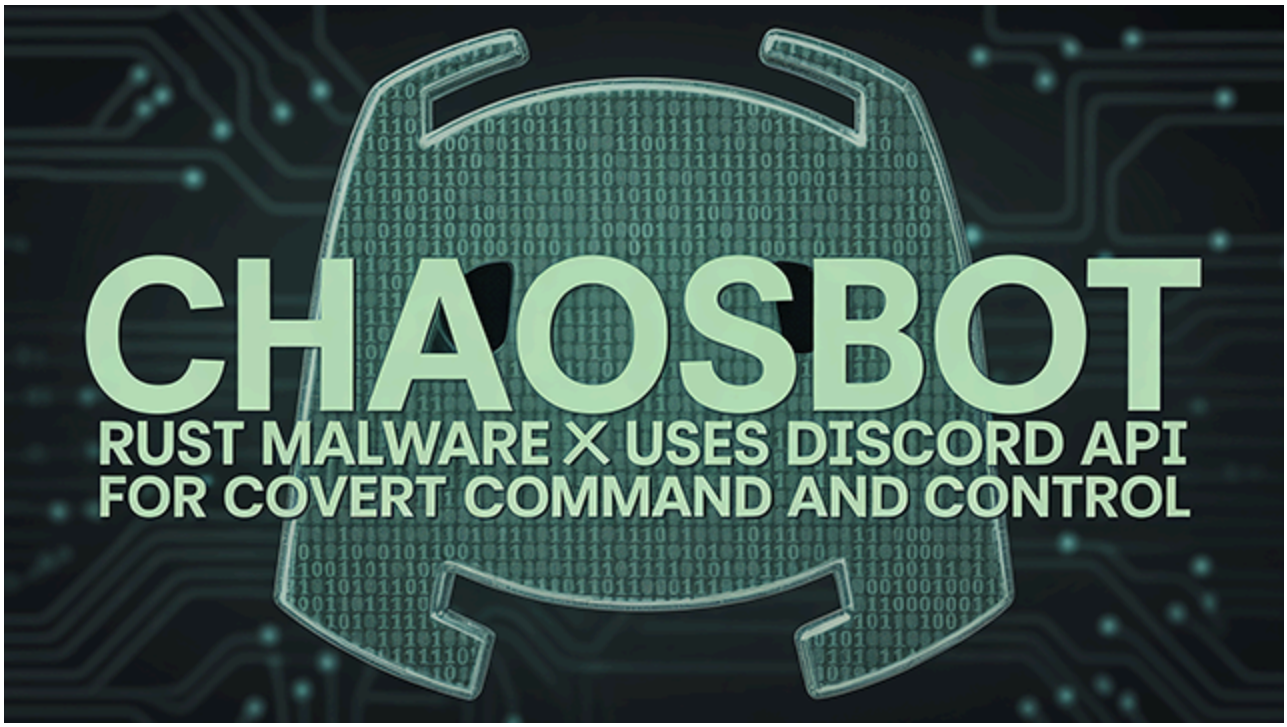
ChaosBot Rust Malware Uses Discord API for Covert Command and Control

cybersecsentinel.com/chaosbot-rust-malware-uses-discord-api-for-covert-command-and-control

Cybersec Sentinel October 15, 2025



Threat Group – Unknown operator using the moniker chaos_00019
Threat Type – Rust based backdoor and remote access trojan
Exploited Vulnerabilities – Valid accounts T1078, phishing T1566, DLL sideloading T1574.001, ETW suppression T1562.001, WMI lateral movement T1047
Malware Used – ChaosBot and Fast Reverse Proxy client
Threat Score – 8.0 🔴 High
Last Threat Observation – 14 October 2025

Overview

ChaosBot is a novel Rust based backdoor that combines stealthy execution with redundant command and control. It was first identified by a threat response team during an investigation in a financial services environment in late September 2025. The operators abuse valid VPN and directory credentials to gain initial access and then move laterally with WMI. They also run targeted phishing that delivers shortcut files which bootstrap the payload through PowerShell while a banking themed decoy document distracts the user.

ChaosBot executes via DLL sideloading through a legitimate Microsoft Edge component placed in a public user directory. It blinds endpoint telemetry by patching Event Tracing for Windows at runtime. The backdoor maintains control through two channels. It uses Discord's HTTPS API for low volume tasking and small exfiltration. It also deploys Fast Reverse Proxy for high throughput persistent access over a dedicated egress port to cloud infrastructure. This dual channel design increases resilience and enables quieter hands on keyboard operations.

Validation of Threat Identity and Scope

- The threat family name is derived from the primary operator profile chaos_00019. A secondary handle lovebb0024 has been observed.
- Initial victim evidence originates from a financial services customer with lure content themed for Vietnamese users. Targeting is not considered exclusive to that locale.
- Confirmed TTPs include valid account abuse for Cisco VPN and Active Directory, WMI based lateral execution, DLL sideloading through an Edge helper binary, ETW patching to suppress telemetry, and web service C2 through Discord.

Required Immediate Actions

These actions are prioritised to interrupt active operations and prevent recurrence.

Priority Remediation Table

Priority	Action	Objective	Notes for Validation
1	Enforce phishing resistant MFA on all VPN and privileged directory logons	Break valid account abuse T1078	Verify no exclusions and disable legacy authentication paths
2	Block egress to 18.162.110.113 and alert on TCP 7000	Disrupt FRP tunnel C2 T1090.003	Add specific detections for long lived 7000 sessions from workstations
3	Sweep endpoints for public folder implants	Identify high fidelity host IOCs	Search for msedge_elf.dll and identity_helper.exe in Public\Libraries and node.exe and node.ini in Public\Music
4	Restrict Discord to sanctioned hosts or block API usage from non browser processes	Reduce web service C2 T1102.002	Profile normal business use and alert on headless API calls
5	Disable sideloading paths through application control	Contain execution and persistence	Deny Edge helper execution from user writable paths using WDAC or AppLocker

Priority	Action	Objective	Notes for Validation
6	Patch Cisco ASA and FTD to current releases and harden VPN portals	Reduce infrastructure exposure	Even if credentials were abused in this incident, address contemporaneous critical flaws to lower parallel risk

Attack Vectors

Initial Access and Lateral Movement

Valid accounts T1078
The operator used compromised Cisco VPN credentials and an over privileged Active Directory service account to enter and propagate. The use of a broadly permissioned service identity constitutes a direct failure of least privilege and enables very rapid fan out.

Phishing T1566
A shortcut attachment triggers obfuscated PowerShell to download and launch the backdoor while displaying a banking themed decoy PDF to mask execution. This provides an alternative path when credential access fails.

WMI lateral execution T1047
After initial entry the operator leverages WMI to remotely spawn command shells and PowerShell on multiple hosts. This reduces noise compared to interactive sessions and accelerates deployment. Analysts should hunt for WmiPrvSE.exe spawning cmd.exe or powershell.exe with parameters that indicate remote execution and file placement in public directories.

Technical Mechanics and Defence Evasion

DLL sideloading T1574.001
The malicious DLL msedge_elf.dll is executed through a legitimate Microsoft Edge helper binary identity_helper.exe (the PWA Identity Proxy Host). Both are staged in C:\Users\Public\Libraries which is often less scrutinised by policy.

ETW suppression T1562.001
ChaosBot patches ntdll's EtwEventWrite by overwriting the prologue with an instruction sequence that forces immediate non logging returns. This blinds rules that rely on event based telemetry and requires defenders to pivot to memory integrity, image load monitoring, and network analytics.

Anti analysis T1497.001
The binary checks for MAC address prefixes associated with common virtualisation platforms and exits when a match is found. This prevents full behaviour exposure during automated detonations.

Persistence and Command and Control

ChaosBot maintains redundant C2 for resilience and flexibility.

Fast Reverse Proxy T1090.003
The backdoor downloads a client binary and configuration into C:\Users\Public\Music then launches it with a PowerShell command that sets output encoding and starts node.exe with a configuration file. The tunnel communicates over TCP port 7000 to an AWS hosted endpoint.

Discord web service C2 T1102.002
The malware authenticates with a bot token, validates through a user query, creates or uses a channel named with the victim hostname, and polls for commands. Supported commands include shell for command execution, download for secondary payloads, and scr for screenshot capture with file upload to the channel.

Table 1 ChaosBot C2 and Persistence Configuration Artifacts

Artifact Type	Description	Value or Location	Notes
Malicious DLL	ChaosBot payload	C:\Users\Public\Libraries\msedge_elf.dll	Executed by the Edge helper loader
Legitimate loader	Edge PWA Identity Proxy Host	C:\Users\Public\Libraries\identity_helper.exe	Abused for DLL sideloading
Sideloading path	Execution directory	C:\Users\Public\Libraries	User writable and less policed
FRP client binary	Persistence and C2 tunnel	C:\Users\Public\Music\node.exe	High throughput channel for operators
FRP configuration	Client configuration file	C:\Users\Public\Music\node.ini	Launched with node.exe -c
FRP egress port	Outbound TCP port	7000	Monitor for long lived sessions
Known C2 address	FRP remote host	18.162.110.113	Cloud hosted endpoint

Artifact Type	Description	Value or Location	Notes
Discord C2 endpoints	Web service API usage	discord dot com slash api slash v10 slash	Focus on API usage from non browser processes
Operator moniker	Threat actor handle	chaos_00019	Secondary handle lovebb0024

Known Indicators of Compromise

File Hashes

There are a lot of ChaosBot IoCs so I have created a separate page to view them:

https://cybersecsentinel.com/chaosbot-iocs/

Accounts and Handles

Type	Value	Purpose
Operator profile	chaos_00019	Discord operator account
Secondary handle	lovebb0024	Reported secondary account
Compromised identity	serviceaccount	Over privileged AD account used for WMI execution

Detection Engineering

Host focused actions

- Detect identity_helper.exe execution from user writable paths with image load events and block execution through application control.
- Detect msedge_elf.dll loads by the Edge helper process.
- Alert on WmiPrvSE.exe spawning command interpreters or PowerShell with remote execution arguments.
- Monitor memory integrity for unexpected modifications to ntdll export prologues. Any hook on EtwEventWrite is high signal.

Network focused actions

- Block and alert on 18.162.110.113 and investigate any prior connections from endpoints.
- Alert on outbound TCP 7000 to unknown destinations from workstations and VDI pools.

- Profile Discord usage. Alert on API heavy patterns from non browser processes or from hosts where Discord is not sanctioned.

File and content focused actions

- Create pre execution YARA signatures for the ETW patch motif and for anti virtual machine OUI checks where available.
- Flag systems where identity_helper.exe co resides with an unsigned DLL in Public libraries.

Mitigation and Prevention

Mitigation Checklist for Gap Analysis

Area	Control	What Good Looks Like	Evidence to Gather
User awareness	Targeted education on shortcut and script lures	Staff recognise .lnk risks and report decoys	Training records and simulated phishing results
Email filtering	Block shortcut and script based attachments	Gateway rejects .lnk and scripts by policy	SEG policy exports and quarantine logs
Antivirus protection	EDR with memory integrity and module allow listing	Alerts on ETW patching and sideloading from Public paths	EDR policy baselines and recent detections
Two factor authentication	MFA on VPN and all privileged accounts	Phishing resistant factors enforced with no bypasses	Conditional access and VPN policy exports
Log monitoring	High fidelity process creation and PowerShell logging	WMI spawned shells and FRP launches are alerted	SIEM rules and recent alert reviews
Regular updates	Timely patching of Cisco ASA and FTD and browsers	Current code levels with emergency advisories applied	Device compliance reports and change tickets
Application control	WDAC or AppLocker allow lists	Signed binaries restricted to approved locations	WDAC policy XML and enforcement scope
Network egress	Least privilege outbound policy	Discord restricted to approved hosts and API calls monitored	Firewall rules, proxy logs, and exception lists

Risk Assessment

Threat score 8.0 🔴 High

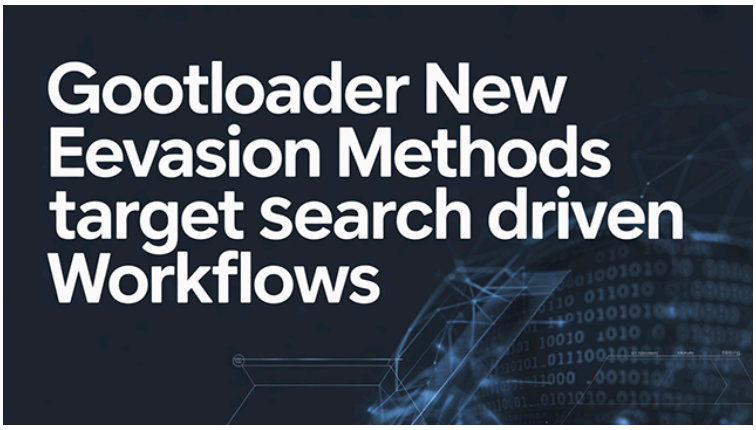
- **Stealth and resilience.** The use of Rust, ETW suppression, signed binary sideloading, and dual C2 channels increases survivability and reduces early detection.
- **Speed to impact.** Valid account access combined with automated WMI based fan out can establish broad coverage before containment.
- **Exposure landscape.** Contemporary critical issues on remote access appliances elevate the likelihood of parallel access paths and credential theft.
- **Operational intent.** Capability set and operator workflow indicate sustained access for reconnaissance and data theft with a clear path to follow on actions.

Conclusion

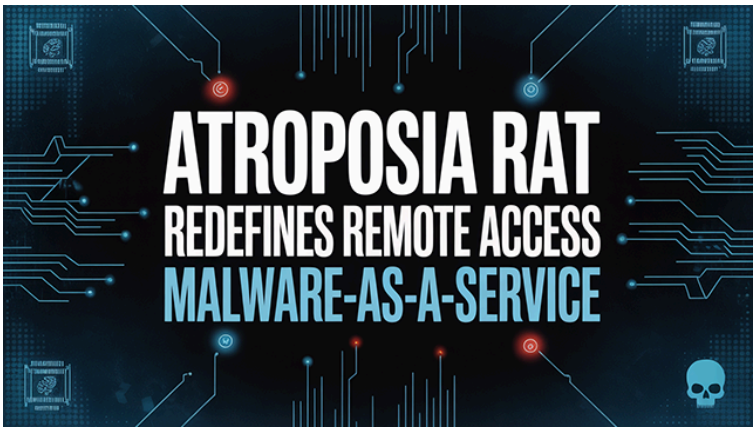
ChaosBot represents a modern enterprise backdoor that privileges stealth, speed, and redundancy. It exploits identity weaknesses, executes through a trusted loader in a permissive location, silences host level telemetry, and splits control between a popular web service and a reverse proxy tunnel. Defenders should assume partial logging blindness on affected hosts and compensate with memory integrity checks, strict execution controls, identity hardening, and egress monitoring. Immediate MFA enforcement, Cisco remote access patching and hardening, enforcement of application allow lists, and active hunts for the public folder artefacts and FRP patterns are expected to materially reduce risk.

Sources

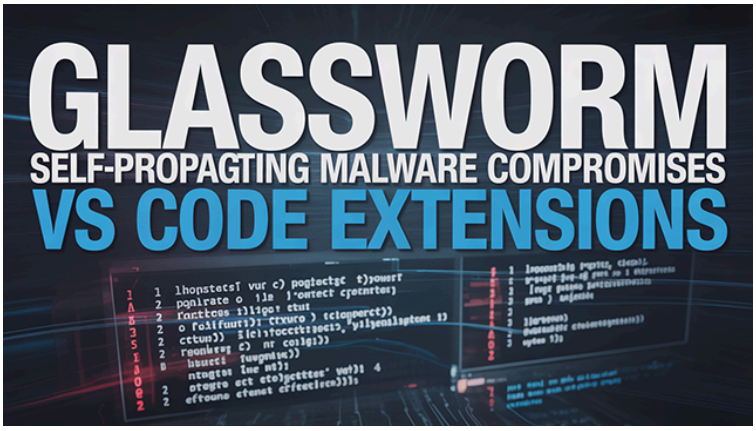
- eSentire – New Rust Malware ChaosBot Uses Discord for Command and Control – https://www.esentire.com/blog/new-rust-malware-chaosbot-uses-discord-for-command-and-control
- eSentire – ChaosBot IoC repository – https://github.com/eSentire/iocs/tree/main/ChaosBot
- The Hacker News – New Rust Based Malware ChaosBot Hijacks Systems via Discord – https://thehackernews.com/2025/10/new-rust-based-malware-chaosbot-hijacks.html
- Broadcom Symantec – ChaosBot Hiding on Your System and Communicating Through Discord – https://www.broadcom.com/support/security-center/protection-bulletin/chaosbot-hiding-on-your-system-and-communicating-through-discord
- Cisco – Cisco Secure Firewall ASA and FTD VPN Web Server Vulnerability CVE 2025 20333 – https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
- NVD – CVE 2025 20333 – https://nvd.nist.gov/vuln/detail/CVE-2025-20333



Threat Group – UNC2565 (also tracked as Storm-0494) Threat Type – Malware Loader and Initial Access Platform Exploited Vulnerabilities – No specific CVE confirmed. Campaign relies on SEO poisoning, compromised WordPress sites, archive format inconsistencies, Windows Script Host execution, and legacy filename behaviour. Malware Used – GootLoader, GootBot, secondary payloads such as Cobalt Strike



Threat Group – Unknown actor likely a financially motivated Malware as a Service operator Threat Type – Remote Access Trojan and Malware as a Service Exploited Vulnerabilities – No specific CVEs publicly linked at time of writing. Built in UAC bypass and a Local Vulnerability Scanner enable dynamic post infection exploitation Malware Used



Threat Group – Unknown (no confirmed attribution) Threat Type – Self-propagating software supply chain malware targeting VS Code and OpenVSX ecosystems Exploited Vulnerabilities – Abuse of trusted publisher credentials and the automated extension update pipeline; no CVE assigned for the platform itself Malware Used – GlassWorm loader and final-stage ZOMBI module (RAT with SOCKS