

## Massive campaign uses YouTube to push password-stealing malware

By Lawrence Abrams

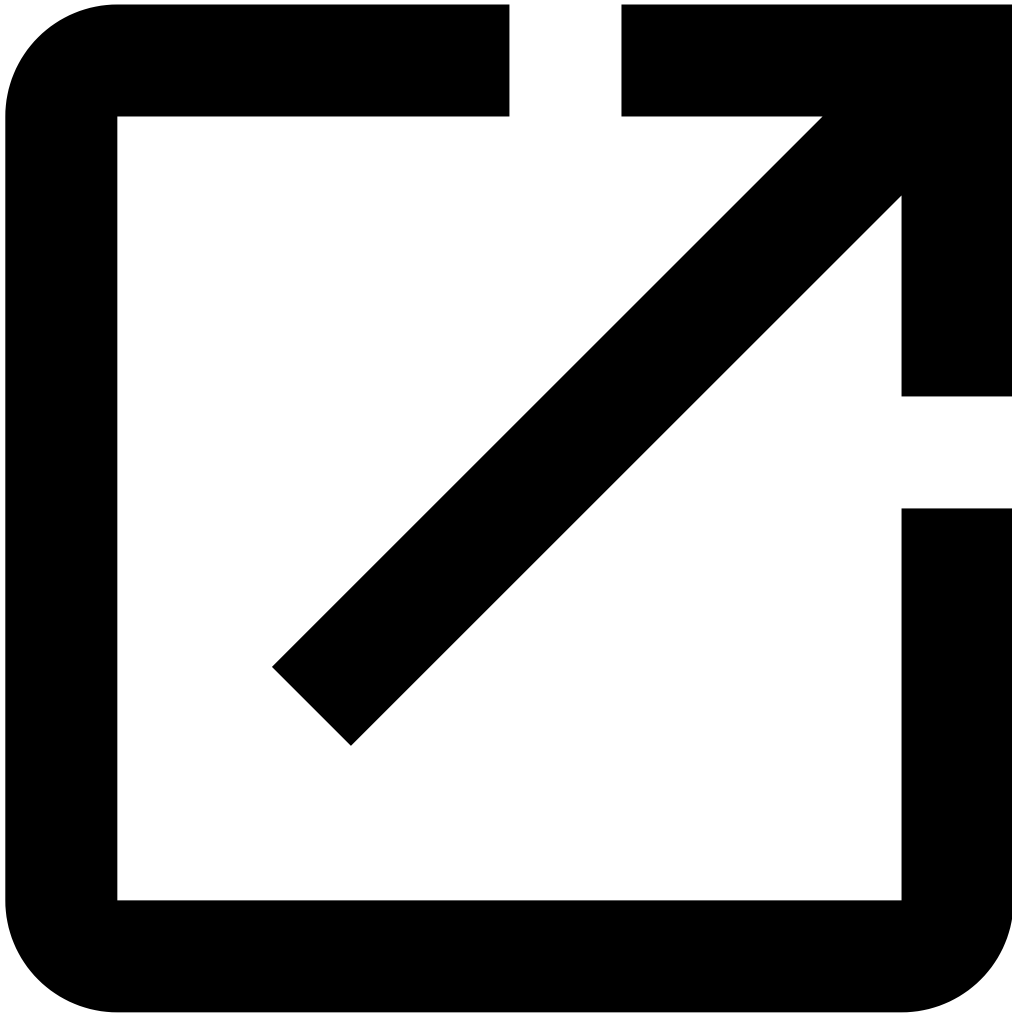
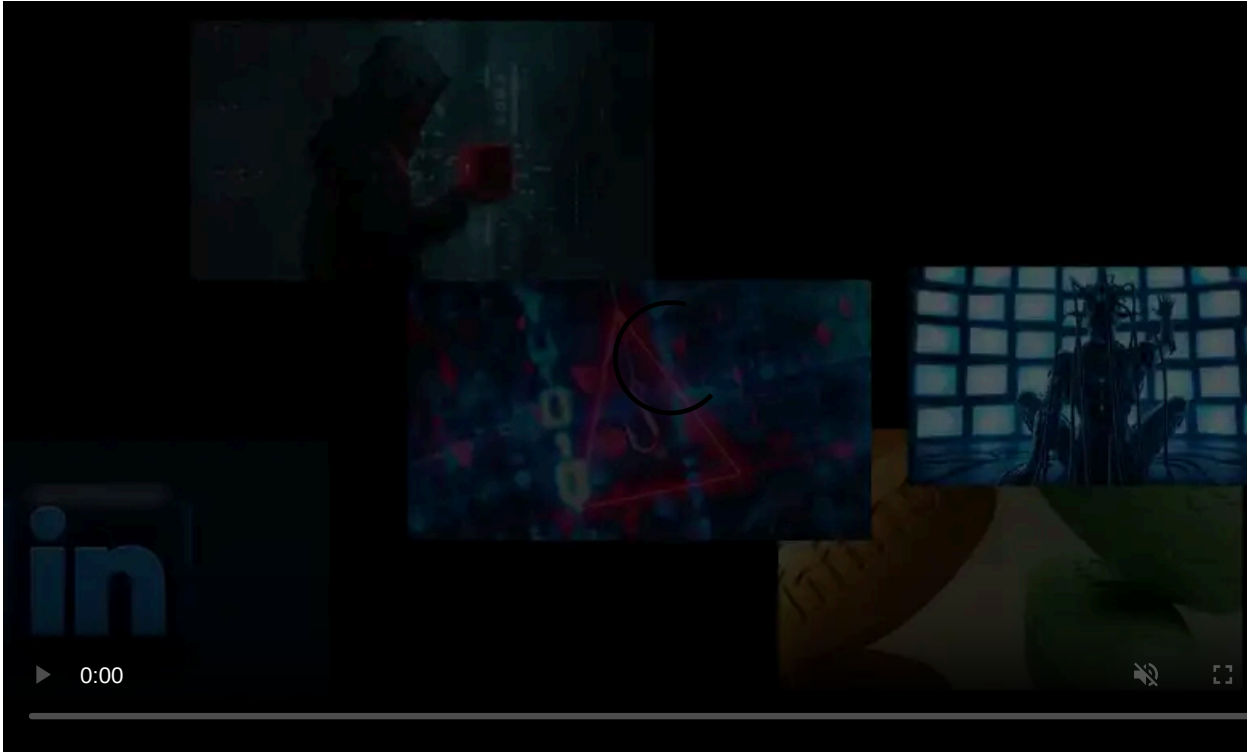
Published: 2021-10-21 · Archived: 2026-04-05 18:45:56 UTC



Widespread malware campaigns are creating YouTube videos to distribute password-stealing trojans to unsuspecting viewers.

Password stealing trojans are malware that quietly runs on a computer while stealing passwords, screenshots of active windows, cookies, credit cards stored in browsers, FTP credentials, and arbitrary files decided by the threat actors.

When installed, the malware will communicate with a Command & Control server, where it waits for commands to execute by the attacker, which could entail the running of additional malware.



Visit Advertiser website [GO TO PAGE](#)

## Malicious YouTube videos gone wild

Threat actors have [long used YouTube videos](#) as a way to distribute malware through embedded links in video descriptions.

However, this week has [Cluster25](#) security researcher [Frost](#) told BleepingComputer that there has been a significant uptick in malware campaigns on YouTube pushing various password-stealing Trojans.

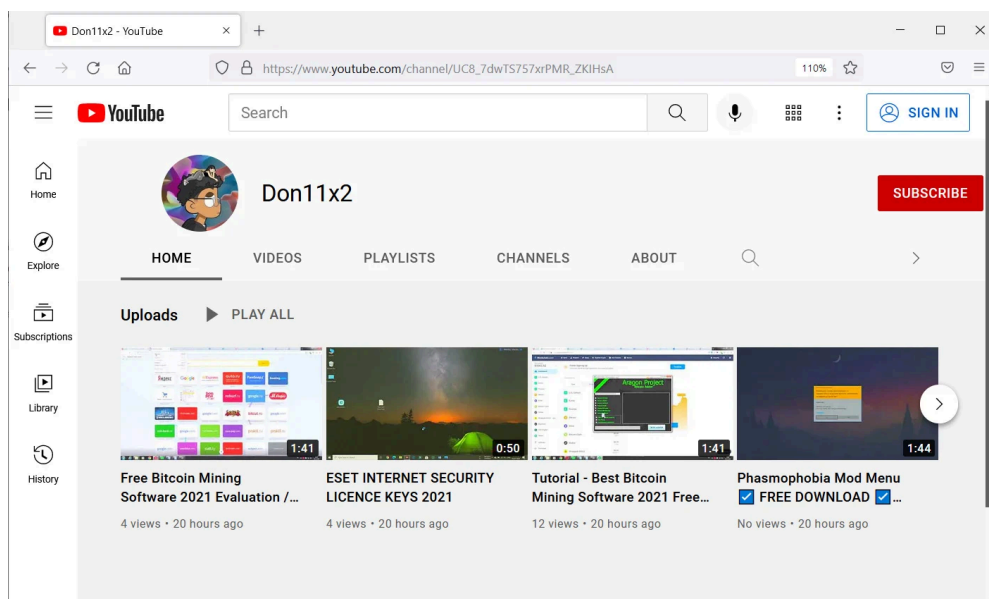
Frost told BleepingComputer that it is likely two clusters of malicious activity being conducted simultaneously - one pushing the RedLine malware and the other pushing Racoon Stealer.

The researcher said that thousands of videos and channels had been made as part of this massive malware campaign, with 100 new videos and 81 channels created in just twenty minutes.

Frost explained that the threat actors use the Google accounts they steal to launch new YouTube channels to spread malware, creating a never-ending and ever-growing cycle.

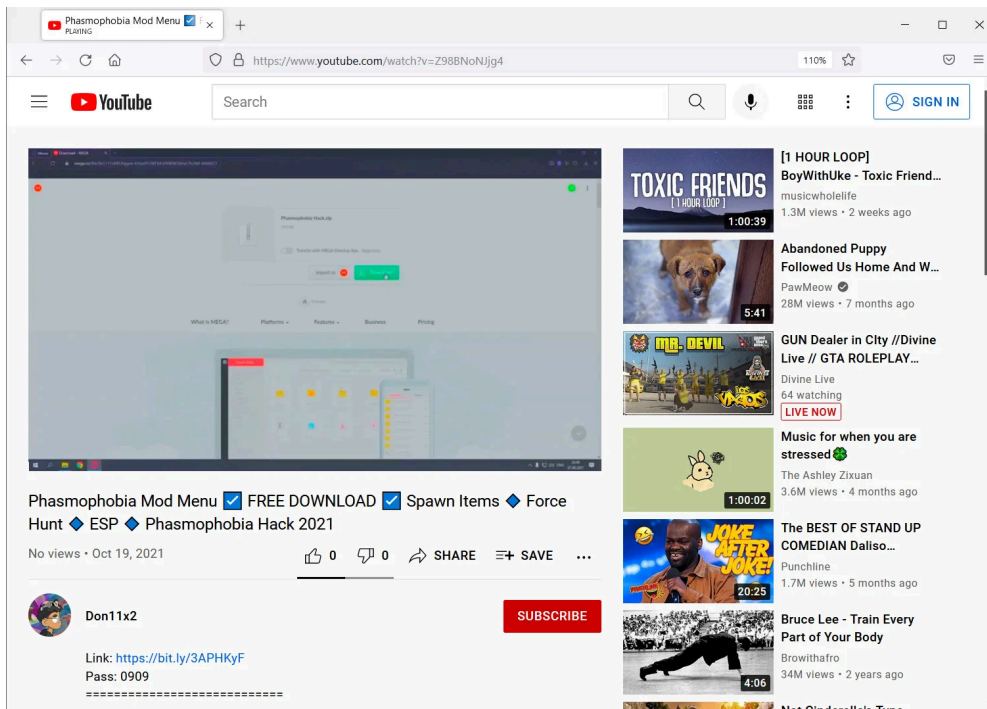
"The threat actors have thousands of new channels available because they infect new clients every day. As part of these attacks, they steal victim's Google credentials, which are then used to create new YouTube Videos to distribute the malware," Frost told BleepingComputer.

The attacks start with the threat actors creating numerous YouTube channels filled with videos about software cracks, licenses, how-to guides, cryptocurrency, mining, game cheats, VPN software, and pretty much any other popular category.



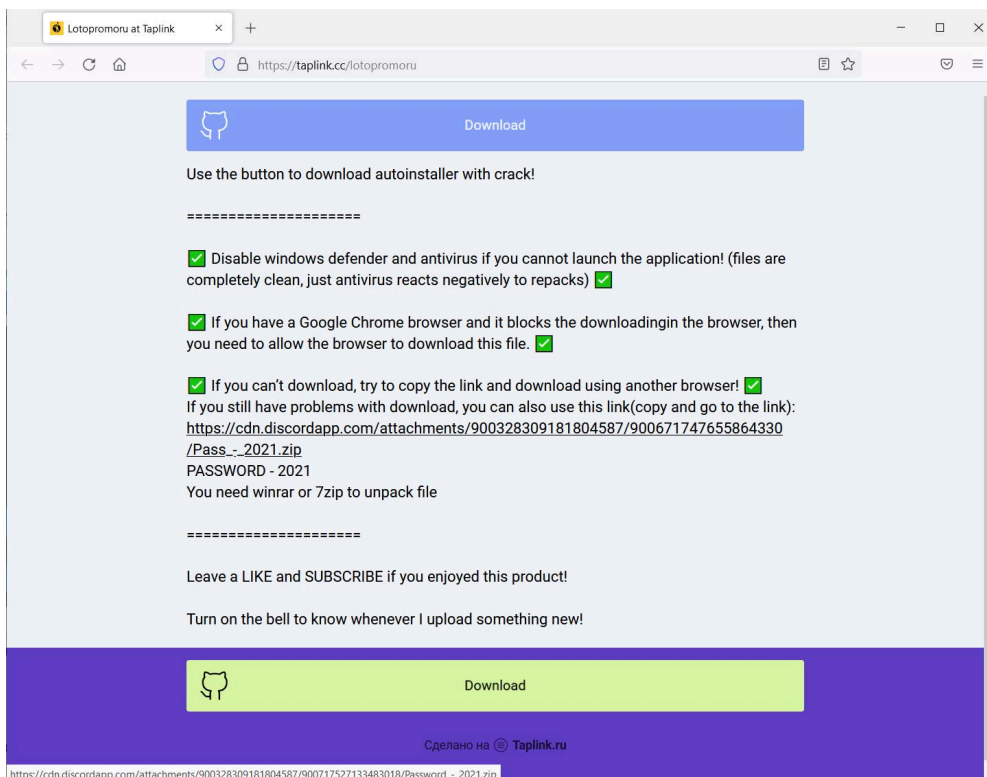
**Example of a malicious YouTube channel**

These videos contain content that explains how to perform a task using a specific program or utility. Additionally, the YouTube video's description includes an alleged link to the associated tool used to distribute the malware.



### Malicious YouTube video pushing RedLine stealer

If a video contains a bit.ly link, it will lead to another file-sharing site hosting the RedLine password-stealing malware infection. However, if it includes an unshortened domain, it will redirect to a page on the taplink[.]cc domain to push Racoon Stealer, as shown below.



### Landing page for the Racoon Stealer

Once a user becomes infected, the malware will proceed to scan all installed browsers and the computer for cryptocurrency wallets, credit cards, passwords, and other data and upload it back to the attacker.

Google told BleepingComputer that they are aware of the campaign and are taking action to disrupt the activity.

"We are aware of this campaign and are currently taking action to block activity by this threat actor and flagging all links to Safe Browsing. As always, we are continuously improving our detection methods and investing in new tools and features that automatically identify and stop threats like this one. It is also important that users remain aware of these types of threats and take appropriate action to further protect themselves." - Google.

Google also disclosed this week a [phishing campaign that distributed password-stealing trojans](#) used to steal the accounts of YouTube Creators. These accounts were then sold on dark web markets or used to perform cryptocurrency scams.

## Downloading software can be dangerous

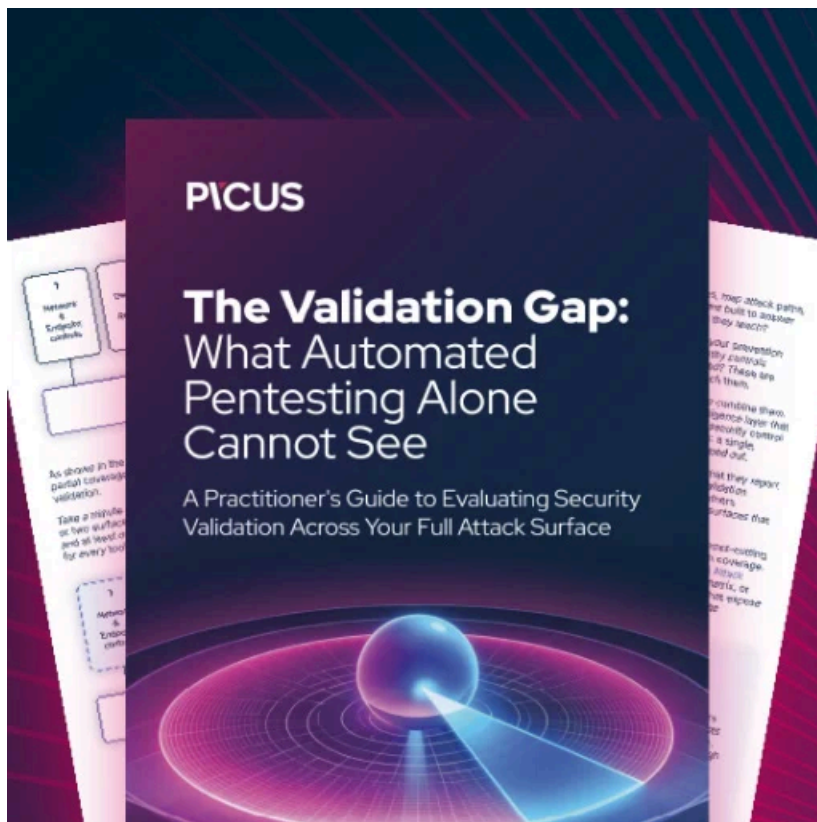
These campaigns illustrate how important it is not to download programs from the Internet haphazardly, as sites like YouTube can not vet every link added by video publishers.

Therefore, a user should research a site before downloading and installing anything from it to determine if they have a good reputation and can be trusted. Even then, it is always suggested that you first upload the program to a site like VirusTotal to confirm if it's safe to run.

If you have accidentally fallen for this attack and installed a program from a similar link, it is strongly suggested that you scan your computer with an antivirus program.

After you have removed any malware detected in a virus scan, you should immediately change any passwords saved in your browsers.

*Update 10/21/21 7:28 PM EST: Added a statement from Google.*



## [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/massive-campaign-uses-youtube-to-push-password-stealing-malware/>