE-2015-2051, which dates back nearly a decade. This flaw permits remote attackers to wield arbitrary commands, thereby affording them the capability to embed malicious commands within a meticulously crafted HTTP request header.

#2 Initially, the attackers leverage CVE-2015-2051 to deploy a "dropper" file, a script engineered to autonomously download, execute, and sanitize potentially malicious files across diverse Linux system architectures. Subsequently, Goldoon is promptly executed following its download and permission adjustments. Once executed, the script meticulously eradicates traces of its activity by removing the executed file and self-deleting.

#3 Upon successful compromise of a targeted device, assailants can wield absolute control, facilitating the extraction of vital system information, the establishment of communication channels with a centralized C2 server, and subsequent utilization of these compromised devices to propagate further attacks, such as distributed denial-of-service (DDoS) attacks.

#4 The malware exhibits a capacity to auto-execute via Linux booting initialization files or applications. Persistently, the Goldoon malware endeavors to establish connections with its designated C2 server until a successful link is established. Notably, Goldoon possesses the capability to orchestrate Denial-of-Service (DoS) attacks across conventional protocols.

Recommendations

Network Filtering: Implement network filtering rules to block access to known malicious IP addresses associated with the Goldoon botnet. Specifically, block access to the IP address "94[.]228[.]168[.]60" on port 8080, as it is used for distributing the Goldoon dropper.

Patch and Update: Immediately apply patches and updates to all D-Link devices to address the CVE-2015-2051 vulnerability. Regularly check for firmware updates from D-Link's official website.

Monitor and Analyze Traffic: Continuously monitor network traffic for any signs of suspicious activity, such as attempts to connect to known C2 servers or unusual patterns of outbound traffic. Analyze this traffic to identify and mitigate potential threats.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
TA0042 Resource Development	T1498 Network Denial of Service	T1133 External Remote Services	T1588.006 Vulnerabilities
T1496 Resource Hijacking	T1055 Process Injection	T1546 Event Triggered Execution	T1016 System Network Configuration Discovery
T1082 System Information Discovery	T1547 Boot or Logon Autostart Execution	T1057 Process Discovery	T1059 Command and Scripting Interpreter
T1219 Remote Access Software	T1018 Remote System Discovery	T1041 Exfiltration Over C2 Channel	T1562.001 Disable or Modify Tools
T1588 Obtain Capabilities	T1562 Impair Defenses	T1070.004 File Deletion	T1070 Indicator Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	94[.]228[.]168[.]60
SHA256	66f21251d7f8c58316f149fec104723beb979a1215ad4e788d83f0ee6fd34696,

TYPE	VALUE
SHA256	712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c, d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee, fdf6dae772f7003d0b7cdc55e047434dbd089e0dc7664a3fae8ccfd9d10ece8c, aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf, fc44018b7432d9e6a1e98f723b0402101fa6e7483d098b10133aac142c0a4a0b, e7b78f16d0dfc91b4c7e8fd50fc31eba1eb22ec7030af9bf7c551b6019c79333, 0e6eb17664943756cab434af5d94fcd341f154cb36fc6f1ef5eb5cfdce68975f, 9af8720766c5f3978718c026c2263801b08634443c93bd67022c56c6ef531ef3, df71219ba6f5835309479b6e3eaca73b187f509b915420656bfe9a9cc32596c2, 48130a7c09a5c92e15b3fc0d2e1eb655e0bd8f759e01ba849f7734e32dbc2652, 8eb9c1eaecd0dcdd242e1bc8c62a1052915b627abe2de8ce147635fb7da3bfcc, b050a1ff0d205f392195179233493ff5b6f44adc93fe0dba1f78c4fe90ebcc46, ffd2d3888b6b1289e380fa040247db6a4fbd2555db3e01fadd2fe41a0fa2debc, 88cea61218bdeea94537b74c67873e75b8ada6d050a30d311569c3118d161c46, 115e15fbee077a9e126cc0eb349445df34cc9404245520c702fadc5f75b6f859, b10e47db989e29ace6c23ed15e29f313993f95e5e615711060881dfa84618071, 037331ab84a841b9d3cfb6f8797c1695e2dc0a2cdcc3f8f3c794dfaa50bcf0df, 5631980fab33525f4de1b47be606cd518403f54fa71b81186f02dbf7e9ed0004, 246142a5e3f3d3f84d8b38f98ff6897b03628e06e31016b8fafc9eb8c2b6201d, 3123a458a6346fd14c5bd7d41cda6c9c9bdabc786366a9ab3d5e7c00132ff835, 45bf2c9c6628d87a3cb85ee78ae3e92a09949185e6da11c41e2df04a53bb1274, c81cfe4d3b98d0b28d3c3e7812beda005279bc6c67821b27571240eba440fa49

Patch Link

https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

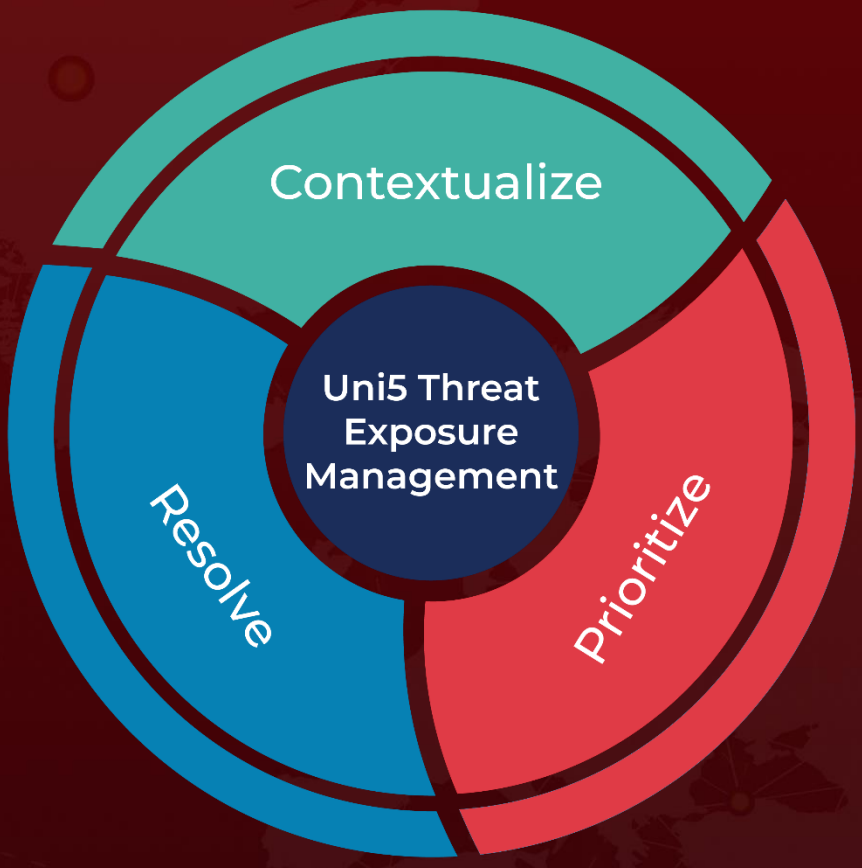
References

https://www.fortinet.com/blog/threat-research/new-goldoon-botnet-targeting-d-link-devices

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 2, 2024 • 5:00 AM

More at www.hivepro.com