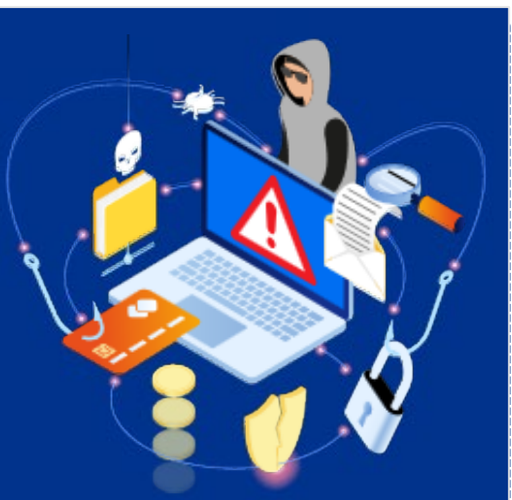
KPMG Cyber Threat Intelligence Platform

Goldoon Botnet – Exploiting Vulnerabilities in D-Link Devices



Goldoon, a newly identified botnet, has been observed exploiting a nearly decade old critical security flaw, CVE-2015-2051, with a CVSS score of 10, targeting D-Link DIR-645 routers. This vulnerability facilitates remote attackers in executing commands via tailored HTTP requests. Goldoon records information about the compromised systems and is used by attackers to conduct DDoS attacks, effectively leveraging the compromised devices for malicious operations.

Attackers exploit CVE-2015-2051 in D-Link devices by sending a crafted HTTP request with embedded commands to the HNAP interface, allowing remote execution of arbitrary commands. The exploited device downloads a dropper script from a remote server. The dropper script executes upon download, adjusts file permissions for subsequent files, and deletes itself after execution to remove traces. The dropper targets various Linux architectures to deploy the main botnet binary "goldoon," which also performs self-cleanup to remain hidden. The downloader decrypts necessary strings with an XOR key, constructs the URI for the final payload, uses a fixed User-Agent, and modifies files to further obscure its presence. Goldoon configures network settings using "WolfSSL" and Google DNS, and establishes persistence by altering boot files, creating a daemon service "goldoon.server," and ensuring execution at logon. Goldoon continuously connects to its C2 server, logs system info, and awaits commands to execute via /bin/bash -c. Goldoon engages in multiple Denial of Service attacks, such as TCP SYN flooding. It collects target information and uses various packets and protocols to execute the attacks.

Goldoon exploiting a decade-old bug highlights the evolving nature of botnets, emphasizing the need for mitigation strategies to protect devices from such persistent threats.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Goldoon Botnet – Exploiting Vulnerabilities in D-Link Devices

Indicators of Compromise: IP Addresses
94.228.168[.]60

Indicators of Compromise: Hashes
dec08165d1c46622e70d3a15e8bd6029
b85a47d2492497e2bf78608c80978ba9
0cd08a7b8c12b5c0effed00f48a7df9b
65528e0e1492411f5b5c96c9210abd9b
154c92fe21a8858cecceb2d3e438e103f
7a17a66d8cbcaf9dfcc293a9d4bcd857
a589c38a2f156302c441cb56987c5479
bbdb76cce040da000c90e426d65c41e5
8f4a8ac9a41f6e1f8f598512943ee691
0f5008ebdd8077e397817f67ea4315ea
01ad2bf6c06f3fbbacfde0e845eebacb
0c5c418d2f6a626c788728d532c34803
4a5b1f003594a21ee449d8f639f5f098
616172fc2252d3d14db4a1273393be41
175e87d023447468fd2bf3d8fc5bd322
50faee5e4f9290c9f3a86bc4b20dc5f6
3b9ffa2f45ae43d6ec18adfc36e941be
89093647cc1256e8f03474f7f0321888
931d7b7f5c9649ccafb9fceebf8fe6a2
a642faa69c40a8e22a439e6717dded98
c05f755dac3a6d8954ac9295a88509a6da003d1a
4956ed591a4929a0988fb2e66898c9dbd014bc3f
285d450027bf8b46eef221ab6927bc959489b08f
998c4465175e6b95b1d0bd0cb69eb3d29b4e763f
f6811f6845d8af402b218cfa3ae9e7afb71f121b
a90883d3cdfaf555ee0fcca2dff78c97e03ea386
e94bf6eb04f2c023a08d160b23cac42fbdd816c1
378a0f405e3115400c06b36d499e202993ad9eab
2a19574c0125d41f0d2efff6d93ec29ab12f07b4
b1647a0799182a755ea5205677e907c541f8c736

KPMG

KPMG Cyber Threat Intelligence Platform

Goldoon Botnet – Exploiting Vulnerabilities in D-Link Devices

Indicators of Compromise: Hashes
944a1e45e4994259d886421e220d1a84bc280489
81e6eaaa20c745e8c85beedc821c6bea5deee8fa
d8b8c637b7c6fdbd49fd3cab6adf2cc3e03e45d6
b344d88edf9edac60aaae8e29a96e7658decb246
b7a1f8dc22518415fefd28a74a1233f261570b2d
872c0af9845de7aa9b92039b70073b3432daf3bf
ba1043529f8c5d6f6793077cf9523521a7edd626
5edf66100fde998826f676f11eb2298e5053c7ac
43fe6a58c294494c1fdf40c696a1c642ebcddcb9
1da3577958faf64745eca04e1e0807d1e70332ad
712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c
d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee
fdf6dae772f7003d0b7cdc55e047434dbd089e0dc7664a3fae8ccfd9d10ece8c
aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf
fc44018b7432d9e6a1e98f723b0402101fa6e7483d098b10133aac142c0a4a0b
e7b78f16d0dfc91b4c7e8fd50fc31eba1eb22ec7030af9bf7c551b6019c79333
0e6eb17664943756cab434af5d94fcd341f154cb36fc6f1ef5eb5cfdce68975f
9af8720766c5f3978718c026c2263801b08634443c93bd67022c56c6ef531ef3
df71219ba6f5835309479b6e3eaca73b187f509b915420656bfe9a9cc32596c2
48130a7c09a5c92e15b3fc0d2e1eb655e0bd8f759e01ba849f7734e32dbc2652
8eb9c1eaecd0dcdd242e1bc8c62a1052915b627abe2de8ce147635fb7da3bfcc
b050a1ff0d205f392195179233493ff5b6f44adc93fe0dba1f78c4fe90ebcc46
ffd2d3888b6b1289e380fa040247db6a4fbd2555db3e01fadd2fe41a0fa2debc
88cea61218bdeea94537b74c67873e75b8ada6d050a30d311569c3118d161c46
115e15fbee077a9e126cc0eb349445df34cc9404245520c702fadc5f75b6f859
b10e47db989e29ace6c23ed15e29f313993f95e5e615711060881dfa84618071
037331ab84a841b9d3cfb6f8797c1695e2dc0a2cdcc3f8f3c794dfaa50bcf0df
5631980fab33525f4de1b47be606cd518403f54fa71b81186f02dbf7e9ed0004
246142a5e3f3d3f84d8b38f98ff6897b03628e06e31016b8fafc9eb8c2b6201d
c81cfe4d3b98d0b28d3c3e7812beda005279bc6c67821b27571240eba440fa49
66f21251d7f8c58316f149fec104723beb979a1215ad4e788d83f0ee6fd34696
3123a458a6346fd14c5bd7d41cda6c9c9bdabc786366a9ab3d5e7c00132ff835
45bf2c9c6628d87a3cb85ee78ae3e92a09949185e6da11c41e2df04a53bb1274