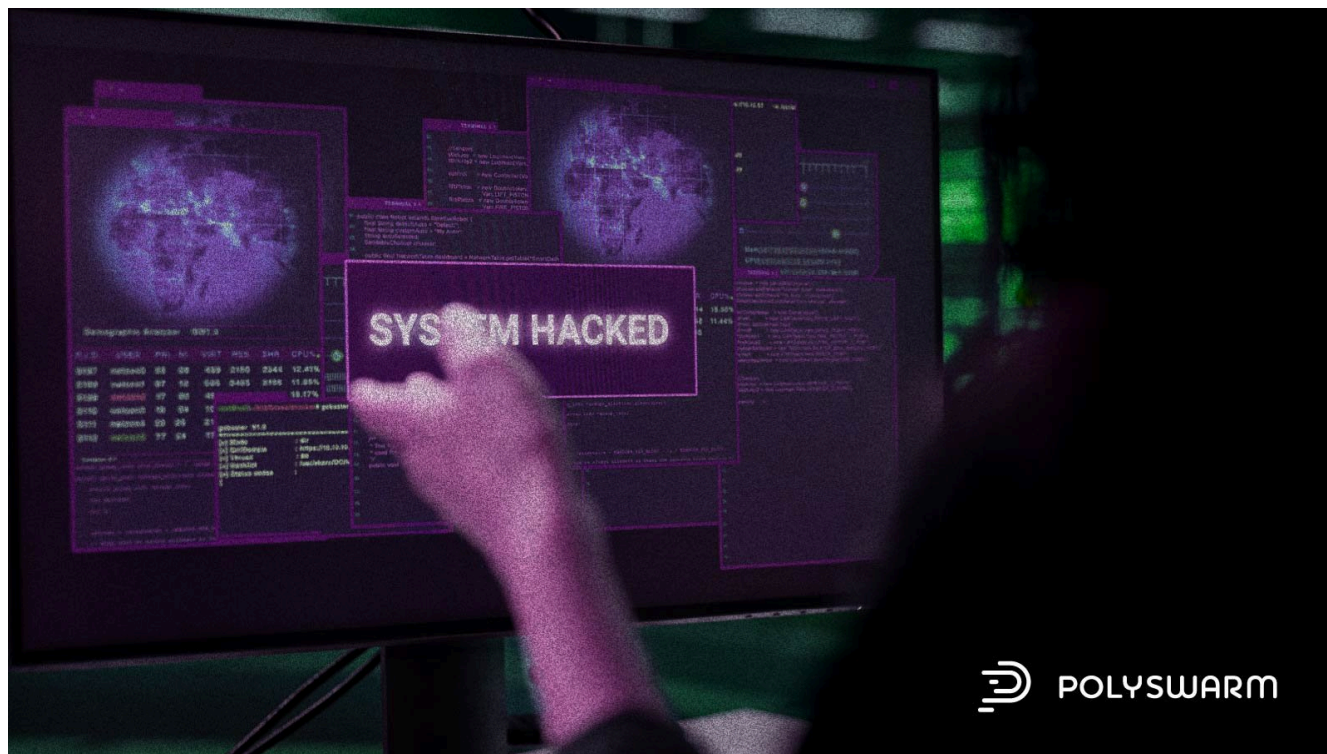


ClickFix-Themed Campaign Deploys Starland RAT and WLDR Framework

blog.polyswarm.io/clickfix-themed-campaign-deploys-starland-rat-and-wldr-framework

The Hivemind



Verticals Targeted: Cryptocurrency

Regions Targeted: United States, Germany, Romania, Venezuela

Related Families: Starland RAT, WLDR Framework, Remcos RAT, CastleStealer

Executive Summary

Industry researchers identified a financially motivated, Russian-speaking threat actor tracked as UAT-11795 conducting a sophisticated malware campaign targeting users primarily in the United States since at least June 2025. The operation employs suspected ClickFix-style social engineering, trojanized software installers, and a custom Python-based remote access tool, Starland RAT, to establish persistent access and deploy additional malware, including the previously undocumented WLDR PowerShell framework, CastleStealer, and Remcos RAT. The campaign

demonstrates a modular architecture, resilient C2 infrastructure, and a strong emphasis on credential theft, cryptocurrency wallet harvesting, and long-term post-compromise access.

Key Takeaways

- UAT-11795 is a Russian-speaking, financially motivated threat actor active since at least June 2025.
- The campaign uses suspected ClickFix-style social engineering, trojanized installers, and Starland RAT to establish persistent access.
- Victims are primarily located in the United States, with additional activity observed in Germany, Romania, and Venezuela.
- The actor deploys the bespoke WLDR PowerShell framework alongside CastleStealer and Remcos RAT.
- Cryptocurrency wallets, browser credentials, and enterprise systems are primary targets.

Background

Cisco Talos has disclosed a sophisticated malware [campaign](#) conducted by UAT-11795, a financially motivated threat actor believed to be Russian-speaking based on developer artifacts identified during analysis. Rather than relying on a single malware family, the operation uses a layered infection chain that provides multiple opportunities for persistence, payload delivery, and long-term remote access.

The campaign begins with suspected ClickFix-style social engineering, reflecting a broader industry [trend](#) in which threat actors increasingly rely on user-executed commands instead of traditional exploit-based delivery to establish initial access. Talos observed weaponized installers for applications including MobaXterm, Cisco WebEx, Zoom, DBEaver Community Edition, and FACEIT. The diversity of these lures suggests an opportunistic, volume-driven distribution model rather than targeting a single industry. Victim telemetry indicates that infections are concentrated in the United States, with additional suspected victims identified in Germany, Romania, and Venezuela.

Technical Analysis

Following execution of a malicious installer, the embedded Python loader decrypts and launches Starland RAT directly in memory. The RAT establishes persistence using scheduled tasks and Startup folder shortcuts while performing anti-analysis checks against common sandbox usernames and hostnames before initiating malicious activity.

Starland RAT performs extensive host reconnaissance, collecting hardware identifiers, operating system details, Active Directory information, installed antivirus products, desktop screenshots, and the presence of more than 40 cryptocurrency wallet applications and browser extensions. The collected information is encrypted and transmitted to attacker-controlled infrastructure to register the compromised host. If the primary C2 infrastructure becomes unavailable, the malware retrieves a fallback domain from a Polygon blockchain smart contract, providing a resilient fallback communication mechanism.

After registration, the RAT polls its C2 server approximately every 50 to 60 seconds and supports execution of shell commands, process injection of both 32-bit and 64-bit shellcode, and delivery of additional executable payloads. Depending on operator objectives, Starland RAT can deploy CastleStealer, Remcos RAT, or the previously undocumented WLDR framework.

The WLDR framework represents one of the campaign's more advanced capabilities. Delivered through an obfuscated PowerShell stager, WLDR operates entirely in memory and supports encrypted communications, concurrent PowerShell Runspace execution, modular task delivery, and robust reconnection logic. WLDR provides operators with an interactive PowerShell-based post-exploitation framework capable of executing additional scripts entirely in memory.

Talos also observed custom shellcode loaders responsible for deploying CastleStealer and Remcos RAT. These loaders resolve Windows APIs dynamically, bypass both the Antimalware Scan Interface (AMSI) and Event Tracing for Windows (ETW), decrypt embedded payloads in memory, and execute them using reflective loading or PowerShell Runspaces. This modular approach enables operators to deploy different payloads depending on campaign objectives.

Detection and Defensive Considerations

Organizations should remain vigilant against suspected ClickFix-style social engineering campaigns that encourage users to execute commands or install software outside trusted distribution channels. Software installers should only be obtained from verified vendor websites, and security teams should monitor for unexpected execution of mshta.exe, pythonw.exe, PowerShell, and scheduled task creation associated with newly installed applications.

Network defenders should also monitor communications with suspicious domains, unexpected Telegram infrastructure communications, and abnormal PowerShell activity associated with memory-resident execution. Because several payloads execute entirely in memory, organizations should supplement signature-based detection with behavioral

monitoring capable of identifying PowerShell abuse, process injection, AMSI bypass attempts, and anomalous scheduled task creation.

Analyst Commentary

This activity illustrates the continued evolution of financially motivated threat actors toward modular intrusion frameworks that combine custom malware, commodity malware, and in-memory PowerShell tooling within a single campaign. Rather than relying on a single malware family, operators can dynamically deploy capabilities based on victim value and operational objectives, making campaigns significantly more adaptable than traditional malware operations.

The campaign also reflects the continued evolution of ClickFix-style social engineering, which has rapidly become one of the most widely adopted initial access techniques across both cybercriminal and state-sponsored operations. By persuading users to manually execute seemingly legitimate commands, attackers can bypass many traditional detection opportunities that focus on malicious attachments or exploit-based delivery. As adversaries continue adapting the technique across multiple platforms and malware families, organizations should expect ClickFix-style lures to remain a prevalent method for initiating compromise.

UAT-11795 activity also demonstrates increasing operational resilience through redundant infrastructure, encrypted communications, blockchain-based fallback C2 discovery, and memory-resident PowerShell implants designed to minimize forensic artifacts. These techniques complicate both incident response and infrastructure disruption efforts while providing operators with persistent access long after initial compromise.

Campaigns such as this one highlight the importance of rapidly identifying both emerging malware families and the commodity payloads they deliver. As threat actors increasingly blend bespoke tooling with established malware, defenders require timely, multi-source threat intelligence capable of identifying novel malware, tracking evolving delivery mechanisms, and correlating related payloads across campaigns. PolySwarm's crowdsourced threat intelligence platform enhances detection and analysis by providing rapid malware classification, broad engine coverage, and rich contextual intelligence that helps security teams identify new threats, prioritize investigations, and respond more effectively to evolving adversary tradecraft.

IOCs

PolySwarm has multiple samples associated with this activity.

6ca7a458985350ac082a9c9820d7f8d39128a4c4bda2f5d32f169a45b7b22bc6
603fd9724de346a06e00c1b8502c2ac1180812a18bbf30032dab8d469e5c18e1
2c7a99f137efd718f89cf8b260379c99af89ea1939568df09314918f2c5999a3
5b9bf7957a9f8869c87ace1a6d76b48e2623073e72739ad0636b5dfa4bb2e0c3
7dc77a5abab119960fbe42b1535c957020cce1b8e0a3cf58d4eddc51b5bf9940
36e3838d07978f49ebe6546d57d2f311b8d6566558bcd58448e921c988cc346a
575ce92c473e6d47810321e309a4e29dd7f52f4152526b0bdca80f54b53aed2f
964256d3259b6e0c701ec04116c45cf0ec381c1c209dc29b09a7930cd7a4810b
a6821c7e9bfe2e6af0f690d906ec6a26161e2198c256fb60f3b4731c317f3ad9
a32ac345e39cb7606322e2155bd7b4d6941c1678619e48d1f14d9301ee53e6c0
451ac8ca34d5bcdfe476465f69eb517b2608f267c7e8d69f8ef36197a6f1d949
365024336c7681ac0854321ac6c140a245b9593285da02d2a590124cdc592370
a080b5380ccc8fc40b24c02151d305efc32d931dc547881e01a2e6f2b070c7dc
2a27b3415114b874da295c19cce5227a8b8d9525cc2da331034a1f45528eeca
1b46f761719dce44baa2d7b417c5214fc41c080f7f9ba485e7e489d949097f1f
896185a89bd7eb0520b03fdcfb8db0be98b43cf15f14041d73b23d3988c1bcab
a1835d333ac3db961a8ff1f4864e3c10a6f73a872c040599091390a009ac7804

Don't have a PolySwarm account? Go [here](#) to sign up for a free Community plan or subscribe.

Contact us at hivemind@polyswarm.io | Check out our [blog](#) | [Subscribe](#) to our reports.

Topics: [Threat Bulletin](#), [Remcos RAT](#), [ClickFix](#), [UAT-11795](#), [Cisco Talos](#), [Starland RAT](#), [WLDR](#), [WLDR PowerShell](#), [CastleStealer](#), [Trojanized installers](#)