New “Goldoon Malware” Botnet Targeting D-Link Devices

Date: 03rd May 2024 | Severity: High

Summary

The Goldoon botnet, first reported by Fortinet. The botnet primarily targets D-Link routers. Botnet targeting a D-Link vulnerability from nearly a decade ago, CVE-2015-2051, has a CVSS score of 9.8 and affects D-Link DIR-645 routers. D-Link devices to commandeer them for malicious activities, primarily Distributed Denial-of-Service (DDoS) attacks.

Attack Vectors

- D-Link DIR-645 routers and allows remote attackers to execute arbitrary commands by means of specially crafted HTTP requests. The payload is then launched on the compromised device and acts as a downloader for the Goldoon malware from a remote endpoint.
- If a targeted device is compromised, attackers can gain complete control, enabling them to extract system information, establish communication with a C2 server, and then use these devices to launch further attacks, such as distributed denial-of-service.
- DDoS flood attacks using various protocols such as DNS, HTTP, ICMP, TCP, and UDP.
- Goldoon payload adapted for different Linux system architectures, including aarch64, arm, i686, m68k, mips64, mipsel, powerpc, s390x, sparc64, x86-64, sh4, riscv64, DEC Alpha, and PA-RISC. Then, to cover its tracks, the dropper script removes the executed file and deletes itself from the system.

Indicator of compromise

INDICATOR TYPE	INDICATORS
IP	• 94[.]228[.]168[.]60
FileHash	• 0e6eb17664943756cab434af5d94fcd341f154cb36fc6f1ef5eb5cfdce68975f • 66f21251d7f8c58316f149fec104723beb979a1215ad4e788d83f0ee6fd34696 • 45bf2c9c6628d87a3cb85ee78ae3e92a09949185e6da11c41e2df04a53bb1274 • 5631980fab33525f4de1b47be606cd518403f54fa71b81186f02dbf7e9ed0004 • aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf • 712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c

	• 246142a5e3f3d3f84d8b38f98ff6897b03628e06e31016b8fafc9eb8c2b6201d • 0e6eb17664943756cab434af5d94fcd341f154cb36fc6f1ef5eb5cfdce68975f • 115e15fbee077a9e126cc0eb349445df34cc9404245520c702fadc5f75b6f859 • b050a1ff0d205f392195179233493ff5b6f44adc93fe0dba1f78c4fe90ebcc46 • 8eb9c1eaecd0dcdd242e1bc8c62a1052915b627abe2de8ce147635fb7da3bfcc • ffd2d3888b6b1289e380fa040247db6a4fbd2555db3e01fadd2fe41a0fa2debc • fc44018b7432d9e6a1e98f723b0402101fa6e7483d098b10133aac142c0a4a0b • df71219ba6f5835309479b6e3eaca73b187f509b915420656bfe9a9cc32596c2 • c81cfe4d3b98d0b28d3c3e7812beda005279bc6c67821b27571240eba440fa49 • 48130a7c09a5c92e15b3fc0d2e1eb655e0bd8f759e01ba849f7734e32dbc2652 • 9af8720766c5f3978718c026c2263801b08634443c93bd67022c56c6ef531ef3 • b10e47db989e29ace6c23ed15e29f313993f95e5e615711060881dfa84618071 • 037331ab84a841b9d3cfb6f8797c1695e2dc0a2cdcc3f8f3c794dfaa50bcf0df • e7b78f16d0dfc91b4c7e8fd50fc31eba1eb22ec7030af9bf7c551b6019c79333 • d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee • 3123a458a6346fd14c5bd7d41cda6c9c9bdabc786366a9ab3d5e7c00132ff835

Recommendation

- Network Monitoring: Implement network monitoring solutions to detect anomalous traffic, which could signal an active infection.
- Strong Firewall Rules: Limit exposure of devices like D-Link routers to the internet unless necessary.
- Stay Informed: Keep up-to-date with the latest security bulletins and patches to stay ahead of evolving threats.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/05/new-goldoon-botnet-targets-d-link.html
- https://www.fortinet.com/blog/threat-research/new-goldoon-botnet-targeting-d-link-devices
- https://www.cybersecurity-review.com/new-goldoon-botnet-targeting-d-link-devices/