Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

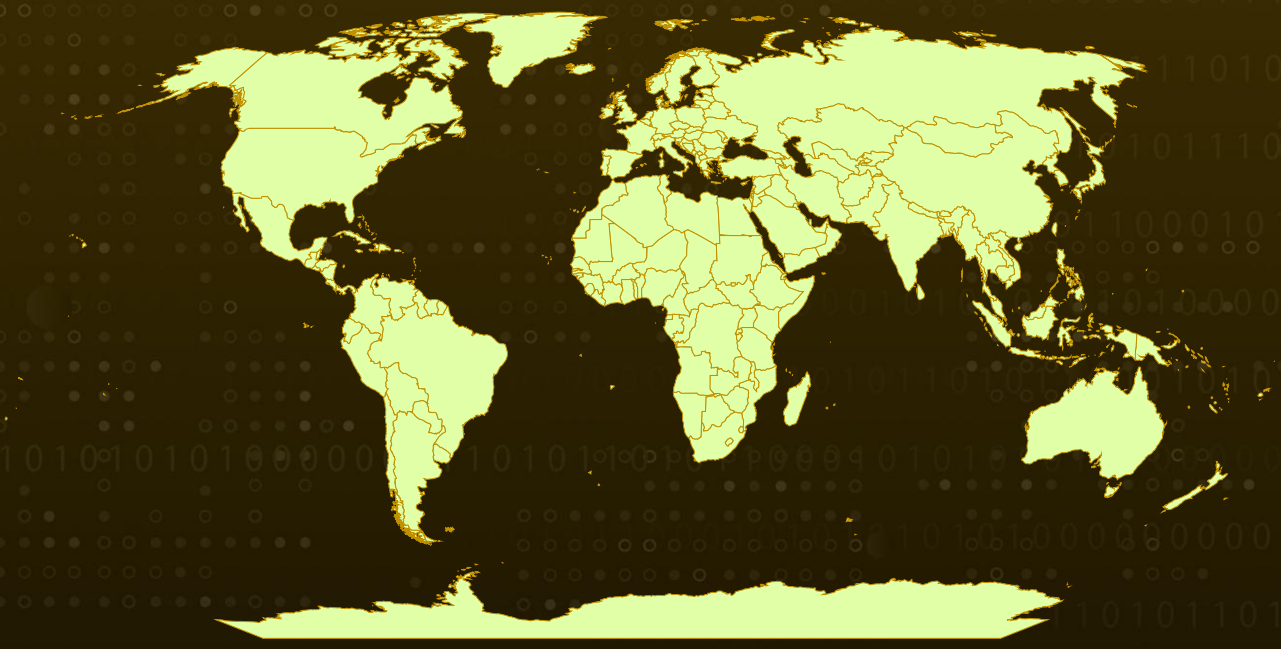
From Likes to Leaks: TikTok Campaign Lures Users into Installing Info-Stealers

Date of Publication	Admiralty Code	TA Number
May 27, 2025	A1	TA2025163

Summary

Malware: Vidar and StealC
Targeted Countries: Worldwide
Attack: A clever malware campaign is using AI-generated TikTok videos to trick users into running malicious PowerShell commands, disguised as software activation steps. These fake tutorials deliver info-stealing malware like Vidar and StealC, all while hiding in plain sight behind slick, trustworthy-looking content.

Attack Regions



Attack Details

#1 A new wave of social engineering attacks has been uncovered, leveraging TikTok to distribute powerful information-stealing malware such as **Vidar** and **StealC**. These campaigns disguise themselves as helpful software-activation tutorials, with AI-generated TikTok videos guiding viewers through seemingly legitimate steps. In reality, users are tricked into executing PowerShell commands that silently install malware on their systems.

#2 TikTok's massive user base and relatively light content moderation have made it an attractive vector for threat actors. By embedding malicious commands in short-form videos, attackers can distribute malware at scale without relying on traditional infrastructure. The use of AI-generated voices and visuals increases the perceived legitimacy of the content while enabling rapid production of convincing, high-volume videos.

#3 One notable account, @gitallowed, posted multiple videos instructing users to run specific commands under the guise of software activation. These videos often nearly identical aside from minor changes in angles or URLs have reached tens of thousands of users. One video alone accumulated nearly 500,000 views and over 20,000 likes, showcasing how effectively users can be misled by polished, step-by-step instructions.

#4 Upon execution, the PowerShell script contacts an external server disguised behind a Spotify-themed URL. It then creates hidden directories in the user's APPDATA and LOCALAPPDATA folders, where it downloads and launches either the Vidar or StealC payload. The script includes capabilities for retrying downloads, operating in stealth mode, cleaning up traces, and establishing persistence for long-term access.

#5 To further evade detection, the malware communicates with its command-and-control (C2) servers by mimicking legitimate traffic to services such as Steam and Telegram. This blending tactic helps attackers bypass network-based defenses and remain undetected.

#6 This campaign reflects a dangerous convergence of AI-driven content generation, social engineering tactics, and advanced malware delivery, enabled by the reach and trust associated with modern social media platforms like TikTok.

Recommendations

- **Think Before You Click or Copy:** If a video or post tells you to run strange commands (like something in PowerShell) to "unlock" or "activate" software don't trust it. No real software company asks you to copy-paste code from a social media post.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.
- **Limit PowerShell Use:** To reduce the risk of malware infections, restrict or monitor PowerShell usage on your device. Setting up alerts or limiting who can run PowerShell helps prevent malicious scripts from executing silently in the background.
- **Stay Skeptical of 'Too Good to Be True' Hacks:** Offers to get premium software for free, just by following a quick trick, are almost always scams.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0010** Exfiltration	**TA0011** Command and Control	**T1588** Obtain Capabilities
T1588.007 Artificial Intelligence	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1036 Masquerading	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3bb81c977bb34fadb3bdeac7e61193dd009725783fb2cf453e15ced70fc39e9b, afc72f0d8f24657d0090566ebda910a3be89d4bdd68b029a99a19d146d63adc5, b8d9821a478f1a377095867aeb2038c464cc59ed31a4c7413ff768f2e14d3886
URL	hxxp[:]//91[.]92[.]46[.]70/1032c730725d1721[.]php, hxxps[:]//allaivo[.]me/spotify, hxxps[:]//amssh[.]co/file[.]exe, hxxps[:]//amssh[.]co/script[.]ps1, hxxps[:]//steamcommunity[.]com/profiles/76561199846773220, hxxps[:]//t[.]me/v00rd
IPv4	49[.]12[.]113[.]201, 116[.]202[.]6[.]216

References

https://www.trendmicro.com/en_us/research/25/e/tiktok-videos-infostealers.html

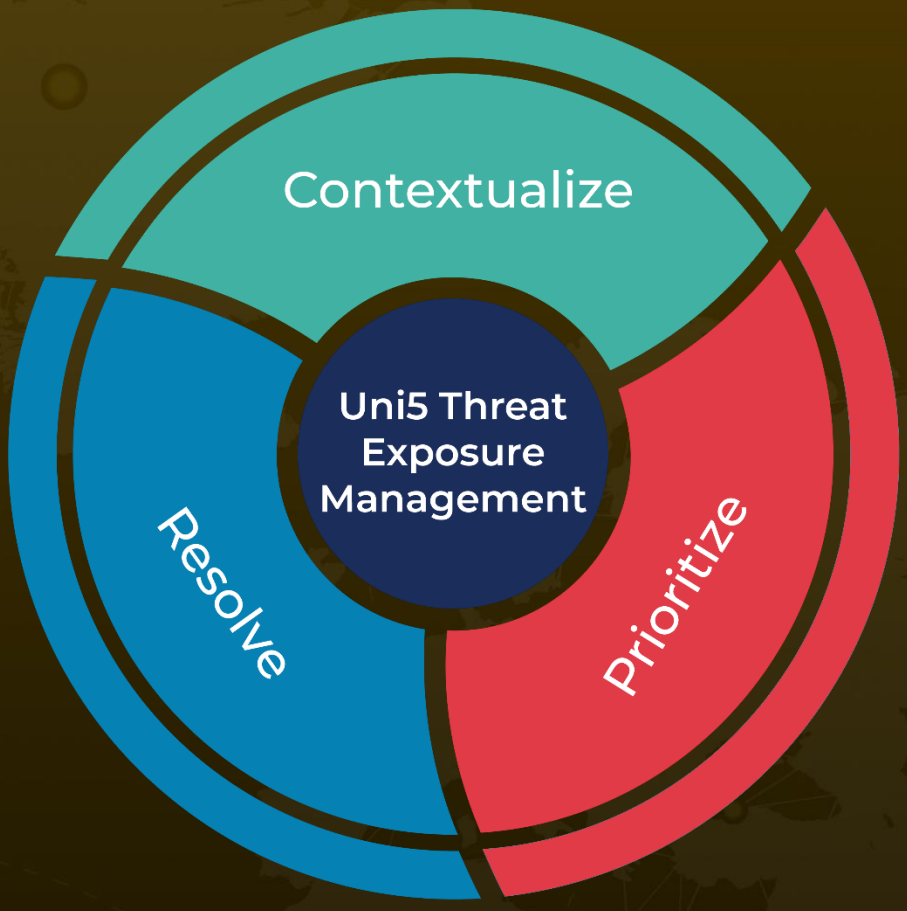
https://hivepro.com/threat-advisory/clearfake-blockchain-powered-malware-lures-thousands-with-fake-security-prompts/

https://hivepro.com/threat-advisory/a-new-info-stealing-malware-named-stealc-targeting-cryptocurrency-wallets/

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

May 27, 2025 • 5:00 AM

More at www.hivepro.com