

Info Stealer Targets 100+ Apps in YouTube Campaign

By cybleinc

Published: 2022-11-08 · Archived: 2026-04-05 21:29:55 UTC

Cyble Research and Intelligence Labs (CRIL) analyzes how Threat Actors use Phishing websites to deliver Info stealer via YouTube Tutorials.

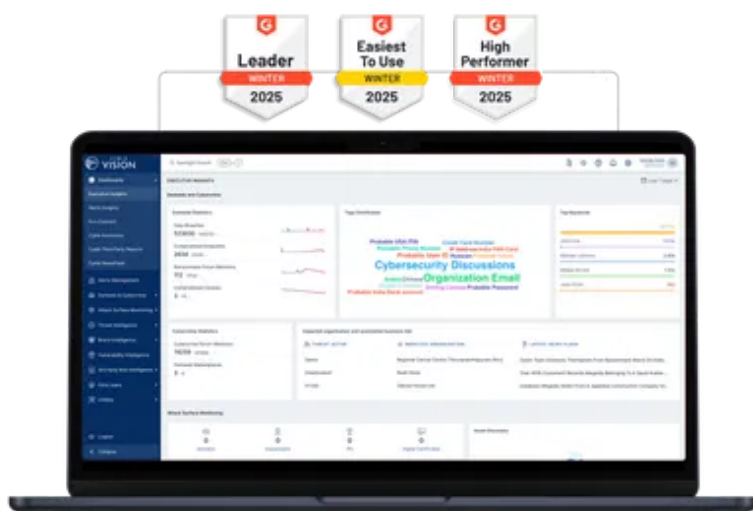
Threat Actors Create Phishing Websites for Mass Infection

Cyble Research & Intelligence Labs (CRIL) identified massive phishing campaigns running on YouTube as tutorials for downloading and installing cracked software, Games for free.

The video tutorial tricks the users into installing Information stealer from the link given in the video description and lures them into believing it is a crack for their desired software.

See Cyble in Action

World's Best AI-Native Threat Intelligence



We have seen many similar campaigns in the past, downloading Pennywise and Redline stealer. In these types of campaigns, the Threat Actor (TA) usually hosts the malicious file in the free file hosting platform.

Still, in this case, the TA has created phishing pages mimicking legitimate websites that provide service to users for downloading various software, games, and other tools.

Going through the different campaigns, we identified several phishing websites mentioned in the video description. The TA has created phishing pages to increase the chances of successful infection. Also, the impact of this campaign can be calculated based on the number of views on each video posted. The maximum number of views we observed on a single video is 18k, indicating the campaign is widespread.

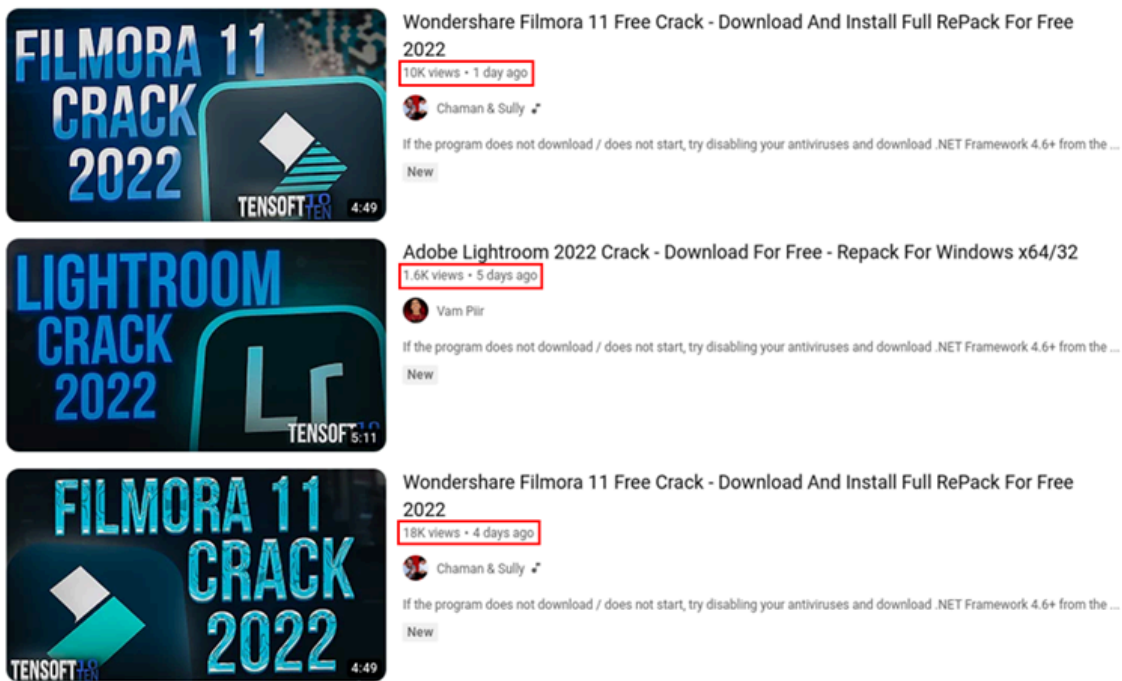


Figure 1 – Views on Videos

The below image depicts the comments in the YouTube videos. Similar comments from different YouTube videos conclude that the TA adds these to convince users to think this software is legitimate.

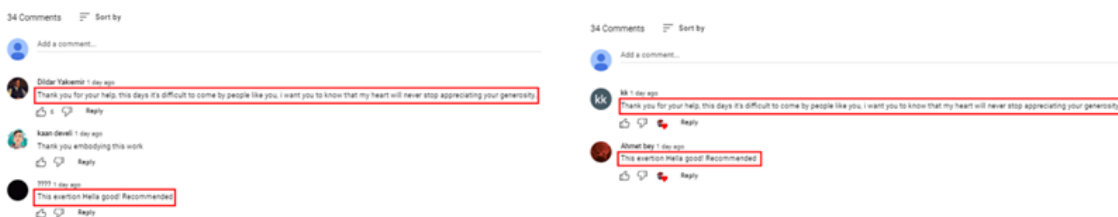
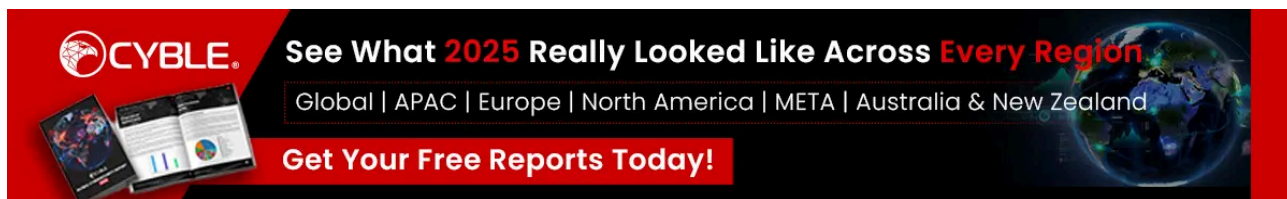


Figure 2 – Comments in the Videos

YouTube Campaigns Analysis:

During our research, we observed that the TA responsible for running these campaigns primarily targets people looking to get paid software for free such as games, programs, etc. To get this software for free, people usually search keywords like “software cracks,” “keygens,” etc. The search result of these keywords redirects users to these YouTube videos, guiding them to install malicious executables pretending to be the software they wanted to install.

The below image depicts a website hosted on the URL: [hxxps://teensoft\[.\]org/](https://teensoft[.]org/), which is being used by the YouTube video campaign to deliver Info stealer. The website delivers Vidar stealer malware posing as legitimate applications such as MS Office, Spotify Premium 2022, Adobe software, etc.

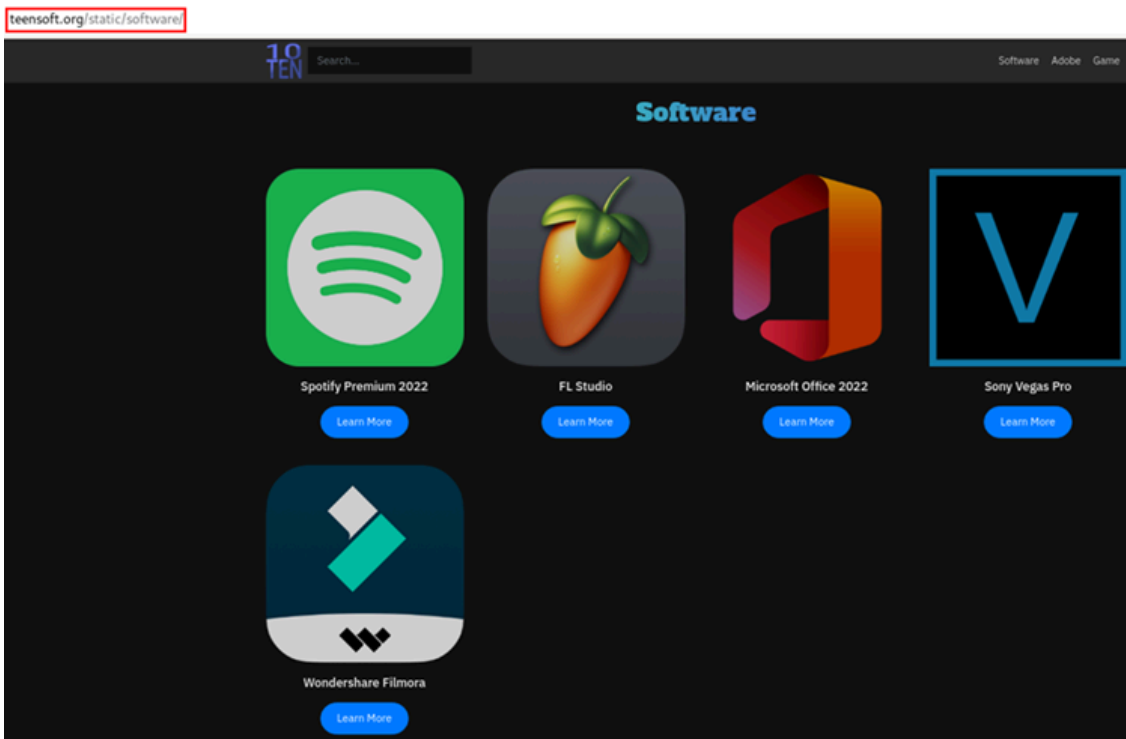


Figure 3 – Website Delivering Vidar Stealer

Campaign 2

The image below showcases a website hosted on the URL: `hxxps://wh1tesoftware[.]me/`, which is used by the malicious YouTube video campaign to deliver stealer [malware](#).

The website's catalog contains various malicious software hosted with legitimate names, such as MS Office, CCleaner PRO, AutoCAD, and Adobe software, which are distributed to target users. Behind these names, the website delivers Vidar stealer.

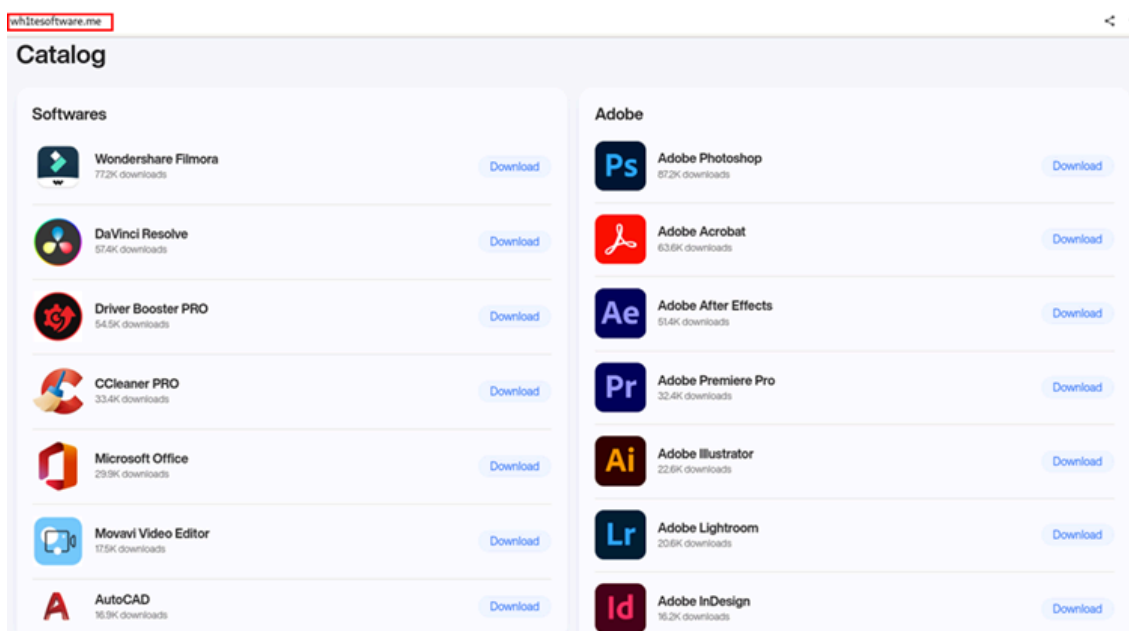


Figure 4 – Website Delivering Vidar Stealer

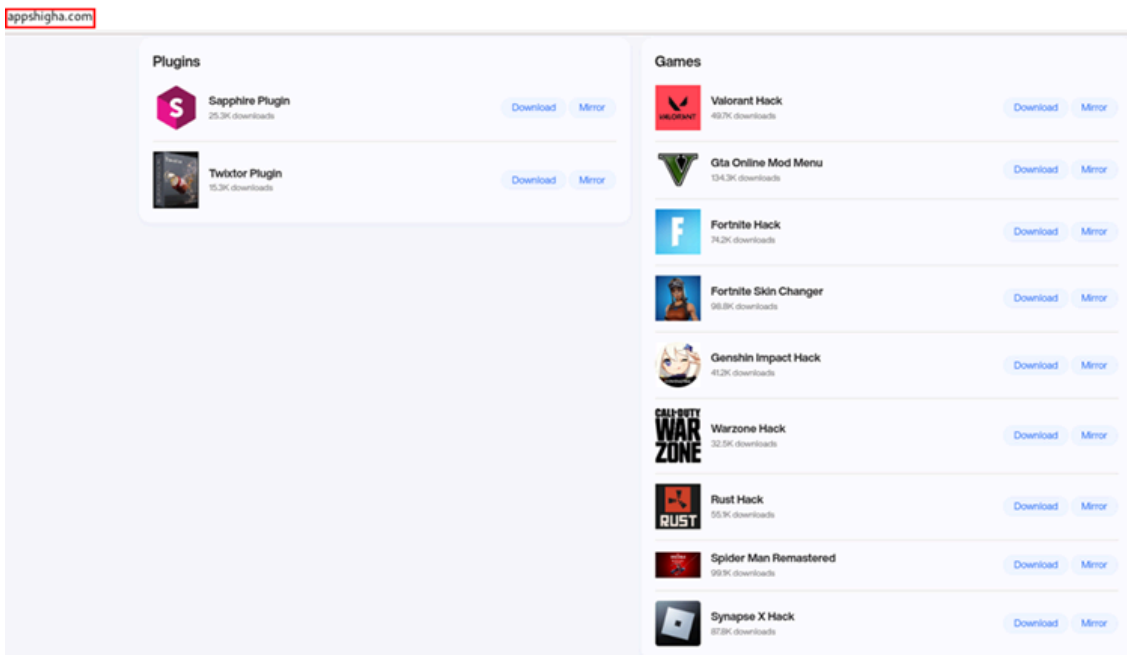


Figure 6 – Website Delivering RecordBreaker Stealer

The below table shows the list of software targeted by the TAs to deliver stealers.

| | | | |
|----------------------|--------------------|-----------------------|---------------------|
| Wondershare Filmora | Driver Booster PRO | CCleaner Professional | FL Studio |
| iCloud Bypass iOS 15 | Lumion 12 Pro | Sketchup | Bandicam |
| Voicemod Pro | Sony Vegas Pro 19 | AutoCAD | 3ds Max |
| Adobe Illustrator | Adobe XD | Adobe After Effects | Adobe Photoshop |
| Adobe Acrobat | Adobe InDesign | DaVinci Resolve | Movavi Video Editor |
| Ableton Live | | | |

The below table shows the list of gaming software the TA claims to deliver for free to infect users.

| | | | | |
|---------------------|---------------------|-----------------------|-----------------------|---------------------|
| Valorant Hack | GTA Online Mod Menu | Fortnite Hack | Fortnite Skin Changer | Genshin Impact Hack |
| Warzone Hack | Rust Hack | Spider-Man Remastered | Synapse X Hack | NBA 2K23 |
| Marvel's Spider-Man | F1 Manager | Saints Row | Elden Ring | Dying Light 2 |

| | | | | |
|---------------------|------------------|--------------------|-------------------------------------|-------------------|
| Wanderer Download | Expeditions Rome | Blackwind Download | Tom Clancy's Rainbow Six Extraction | Aery – Dreamscape |
| Monster Hunter Rise | The Kids We Were | God of War | Weird West | Far Cry 6 |

The below table shows the list of ROBLOX scripts targeted by the YouTube campaign. We have mentioned only 25 targeted ROBLOX script names here.

| | | | | |
|---------------------------|------------------------|--------------------------|------------------------|------------------------|
| Tatakai V.2 | Project Slayers | Limited Words | PLS STEAL | Gumball Factory Tycoon |
| Apocalypse Rising 2 | Viet Nam Piece | Mining Clicker Simulator | Your Bizarre Adventure | Legend Piece |
| Anime World Tower Defense | Pet Posse Script | Anime Adventures | Bid Battles | Bid Battles |
| Raise A Floppa | ARCH PIECE | Combat Warriors | Telekinesis | Lumber Tycoon |
| Decaying Winter | Anime Battle Simulator | Anime Sword Simulator | World Of Stands | Prison Life |

The below table shows the list of cheats and plugins targeted.

CHEATS:

| | |
|-------------------------------|-------------------------|
| Download Kiddions Modest Menu | free-rust-hack-download |
|-------------------------------|-------------------------|

PLUGINS:

| | |
|-----------------|----------------|
| Sapphire Plugin | Twixtor Plugin |
|-----------------|----------------|

Most of the binaries hosted on these phishing sites act as either downloaders or droppers for the stealer payload. The malware infection happens in multiple stages and at the end, executes the stealer payload. These stealers mainly exfiltrate sensitive user data such as cookies, system information, login credentials, etc. to their Command and Control (C&C) server.

This exfiltrated data is referred to as Stealer Logs , which are usually sold on cybercrime marketplaces and can be leveraged by other TAs to target individuals or get into corporate networks. The phishing campaign discussed in this blog was mainly distributing Vidar and RecordBreaker stealer.

Vidar Stealer

Vidar InfoStealer is based on C/C++ programming language. The Vidar malware family, which was first identified in 2018, can steal [sensitive data](#) from the victim’s PC. This includes banking information, saved passwords, IP addresses, browser history, login credentials, and crypto wallets, which can then be transferred to the TAs Command and C&C. We witnessed in past also where TAs used delivery mechanisms such as spam mail, cracked software, keygens, etc. to distribute this malware.

RecordBreaker Stealer

RecordBreaker stealer is suspected to be a recent version of the Raccoon stealer, which was spotted in the wild in 2022. While executing, this stealer performs several GET\POST requests with Command and Control (C&C) Server. Initially, it fetches the configuration and DLLs and then exfiltrates the victim’s data to C&C using a POST request. The stealer can also deliver other malware payloads based on the configuration’s settings. The figure below shows the stealer receiving configuration file.

```
referrer-policy: no-referrer
K-XSS-Protection: 0
ETag: W

libs_nss3: http://51.255.211.253/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
libs_msvcpl40: http://51.255.211.253/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcpl40.dll
libs_vcruntime140: http://51.255.211.253/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll
libs_mozglue: http://51.255.211.253/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
libs_freeb13: http://51.255.211.253/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freeb13.dll
libs_softkn3: http://51.255.211.253/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softkn3.dll
ews_meta_e: ejbalbakop1chlghcedalmeeeajnimhm;MetaMask;Local Extension Settings
ews_tronl1: ibnejdfjmmpcn1pebk1mkoioihofec;TronLink;Local Extension Settings
libs_sqlite3: http://51.255.211.253/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
ews_bsc: fhboh1mae1bohpbjbb1dcngcnapndodjp;BinanceChain;Local Extension Settings
ews_ronin: fnjhmkhmkbjkkabndcnnogagobneec;Ronin;Local Extension Settings
wts_exodus: Exodus;26;exodus;*;partitio*;*cache*;*dictionary*
wts_atomic: Atomic;26;atomic;*;cache*;*IndexedDB*
wts_jaxx1: JaxxLiberty;26;com.liberty.jaxx;*;cache*
wts_binance: Binance;26;Binance;*app-store.*.*.fp;-
wts_coinomi: Coinomi;28;Coinomi\Coinomi\wallets;*;-
wts_electrum: Electrum;26;Electrum\wallets;*;-
wts_electlc: Electrum-LTC;26;Electrum-LTC\wallets;*;-
wts_elecch: ElectronCash;26;ElectronCash\wallets;*;-
wts_guarda: Guarda;26;Guarda;*;cache*;*IndexedDB*
wts_green: BlockstreamGreen;28;Blockstream\Green;*;cache,gdk,*logs*
wts_ledger: Ledger Live;26;Ledger Live;*;cache*;*dictionary*;*sqlite*
ews_ronin_e: kjmooh1gokccodicjjfbfom1bjjgfhk;Ronin;Local Extension Settings
ews_meta: nkbinfbogaeaoeh1efnkodbefggpkn;MetaMask;Local Extension Settings
```

Figure 7- RecordBreaker Configuration File

Conclusion

[Threat Actors](#) are constantly enhancing their techniques to deliver malicious programs. In this particular case, the TA uses YouTube channels to spread malicious payloads hosted on phishing websites. This campaign primarily leverages YouTube videos (with step-by-step tutorials) to trick users into installing malicious programs on their systems. CRIL has been observing increasing trends in [social media](#) scams of late.

Cyble Research and Intelligence Labs’ mission is to continuously monitor and alert our audience to high-tech cyber scams and protect our clients in cyberspace by supporting them in achieving their goals.

Our Recommendations

We have listed some [essential cybersecurity](#) best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Avoid downloading pirated software from unverified sites.
- Use strong passwords and enforce [multi-factor authentication](#) wherever possible.

- Keep updating your passwords after certain intervals.
- Use a reputed anti-virus and [internet security](#) software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TA.
- Enable Data Loss Prevention (DLP) Solutions organization wide.

MITRE ATT&CK® Techniques

| Tactic | Technique ID | Technique Name |
|---------------------|--|--|
| Execution | T1204 | User Execution |
| Defense Evasion | T1140 T1497 T1055.012 | Deobfuscate/Decode Files or Information Virtualization/Sandbox Evasion Process Injection: Process Hollowing |
| Credential Access | T1555 T1539 T1552 T1528 | Credentials from Password Stores Steal Web Session Cookies Unsecured Credentials Steal Application Access Token |
| Collection | T1113 | Screen Capture |
| Discovery | T1518 T1124 T1007 | Software Discovery System Time Discovery System Service Discovery |
| Command and Control | T1071 | Application Layer Protocol |
| Exfiltration | T1041 | Exfiltration Over C2 Channel |

Indicators of Compromise (IOCs)

| Indicators | Indicator Type | Description |
|---|-----------------------|------------------------------|
| e99bebb8facdff476c4d1163dfa85cb b04cdfb5b57b309a1d9a2e5f0bd9c01cb490854b f1e8f4fba1da25cc02d0673f8cc3962c7419d769cb139f818f8f1e4d56a891df | MD5 SHA1 SHA256 | Campaign 2: Vidar Stealer |
| hxxp://95.217.27.240/ | URL | Campaign 2: C&C |
| 95.217.27.240 | IP | Campaign 2 C&C |

| | | |
|--|-----------------------|--|
| 8e636392c37a87f6f80d94105eff13f3 efac1bb38a50284b74d5f9e90ba3909d7a998df7 65509ae4d5b04ea786423cbdee234ddca5363da3db68f49ba4fc0db16ceba799 | MD5 SHA1 SHA256 | Campaign 1: Vidar Stealer |
| hxxp://95.217.27.240/ | URL | Campaign 1 C&C |
| hxxp://195.201.251.82:80 | URL | Campaign 1 C&C |
| 78c988133da5464c206078efe56b9191 3024b41db4386592449a7ecb19bf8acc3853d9b7 81ae14e327301b347ff43d58c2a907fb2fb94dc3e73c750bad64ab824066b34c | MD5 SHA1 SHA256 | Campaign 3 RecordBreaker stealer |
| hxxp://91.213.50.70/Objhkcgmib.bmp | URI | Campaign 3 Malicious URI |
| hxxp://51.255.211.253/ | URL | Campaign 3 C&C |
| 46b417fe39b7cf62a63b665a8caef5ea 5448de47e5e922686ed66fbc21ba6ebf830e0cc7 edcabbcc1389f1a4d2ad030c28dcb97d065027e0645faa3199f66b05505cced5 | MD5 SHA1 SHA256 | Campaign 4 RecordBreaker stealer |
| hxxp://146.70.86[.]136 | | Campaign 4 C&C |

Source: <https://blog.cyble.com/2022/11/08/massive-youtube-campaign-targeting-over-100-applications-to-deliver-info-stealer/>