ultraviolet

THREAT ADVISORY

ClickFix MIMICRAT

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
February 24, 2026
TLP:GREEN

Executive Snapshot

MIMICRAT exemplifies an emerging category of intrusion activity that deliberately blends trusted web infrastructure, user-assisted execution, and fileless malware tradecraft to evade traditional perimeter and endpoint defenses. By abusing compromised legitimate websites and coercing users into manually executing obfuscated commands, this threat shifts the initial access burden from technical exploitation to social engineering, significantly increasing risk in environments with permissive scripting access and decentralized user populations. The malware's multi-stage execution chain, early suppression of host telemetry, and stealthy command-and-control communications over encrypted web traffic enable attackers to establish persistent, low-visibility access suitable for reconnaissance, credential abuse, and lateral movement. For enterprise leaders, this activity underscores the need to reassess assumptions around "trusted" web interactions and to treat user-initiated script execution as a high-risk control gap rather than an edge case.

- Enforce restrictive PowerShell and scripting controls, including constrained language mode, enhanced logging, and policies that limit user-initiated execution of obfuscated or clipboard-based commands.
- Expand endpoint detection and response coverage to reliably detect in-memory execution, AMSI and ETW tampering, and abnormal scripting engine behavior indicative of multi-stage loaders.
- Monitor for unexpected commands executed via the Windows Run dialog box, as well as token impersonation and theft.
- Update security awareness training and internal guidance to explicitly warn users against executing commands prompted by websites, fake verification pages, or unsolicited technical instructions, and validate these controls through regular simulation and response testing.

TIDE Team Analysis

An emerging malware campaign has been identified delivering a previously undocumented remote access trojan, referred to as MIMICRAT, that demonstrates a notable shift toward stealthier and more socially engineered initial access techniques. Rather than relying on traditional phishing attachments or malicious downloads, this activity leverages compromised legitimate websites to deliver payloads, increasing trust and reducing the likelihood of early detection. This approach reflects a broader trend in which attackers increasingly abuse trusted infrastructure to bypass perimeter defenses and user suspicion.

The initial infection vector relies on a social engineering technique known as “ClickFix,” where injected JavaScript on compromised websites presents users with a fake browser verification prompt. Victims are instructed to manually copy and paste an obfuscated PowerShell command into their system, creating a high-risk execution path that bypasses many browser-based security controls. Because no direct malware file is downloaded, this technique evades common download inspection and reputation-based protections, placing greater emphasis on user behavior as the attack enabler.

Once executed, the PowerShell command initiates a multi-stage infection chain designed to degrade host-based security controls early in the attack lifecycle. Subsequent scripts disable Windows telemetry and malware scanning interfaces, significantly reducing endpoint visibility for defenders. This early suppression of defensive mechanisms allows the attacker to safely deploy additional components while minimizing the likelihood of alerting or forensic reconstruction.

The attack chain then introduces a custom Lua-based loader that decodes and executes shellcode entirely in memory. This fileless execution technique complicates traditional malware detection and reduces forensic artifacts on disk. By leveraging scripting languages and in-memory loaders, the operators demonstrate a clear understanding of modern endpoint detection thresholds and an intent to remain resident for extended periods without triggering alarms.

The final payload, MIMICRAT, is a custom native implant that does not directly align with known commodity command-and-control frameworks. It exposes a broad set of post-exploitation capabilities, including interactive remote shells, file and process manipulation, credential and token abuse for privilege escalation, and network proxying through SOCKS functionality. These features provide attackers with flexibility to conduct reconnaissance, lateral movement, and long-term persistence within compromised environments.

Command-and-control communications are conducted over encrypted HTTPS traffic using patterns intentionally crafted to resemble benign web analytics activity. Key elements of the communication protocol, including headers and request paths, are dynamically decoded at runtime to hinder static detection. This blending of malicious traffic into normal web activity increases the difficulty of network-based detection.

The campaign appears to target users opportunistically rather than focusing on a single industry vertical, with infrastructure supporting multiple languages to increase engagement across regions. This broad targeting, combined with the use of trusted web properties and localized lures, expands the potential impact to global enterprises. Organizations with decentralized user bases and permissive scripting environments are particularly exposed to this type of threat.

To mitigate this risk, organizations should enforce tighter controls around script execution, particularly PowerShell, and invest in endpoint visibility capable of detecting in-memory execution and security control tampering. Equally

important is continued user education to discourage executing copied commands from web prompts, alongside regular testing of detection and response capabilities against multi-stage, socially engineered intrusion scenarios.

Why It Matters

ClickFix-style attacks represent a durable and increasingly effective evolution of social engineering that exploits a persistent blind spot in enterprise security models: user-initiated command execution. Unlike exploit-driven malware delivery, these campaigns do not rely on vulnerabilities or malicious file downloads. Instead, they abuse trust in legitimate web content and standard administrative tooling, convincing users to manually execute commands under the guise of troubleshooting, verification, or security checks. This technique bypasses many preventive controls by design, as the action originates from the user and leverages native system utilities that are often broadly permitted in corporate environments.

Historically, similar tradecraft has appeared in multiple forms, including fake CAPTCHA prompts delivering PowerShell loaders, fraudulent browser update pages instructing users to run terminal commands, and helpdesk-themed lures that mimic internal IT remediation steps. Over time, these attacks have steadily increased in sophistication, incorporating localization, trusted infrastructure abuse, and fileless execution to reduce friction and detection. The recurring success of these techniques demonstrates that attackers do not need zero-day exploits when they can reliably induce users to execute high-privilege actions themselves.

From an enterprise risk perspective, ClickFix attacks blur the line between technical compromise and policy failure. They expose gaps in user education, scripting governance, and behavioral detection that traditional security investments may not adequately address. As attackers continue refining these lures and pairing them with stealthy, custom implants, organizations that fail to treat user-driven execution as a primary attack vector risk sustained, low-visibility compromise. Addressing this threat requires not only better tooling, but a strategic shift toward reducing implicit trust in interactive commands and reinforcing the idea that social engineering remains one of the most scalable and effective intrusion methods available to adversaries.

How to Respond

- Strictly adhere to CyberSecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Ensure all users in your organization are briefed on ClickFix style attacks, with special focus on how legitimate services will never ask to copy/paste strings into run prompts.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a RedTeam or PurpleTeam engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking and monitoring Social Engineering attacks through open and closed source intelligence sharing partnerships.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---