ultraviolet

THREAT ADVISORY

TWINLOOT Malware Threats

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

Published Date:
August 19, 2026
TLP:GREEN

Executive Snapshot

TWINLOOT is a newly disclosed Python implant that operates entirely inside trusted Microsoft 365 infrastructure, using SharePoint dead-drops, Teams TURN relays, and a headless instance of the victim's own Edge browser to blend command-and-control traffic with legitimate enterprise activity, while harvesting Windows credentials via fake lock-screen prompts and enabling lateral movement through an integrated SOCKS5 proxy. Initial access relies on Teams-based social engineering where attackers impersonate IT support, and the malware's abuse of trusted cloud services reflects a broader pattern now seen across at least three independent threat actors in the past year. Organizations should take the following steps to reduce exposure:

- **Restrict and audit PowerShell execution policy** enterprise-wide, requiring signed scripts and disabling unrestricted execution for standard users to break the initial infection chain.
- **Enforce Teams external communication controls**, restricting or requiring approval for messages from external tenants and reinforcing user training on IT-support impersonation tactics specifically within Teams.
- **Disable or tightly govern browser remote debugging interfaces** (e.g., Edge/Chrome DevTools Protocol) via group policy, since TWINLOOT and comparable tools depend on CDP access to drive the victim's browser as a C2 transport.
- **Enforce phishing-resistant MFA and conditional access policies** on Microsoft 365 and Azure AD accounts to limit the value of credentials harvested through fake lock-screen prompts, and restrict SharePoint/Graph API app permissions to reduce dead-drop viability.

TIDE Team Analysis

A newly disclosed Python-based implant framework, tracked as TWINLOOT, demonstrates a significant evolution in adversary tradecraft by operating its entire command-and-control infrastructure inside trusted Microsoft 365 services. Researchers at Ontinue identified the malware during a July 2026 incident response engagement and assess the operator to be highly skilled in both offensive tradecraft and Microsoft's cloud architecture. TWINLOOT routes tasking through SharePoint Online via the Microsoft Graph API, relays interactive operator sessions through Microsoft Teams TURN servers using WebRTC DataChannels, and drives all of this traffic through a headless instance of the victim's own Edge browser. The result is C2 activity that is functionally indistinguishable from legitimate Microsoft 365 usage at the network layer, a design choice that directly undermines detection strategies built around domain reputation, TLS fingerprinting, or anomalous destination analysis.

Initial access is achieved through Teams-based social engineering, in which an attacker posing as IT support convinces a target to execute a PowerShell command that downloads a Python runtime and a 39 MB compiled loader. Once established, TWINLOOT operates two parallel channels: a SharePoint dead-drop that polls for instructions every 15 seconds and exfiltrates data, and a reverse SOCKS5 tunnel that enables interactive lateral movement over SMB, RDP, WinRM, and MSSQL ports. Credential theft is achieved through convincing fake Windows lock-screen prompts. Notably, the malware does not validate entered passwords against the operating system, instead always returning an error on the first attempt to compel the victim to re-enter their true credentials on the second try, which are then encrypted and exfiltrated for use in subsequent lateral movement.

This disclosure is not an isolated finding but confirms a broader trend: TURN relay abuse for covert C2, a technique publicly documented as "Ghost Calls" by Praetorian in 2025, has now been independently adopted by at least three distinct threat actors within roughly a year. DragonForce ransomware's Backdoor.Turn abused Teams TURN relays via QUIC, and the Chaos ransomware group's msaRAT used the identical headless-browser-via-CDP approach against Twilio's infrastructure. TWINLOOT's convergence with msaRAT on the specific technique of driving a victim's own browser as a C2 transport, despite no evident coordination between the groups, indicates this is becoming a standard technique in the ransomware and intrusion ecosystem rather than a one-off innovation.

Persistence is equally noteworthy from a defensive standpoint. TWINLOOT employs four methods, including TypeLib COM scriptlet hijacking and TaskCache manipulation, but its most significant technique is the first recorded malicious use of a mandatory profile hive (NTUSER.MAN) built entirely offline using undocumented Windows APIs (RegLoadAppKeyW and offreg.dll). This method allows the creation of persistent HKEY_CURRENT_USER registry keys without administrator privileges and without triggering typical endpoint security monitoring, since Windows prioritizes NTUSER.MAN over the standard NTUSER.DAT profile on load. Ontinue also notes operational overlaps with a cluster called STAC4749, previously linked to Teams vishing campaigns delivering Chaos ransomware, though the underlying tooling differs enough that this may represent a full retooling rather than a shared toolkit.

For enterprise environments, TWINLOOT represents a category of threat that legacy network-centric detection is poorly equipped to handle. Organizations should prioritize monitoring for anomalous process-to-network behavior from browser processes (particularly headless Edge instances with remote debugging enabled), unusual polling patterns against SharePoint and Graph API endpoints from endpoint agents rather than user sessions, and unexpected pythonw.exe connections to internal SMB, RDP, WinRM, or MSSQL ports. Teams-based social engineering training should be reinforced given its role as the initial access vector across multiple related campaigns. Security teams should also validate EDR and identity monitoring coverage for the NTUSER.MAN persistence

technique and audit registry-load API usage (RegLoadAppKeyW) as a detection opportunity, since this technique's use of legitimate Microsoft infrastructure for C2 and its living-off-the-cloud approach are likely to be adopted more broadly given the demonstrated ease of implementation across three unrelated threat actors.

Why It Matters

The rapid, independent convergence of three unrelated threat actors on the same TURN-relay and headless-browser C2 concept within a single year signals a shift in adversary economics rather than a one-off tooling choice. Praetorian's 2025 "Ghost Calls" research was intended as a defensive disclosure to get ahead of the technique, yet the speed at which DragonForce, the Chaos group, and now TWINLOOT's operators independently operationalized it demonstrates that publicly disclosed offensive research is being weaponized faster than defensive tooling can adapt to it. This compressed timeline between disclosure and adoption is itself the strategic concern: security programs that calibrate their roadmaps around annual or multi-year threat cycles are no longer aligned with the pace at which sophisticated actors are moving. Organizations should consider adopting a more proactive, frequent (quarterly or monthly), review of the threat landscape to better align their security programs and objectives.

More consequential than the specific TTPs is what this technique class reveals about the direction of adversary tradecraft. By routing C2 through services an enterprise already trusts, pays for, and grants broad default permissions to, attackers are effectively outsourcing their infrastructure risk to the cloud provider's reputation. This makes the traditional security perimeter model, which assumes malicious infrastructure is distinguishable from legitimate infrastructure, increasingly unreliable for a growing share of intrusions. Organizations that have invested heavily in network-layer detection and domain reputation filtering, without corresponding investment in cloud API behavioral baselining and identity telemetry, are likely to have a detection blind spot that scales with their adoption of Microsoft 365 and similar SaaS platforms.

Looking ahead, this trajectory is unlikely to plateau. The techniques underlying TWINLOOT, from TURN relay abuse to offline registry hive manipulation for persistence, depend on capabilities and open-source tooling that are becoming more accessible rather than more scarce, lowering the skill floor required to replicate this tradecraft. Enterprises should expect the same conceptual pattern (driving trusted, victim-owned infrastructure such as browsers and collaboration platforms as covert C2 transport) to reappear against additional SaaS ecosystems beyond Microsoft, and should treat this incident as justification for prioritizing long-term, cross-platform behavioral detection investment over reactive, indicator-based response to this specific campaign.

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.
- Enforce phishing-resistant MFA and conditional access policies on Microsoft 365 and Azure AD accounts to limit the value of credentials harvested through fake lock-screen prompts, and restrict SharePoint/Graph API app permissions to reduce dead-drop viability.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- 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

---