Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

MIMICRAT Remote Control Delivered Through Trusted Platforms

Date of Publication	Admiralty Code	TA Number
February 23, 2026	A1	TA2026052

Summary

First Seen: February 2026
Malware: MIMICRAT (alias AstarionRAT), Lua loader
Targeted Region: Global
Targeted Platform: Windows
Targeted Industries: Higher Education, Financial Services
Attack: The ClickFix campaign turns trusted websites into silent launchpads for attacks. The operation concludes with the deployment of MIMICRAT, a stealthy remote access trojan that conceals its encrypted command traffic within normal web activity. The result is a clean, low-noise compromise designed to evade detection while granting full remote control.

Attack Regions

Targeted Non-Targeted

Attack Details

#1

The ClickFix campaign marks a calculated shift in how attackers deliver advanced malware, culminating in the deployment of the custom MIMICRAT (alias AstarionRAT) Remote Access Trojan. Instead of relying on attacker-controlled servers, the operation begins by breaching legitimate, trusted websites. A genuine Bank Identification Number (BIN) validation service was compromised to inject malicious JavaScript.

#2

That script silently loads additional code from a second compromised site, an Indian mutual fund investment platform. The loaded script poses as the jQuery library and displays a counterfeit Cloudflare verification page. Victims are instructed to copy and run a PowerShell command from their clipboard. No file is downloaded, allowing the attack to bypass browser security controls. The lure is localized in 17 languages, expanding its global reach.

#3

When the victim runs the PowerShell command, a five-stage infection chain begins. The first stage is a heavily obfuscated one-liner that rebuilds its command-and-control domain during execution, leaving no readable traces in the script. It downloads a second PowerShell payload that disables security defenses. The script forces the Antimalware Scan Interface (AMSI) to fail and alters in-memory functions to avoid monitoring. With protections neutralized, it extracts a hidden Base64-encoded archive into a randomly named folder and launches a Lua-based loader.

#4

The third stage introduces a custom Lua loader with a built-in interpreter. The binary decrypts an embedded Lua script using a simple XOR routine. The fourth-stage shellcode acts as a reflective loader. It deploys the final payload, MIMICRAT. This Remote Access Trojan is a 64-bit Windows executable compiled with Microsoft Visual Studio. It communicates over HTTPS on port 443, calling back every ten seconds. Its traffic is designed to resemble normal web analytics data. The command-and-control server address is encrypted with RC4.

#5

MIMICRAT provides 22 post-exploitation commands. These include file and process control, interactive shell access, token theft and impersonation, reflective shellcode injection, SOCKS5 proxy tunneling, and adjustable beacon timing. The campaign's infrastructure is divided into two clusters: one handles initial delivery, and the other manages ongoing control, with Amazon CloudFront used as a relay to mask command traffic.

Recommendations

Detect Obfuscated PowerShell Execution: Configure endpoint detection and response (EDR) solutions to alert on PowerShell execution with obfuscated command-line arguments, minimized windows, and string-slicing or arithmetic-based string reconstruction patterns. Monitor for clipboard-based command execution initiated from browser contexts.

Monitor for ETW and AMSI Tampering: Deploy detection rules that alert on attempts to disable Event Tracing for Windows (ETW) by patching EventProvider fields, set amsiInitFailed to true, or perform in-memory method handle patching against AMSI scanning functions. These are high-fidelity indicators of advanced malware activity.

Restrict PowerShell Execution: Enforce PowerShell Constrained Language Mode and configure execution policies to limit script execution to signed scripts from trusted publishers. Apply application whitelisting to prevent unauthorized binaries from executing under %ProgramData% directories.

Hunt for Suspicious CloudFront C2 Traffic: Enhance network monitoring to detect anomalous outbound HTTPS traffic to Amazon CloudFront endpoints, particularly those matching the URI patterns /intake/organizations/events and /discover/pcversion/metrics. Implement SSL/TLS inspection where feasible to identify malicious encrypted C2 communications.

Detect Token Impersonation and SOCKS5 Tunneling: Deploy behavioral detection rules for Windows token theft and impersonation activity, particularly processes that duplicate security tokens by PID. Monitor for unauthorized SOCKS proxy establishment that may indicate covert network tunneling for lateral movement.

Review and Harden Compromised Website Detection: For organizations operating web properties, implement integrity monitoring and web application firewalls to detect unauthorized JavaScript injection. Regularly audit externally loaded scripts to prevent supply-chain-style compromises.

Implement Network Segmentation and Least Privilege: Apply network segmentation to limit lateral movement opportunities and enforce least-privilege access controls to reduce the impact of token impersonation and credential theft techniques used by MIMICRAT.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1189: Drive-by Compromise	
	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1204: User Execution	T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1053: Scheduled Task/Job	
Defense Evasion	T1027: Obfuscated Files or Information	T1027.010: Command Obfuscation
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
	T1620: Reflective Code Loading	
	T1055: Process Injection	
Privilege Escalation	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
Discovery	T1057: Process Discovery	
	T1083: File and Directory Discovery	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	bcc7a0e53ebc62c77b7b6e3585166bfd7164f65a8115e7c8bda568279ab4f6f1, 5e0a30d8d91d5fd46da73f3e6555936233d870ac789ca7dd64c9d3cc74719f51, a508d0bb583dc6e5f97b6094f8f910b5b6f2b9d5528c04e4dee62c343fce6f4b, 055336daf2ac9d5bbc329fd52bb539085d00e2302fa75a0c7e9d52f540b28beb
IPv4	45[.]13[.]212[.]251, 45[.]13[.]212[.]250, 23[.]227[.]202[.]114
Domains	xmri[.]network, wexmri[.]cc, www[.]ndibstersoft[.]com, d15mawx0xveem1[.]cloudfront[.]net
URLs	hxxp[:]//www[.]investonline[.]in/js/jq[.]php, hxxp[:]//backupdailyawss[.]s3[.]us-east-1[.]amazonaws[.]com/rgen[.]zip

References

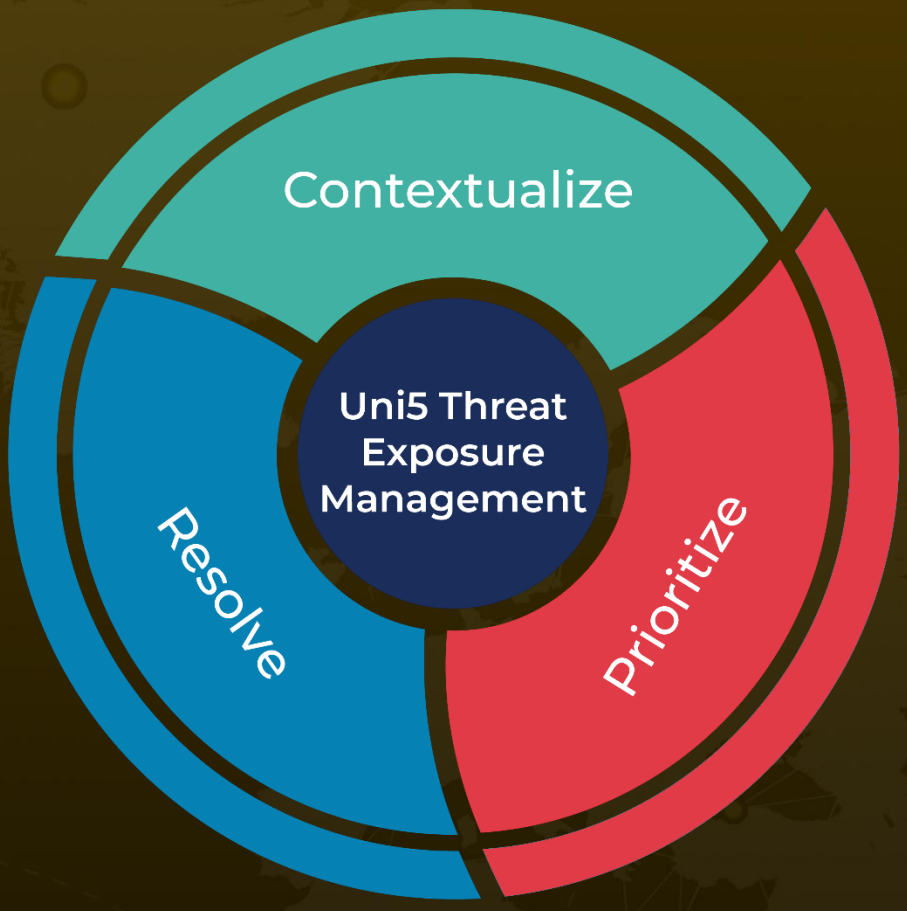
https://www.elastic.co/security-labs/mimicrat-custom-rat-mimics-c2-frameworks

https://hivepro.com/threat-advisory/clickfix-to-control-matanbuchus-campaign-deploys-astarionrat-in-minutes/

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

February 23, 2026 • 06:00 AM

More at www.hivepro.com