Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

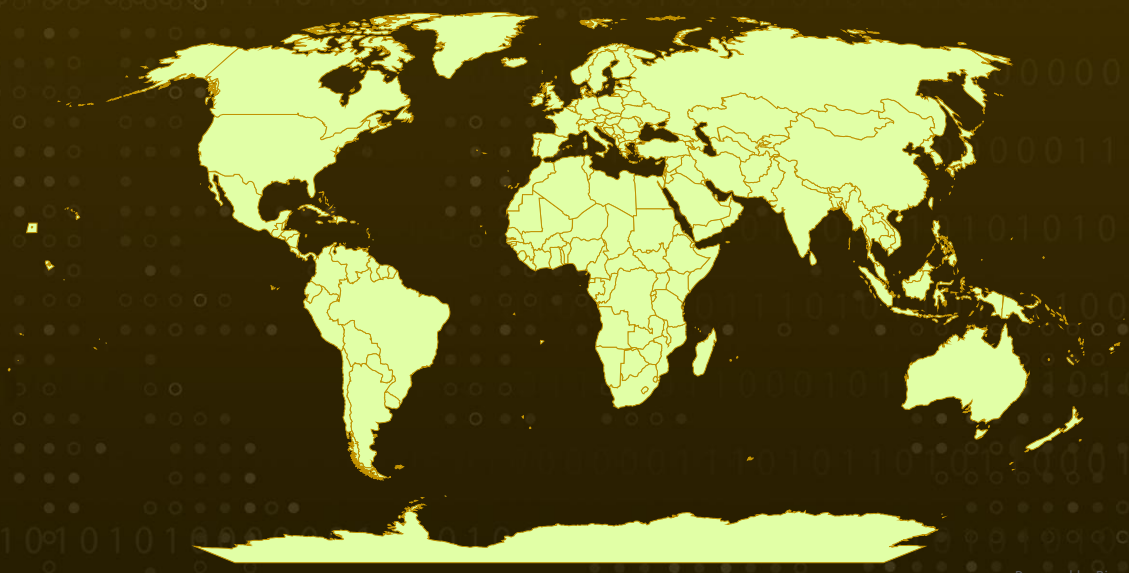
Chaos RAT: Open-Source Tool Turned Cyber Threat

Date of Publication	Admiralty Code	TA Number
June 5, 2025	A1	TA2025175

Summary

First Seen: November 2022
Targeted Region: Worldwide
Malware: Chaos RAT
Affected Platform: Windows and Linux
Targted Industry: Cryptocurrency
Attack: Chaos RAT is a cross-platform, open-source malware written in Go, originally intended for remote administration but weaponized by cybercriminals. It spreads via phishing emails and enables attackers to control infected Windows and Linux systems, steal data, and maintain persistence. Its web control panel had critical vulnerabilities, now patched, highlighting risks to both victims and attackers. Its low detection rates and adaptability make it a significant threat for espionage and ransomware operations.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-30850	CHAOS Remote Code Execution Vulnerability	CHAOS	✗	✗	✓
CVE-2024-31839	CHAOS Cross Site Scripting Vulnerability	CHAOS	✗	✗	✓

Attack Details

#1

Chaos RAT (Remote Access Trojan) is a cross-platform malware written in Go, originally released in 2022 as an open-source remote administration tool. Designed for legitimate system management, it supports both Windows and Linux platforms. However, its powerful capabilities quickly attracted cybercriminals, who weaponized the tool for malicious operations. By 2024–2025, Chaos RAT had evolved into an active global cyber threat, with increasingly sophisticated variants deployed in targeted campaigns.

#2

The malware is typically spread through phishing emails containing disguised links or attachments, often posing as network utilities for Linux environments. Once executed, Chaos RAT connects to a command-and-control (C2) server, enabling attackers to perform file management, system reconnaissance, reverse shell access, screenshot capture, and arbitrary URL execution. It maintains persistence by modifying scheduled tasks, such as the Linux /etc/crontab, and frequently updates its payloads.

#3

Recent variants focus on 64-bit platforms and remain actively maintained, with updates observed in October 2024. Its open-source availability makes it easy for threat actors to adapt and repurpose, complicating attribution and detection.

#4

Chaos RAT's web-based control panel was found to contain critical security flaws: a command injection vulnerability (CVE-2024-30850) and a cross-site scripting bug (CVE-2024-31839), both patched in May 2024. These weaknesses allowed researchers to execute code on attacker-controlled servers, highlighting the dual risk to both victims and malicious operators.

#5

The malware's low detection rates and open-source nature make it attractive for espionage, data exfiltration, and establishing persistent footholds for ransomware and other post-compromise operations. Its availability on GitHub allows threat actors to modify and repurpose it, complicating attribution and defense efforts. Chaos RAT exemplifies how legitimate open-source tools can be weaponized for cybercrime, posing significant challenges to defenders.

Recommendations

Implement Endpoint Detection and Response (EDR): Deploy EDR solutions capable of monitoring and analyzing endpoint activities to detect suspicious behaviors associated with Chaos RAT, such as unauthorized file modifications and unusual network connections.

Enhance Email Security and Awareness: Implement advanced email filtering to block phishing emails containing malicious links or attachments. Conduct regular user training to recognize phishing attempts and avoid executing unknown files or links.

Patch Vulnerabilities Promptly: Ensure all security patches and updates for software and administrative panels, including those related to Chaos RAT control infrastructure, are applied immediately to eliminate known vulnerabilities like CVE-2024-30850 and CVE-2024-31839.

Monitor Network Traffic: Regularly analyze network traffic for unusual patterns or connections to unknown command-and-control (C2) servers. This can aid in early detection of malware communications.

Restrict Administrative Privileges: Limit administrative rights to essential personnel only. This minimizes the potential impact of malware attempting to perform unauthorized actions or lateral movement within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0003 Persistence
TA0011 Command and Control	TA0010 Exfiltration	TA0009 Collection	TA0007 Discovery
T1070.004 File Deletion	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1566.001 Spearphishing Attachment

T1566 Phishing	T1566.002 Spearphishing Link	T1204.002 Malicious File	T1204 User Execution
T1053.003 Cron	T1053 Scheduled Task/Job	T1027 Obfuscated Files or Information	T1082 System Information Discovery
T1083 File and Directory Discovery	T1105 Ingress Tool Transfer	T1113 Screen Capture	T1056 Input Capture
T1070 Indicator Removal	T1529 System Shutdown/Reboot		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1e074d9dca6ef0edd24afb2d13ca4429def5fc5486cd4170c989ef60efd0bbb0, d0a63e059ed2c921c37c83246cdf4de0c8bc462b7c1d4b4ecd23a24196be7dd7, 773c935a13ab49cc4613b30e8d2a75f1bde3b85b0bba6303eab756d70f459693, c8dc86afd1cd46534f4f9869efaa3b6b9b9a1efaf3c259bb87000702807f5844, 90c8b7f89c8a23b7a056df8fd190263ca91fe4e27bda174a9c268adbfc5c0f04, 8c0606db237cfa33fa3fb99a56072063177b61fa2c8873ed6af712bba2dc56d9, 2732fc2bb7b6413c899b6ac1608818e4ee9f0e5f1d14e32c9c29982eecd50f87, 839b3a46abee1b234c4f69acd554e494c861dcc533bb79bd0d15b9855ae1bed7, 77962a384d251f0aa8e3008a88f206d6cb1f7401c759c4614e3bfe865e3e985c, 57f825a556330e94d12475f21c2245fa1ee15aedd61bffb55587b54e970f1aad,

TYPE	VALUE
SHA256	44c54d9d0b8d4862ad7424c677a6645edb711a6d0f36d6e87d7bae7a2cb14d68, c9694483c9fc15b2649359dfbd8322f0f6dd7a0a7da75499e03dbc4de2b23cad, 080f56cea7acfd9c20fc931e53ea1225eb6b00cf2f05a76943e6cf0770504c64, a583bdf46f901364ed8e60f6aadd2b31be12a27ffccecc962872bc73a9ffd46c, a364ec51aa9314f831bc498ddaf82738766ca83b51401f77dbd857ba4e32a53b, a6307aad70195369e7ca5575f1ab81c2fd82de2fe561179e38933f9da28c4850, c39184aeb42616d7bf6daaddb9792549eb354076b4559e5d85392ade2e41763e, 67534c144a7373cacbd8f9bd9585a2b74ddbb03c2c0721241d65c62726984a0a, 719082b1e5c0d18cc0283e537215b53a864857ac936a0c7d3ddbaf7c7944cf79

Patch Link

https://github.com/tiagorlampert/CHAOS/releases

References

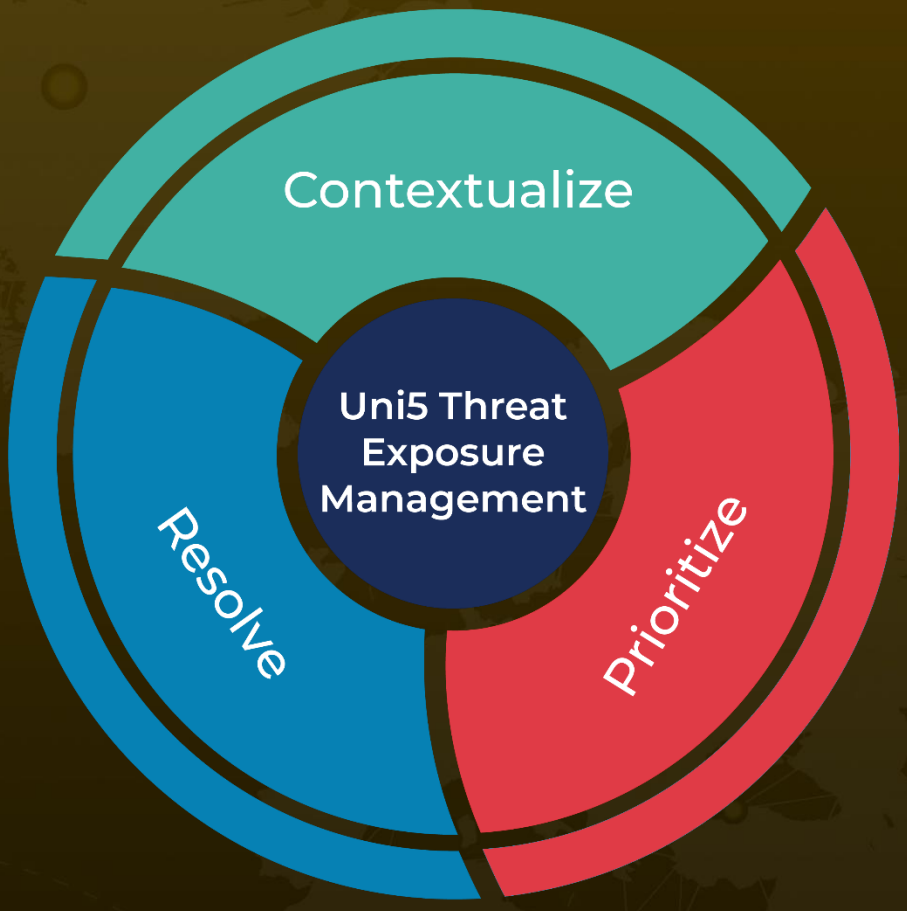
https://www.acronis.com/en-us/cyber-protection-center/posts/from-open-source-to-open-threat-tracking-chaos-rats-evolution/

https://github.com/AndroVirus/CHAOS-RAT

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

June 5, 2025 • 7:30 AM

More at www.hivepro.com