Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

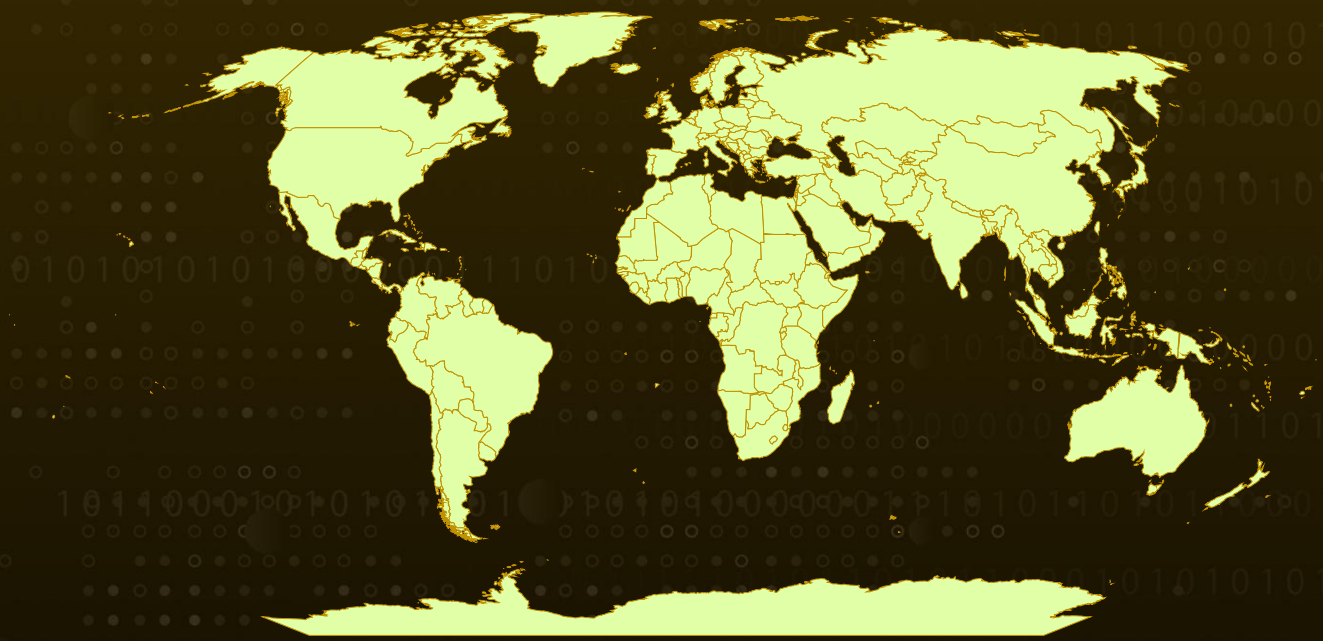
Inside the PHANTOMPULSE Social Engineering Kill Chain

Date of Publication	Admiralty Code	TA Number
April 17, 2026	A1	TA2026105

Summary

First Seen: February 12, 2026
Targeted Regions: Worldwide
Targeted Platforms: Windows, macOS
Targeted Products: Obsidian
Targeted Industries: Financial Services, Cryptocurrency
Malware: PHANTOMPULSE, PHANTOMPULL
Campaign: REF6598
Attack: What begins as a seemingly legitimate business conversation on LinkedIn quickly unravels into a highly orchestrated intrusion, where attackers exploit trust to guide victims into a weaponized Obsidian environment. By convincing targets to enable plugin synchronization, they silently trigger a multi-stage infection chain that deploys the PHANTOMPULL loader and ultimately the PHANTOMPULSE RAT. The malware blends advanced evasion with an unconventional blockchain-based C2 mechanism, leveraging public Ethereum transactions to dynamically resolve attacker infrastructure. With capabilities ranging from in-memory execution and privilege escalation to full system surveillance, the campaign demonstrates a refined fusion of social engineering and technical sophistication, turning a simple note-taking tool into a covert gateway for persistent compromise.

Attack Regions



Attack Details

#1 A novel social engineering campaign has been observed abusing Obsidian as a covert entry point, blending business pretexting with plugin-based exploitation to deliver a multi-stage malware chain. The attack is meticulously staged, beginning on LinkedIn, where threat actors impersonate venture capital representatives to build trust. Once rapport is established, the conversation is moved to a Telegram group populated with seemingly credible partners, reinforcing legitimacy. Framed around financial services and cryptocurrency liquidity, the narrative persuades the target to adopt Obsidian as the firm's internal management platform, granting access to an attacker-controlled vault. The critical turning point comes when the victim is convinced to manually enable the "community plugins" sync feature, disabled by default, allowing a weaponized plugin configuration to propagate and initiate execution.

#2 Once this trust boundary is crossed, the compromise unfolds rapidly. The synced configuration triggers the Shell Commands plugin, which executes Base64-encoded PowerShell on vault access. The initial stage retrieves a second-stage script from a hardcoded IP, which in turn downloads a payload (syncobs.exe) acting as the PHANTOMPULL loader. This loader decrypts an embedded payload using AES-256-CBC and executes it directly in memory via reflective loading, leveraging techniques like timer queue callbacks to evade sandbox detection. It then fetches the final payload, PHANTOMPULSE, over HTTPS, decrypts it using a rotating XOR key, and executes it while employing multiple anti-analysis techniques such as runtime API resolution and decoy logic.

#3 PHANTOMPULSE operates as a sophisticated, AI-assisted Windows RAT, introducing an unconventional command-and-control mechanism. Instead of relying solely on traditional infrastructure, it leverages public Ethereum blockchain data as a dead-drop resolver. By querying transaction data tied to a hardcoded wallet address, it extracts and decrypts C2 instructions embedded within blockchain transactions. However, the lack of sender verification introduces a notable flaw; any actor aware of the wallet and key could hijack the communication flow. Beyond this, the malware communicates via WinHTTP with multiple endpoints to handle telemetry, command execution, data exfiltration, and keylogging. Its capabilities extend to process injection, privilege escalation to SYSTEM, persistence manipulation, and comprehensive system control.

#4 On macOS, the attack follows a parallel yet platform-specific path. The malicious plugin executes a Base64-encoded payload via osascript, establishing persistence through a LaunchAgent configured to run continuously. The payload is heavily obfuscated, using fragmented strings and character-based encoding to hinder analysis. For command-and-control, it cycles through predefined domains and even scrapes a public Telegram channel as a fallback mechanism, enabling dynamic infrastructure rotation. A secondary payload is then fetched and executed directly in memory. Additionally, the attackers deploy the Hider plugin to suppress key interface elements within Obsidian, effectively masking the malicious activity. In the observed case, the intrusion was intercepted early, preventing the final payload from fully executing.

Recommendations

- **Monitor Obsidian Child Process Execution:** Deploy detection rules to alert on anomalous child process creation (PowerShell, cmd.exe, bash, osascript) spawned by the Obsidian application binary, as this is the primary behavioral indicator of REF6598 activity.

- **Restrict Community Plugin Sync in Obsidian:** Enforce organizational policies that prohibit users from enabling community plugin sync in Obsidian, particularly when connecting to vaults provided by external parties. Educate users that the "Installed community plugins" sync option should remain disabled by default.

- **Hunt for Obsidian Shell Commands Plugin Artifacts:** Proactively search endpoints for the presence of obsidian-shellcommands directories and associated data.json configuration files under .obsidian/plugins/ paths, as these indicate potential weaponized vault configurations.

- **Strengthen Social Engineering Awareness for Finance and Crypto Teams:** Conduct targeted security awareness training for personnel in financial services and cryptocurrency roles, emphasizing the risks of engaging with unknown entities on LinkedIn and Telegram who request installation of software or sharing of vault credentials.

Inspect LaunchAgent Persistence on macOS: Audit macOS endpoints for suspicious LaunchAgent plist files under ~/Library/LaunchAgents/, particularly those with randomized naming patterns and KeepAlive/RunAtLoad configurations that execute shell commands piped to osascript.

Enforce Application Allowlisting and Script Controls: Implement application control policies that restrict PowerShell execution to approved scripts and prevent unsigned AppleScript/osascript payloads from executing, reducing the attack surface for both the Windows and macOS execution chains.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.011: Plist Modification
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1620: Reflective Code Loading	
	T1497: Virtualization/Sandbox Evasion	
	T1055: Process Injection	

Tactic	Technique	Sub-technique
Discovery	T1082: System Information Discovery	
Collection	T1056: Input Capture	T1056.001: Keylogging
Collection	T1113: Screen Capture	
Command and Control	T1071: Application Layer Protocol	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA-256	70bbb38b70fd836d66e8166ec27be9aa8535b3876596fc80c45e3de4ce327980, 33dacf9f854f636216e5062ca252df8e5bed652efd78b86512f5b868b11ee70f
IPv4	195[.]3[.]222[.]251
Domain	panel.fefea22134[.]net, 0x666[.]info, thoroughly-publisher-troy-clara[.]trycloudflare[.]com
URL	t[.]me/ax03bot, hxxps[:]//panel[.]fefea22134[.]net, hxxps[:]//thoroughly-publisher-troy-clara[.]trycloudflare[.]com
Ethereum Wallet	0xc117688c530b660e15085bF3A2B664117d8672aA, 0x38796B8479fDAE0A72e5E7e326c87a637D0Cbc0E

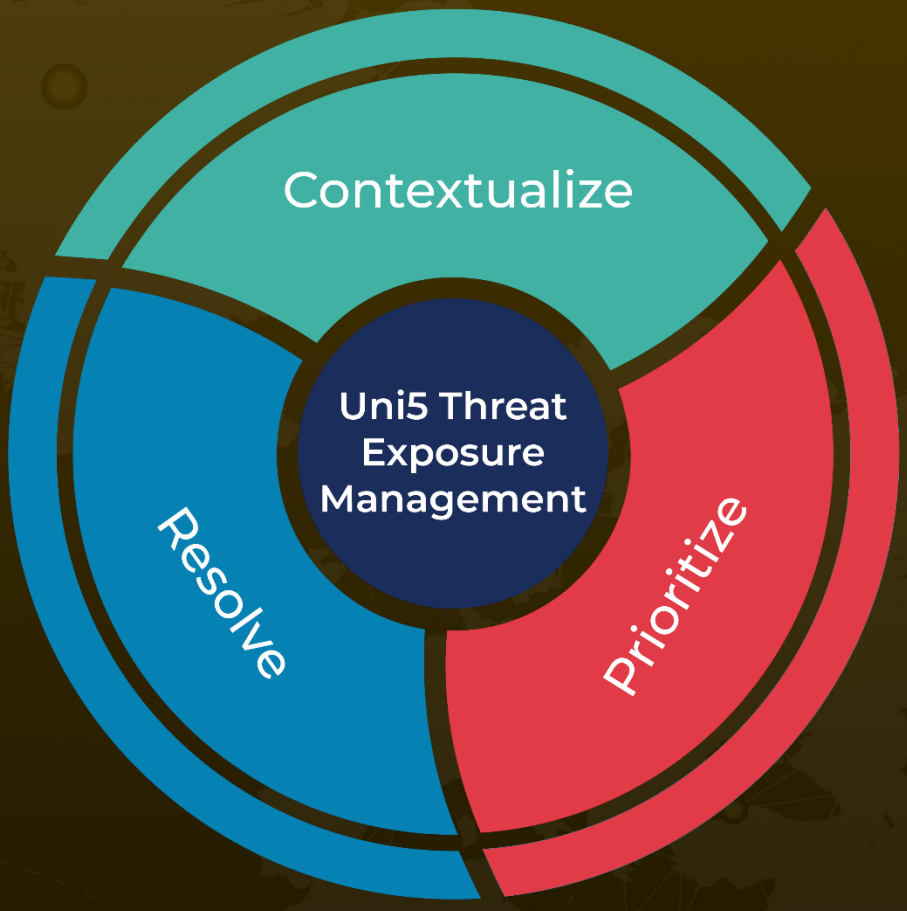
References

https://www.elastic.co/security-labs/phantom-in-the-vault

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

April 17, 2026 • 11:30 AM

More at www.hivepro.com