Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

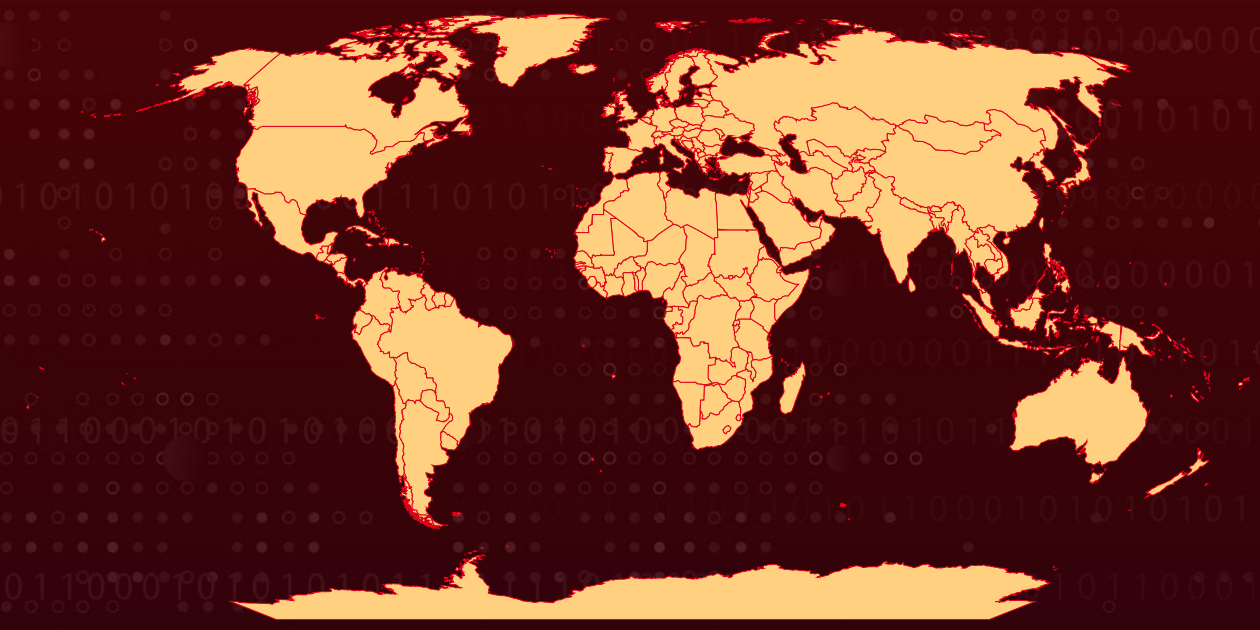
RustDuck DDoS Botnet Targeting IoT and Server Infrastructure

Date of Publication	Admiralty Code	TA Number
July 01, 2026	A1	TA2026183

Summary

First Seen: February 2026
Targeted Regions: Worldwide
Targeted Platforms: IoT devices (routers, IP cameras, DVRs), Android, Linux servers
Targeted Products: Huawei HG532, D-Link DIR-823X, Totolink X6000R, Apache CouchDB, TP-Link, ZTE, Ruijie, TVT, ThinkPHP, Jenkins, Hadoop YARN
Malware: RustDuck
Attack: RustDuck is a two-stage (Loader plus Core) botnet, active since February 2026, whose core function is large-scale distributed denial-of-service attacks. It spreads opportunistically via weak Telnet and SSH passwords, exposed Android Debug Bridge interfaces, and a mix of historical vulnerabilities in devices and web applications affecting routers, DVRs, IP cameras, and Linux servers. The core module is being migrated from C to Rust and incorporates layered anti-analysis, HKDF-SHA256 key derivation, and encrypted command-and-control channels that masquerade as ordinary TLS traffic.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-29635	D-Link DIR-823X Command Injection Vulnerability	D-Link DIR-823X	✗	✓	EOL
CVE-2017-17215	Huawei HG532 Remote Code Execution Vulnerability	Huawei HG532	✓	✗	EOL
CVE-2018-8007	Apache CouchDB Privilege Escalation Vulnerability	Apache CouchDB	✗	✗	✓
CVE-2024-1781	Totolink Command Injection Vulnerability	Totolink X6000R	✗	✗	✓

Attack Details

#1

RustDuck is a new two-stage malware family that hijacks home routers, IP cameras, Android boxes, and weakly secured servers, then links them into a network used to knock websites and online services offline. It does not rely on one trick. It uses whatever works: guessing weak passwords on exposed Telnet and SSH services, and exploiting known remote code execution and command-injection flaws in both consumer and enterprise devices.

#2

Those flaws include CVE-2017-17215 in Huawei HG532 routers, CVE-2025-29635 in D-Link DIR-823X routers, CVE-2024-1781 in Totolink X6000R routers, and CVE-2018-8007 in Apache CouchDB. It also abuses exposed Android Debug Bridge interfaces and other device flaws in TVT, Ruijie, TP-Link, and ZTE hardware. On the server side it goes after ThinkPHP, Jenkins, and Hadoop YARN, so its reach runs from cheap home devices to exposed servers. Once it lands on a host, RustDuck installs in two stages. A small loader holds the startup code, and the compressed core payload and a config block are tacked onto the end of the file. At runtime, the loader decrypts and unpacks the core.

#3

Before it runs, the core checks whether it is being watched. It works through a series of environment checks, adding to a risk score as it goes, and if that score passes a set limit it wipes its traces and quits. For command and control, it follows the IK pattern of the Noise protocol. It pairs a hardcoded server public key with a fresh runtime key in a Curve25519 exchange, then derives session keys with HKDF-SHA256 and rotates them every ten minutes.

#4

A single message ID runs through every phase to keep messages in order and help roll new keys. The handshake uses ChaCha20 encryption and a four-step sequence (login, verify, confirm, ack) that reports the host's architecture, CPU core count, and memory, and sets a unique bot ID. After the handshake, traffic switches to an AES-GCM command loop. It adds a three-byte SSL-like marker to look like normal TLS traffic and uses separate keys for sending and receiving to block man-in-the-middle interception. The C2 servers rely on free dynamic-DNS services such as duckdns.org. Operators can start or stop DDoS attacks, request status, pull new samples for a hot update, and switch to new C2 domains or IPs on the fly.

Recommendations

- **Remove Remote Management from Public Exposure:** Take Telnet, SSH, and device web-configuration interfaces off the public internet and restrict them to trusted management networks or VPN access, since exposed remote-login services are RustDuck's primary entry point.
- **Eliminate Default and Weak Credentials:** Enforce unique, strong passwords on all network-reachable devices and services and disable default accounts, because weak-password brute forcing against Telnet and SSH is a core propagation method.
- **Upgrade Apache CouchDB:** Update affected CouchDB instances to release 1.7.2 or 2.1.2 or later to remediate CVE-2018-8007, which allows an authenticated admin to escalate to remote code execution.
- **Retire End-of-Life D-Link DIR-823X Devices:** Remove DIR-823X routers from service rather than waiting for a fix; per D-Link advisory SAP10469, the model is End-of-Life and End-of-Service across all hardware revisions, and no patch will be issued for CVE-2025-29635.
- **Monitor for TLS-Masquerading Outbound Traffic:** Watch for anomalous outbound sessions that carry the SSL-like magic header but do not complete a standard TLS handshake, and for periodic beaconing to dynamic-DNS domains, to surface RustDuck C2 activity.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	T1078.001: Default Accounts
Execution	T1059: Command and Scripting Interpreter	
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
	T1622: Debugger Evasion	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1480: Execution Guardrails	
	T1036: Masquerading	
Discovery	T1082: System Information Discovery	
Credential Access	T1110: Brute Force	T1110.001: Password Guessing
Command and Control	T1071: Application Layer Protocol	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography

Tactic	Technique	Sub-technique
Command and Control	T1568: Dynamic Resolution	
	T1008: Fallback Channels	
	T1105: Ingress Tool Transfer	
Impact	T1498: Network Denial of Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	8315f650e9e4f67c00277b076ab304eed23db47d, 6aa791c76b3107fca9d57b7ecea8f46d97d83738, 4d11bd496da82d15b3ed13050f414e44f5a892d4, d39a3ee96be6b8f5238cb1253514ab55c88f714c
Domains	gayporn[.]twilightparadox[.]com, bigniggadick[.]ignorelist[.]com, ilovefemboy[.]mooo[.]com, igmc[.]duckdns[.]org, qewqewqewqtq[.]duckdns[.]org, qewqewqewqtqthree[.]duckdns[.]org, qewqewqewqtqtwo[.]duckdns[.]org, disciplinenahidwin[.]st, criminalcloudflare[.]online, dhdsjsdjxc[.]duckdns[.]org, fcfrfxrfrsfs5f[.]duckdns[.]org
IPv4	176[.]65[.]139[.]204

Patch Details

CVE-2025-29635: D-Link DIR-823X, **CVE-2025-29635 - EoL/EoS** advisory; no patch, device retirement recommended.
Link:
https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10469

CVE-2017-17215: Huawei HG532, **CVE-2017-17215 - EoL/EoS** advisory; no patch, device retirement recommended.
Link:
https://www.huawei.com/en/psirt/security-notices/2017/huawei-sn-20171130-01-hg532-en

CVE-2018-8007: fix available via upgrade to CouchDB 1.7.2 or 2.1.2
Link:
https://couchdb.apache.org/#download

CVE-2024-1781:
https://www.totolink.tw/support_view/X6000R

References

https://blog.xlab.qianxin.com/rustduck-en/

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 Demo of **HivePro**.

REPORT GENERATED ON

July 01, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com