Threat Actors Abuse AI-Generated Youtube Videos to Spread Stealer Malware

By Pavan Karthick M

Published: 2025-08-21 · Archived: 2026-04-05 17:08:01 UTC

Back

Since November 2022 there has been a 200-300% month-on-month increase in Youtube videos containing links to stealer malware such as Vidar, RedLine, and Raccoon in their descriptions. The videos lure users by pretending to be tutorials on how to download cracked versions of software such as Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD, and other products that are licensed products available only to paid users.

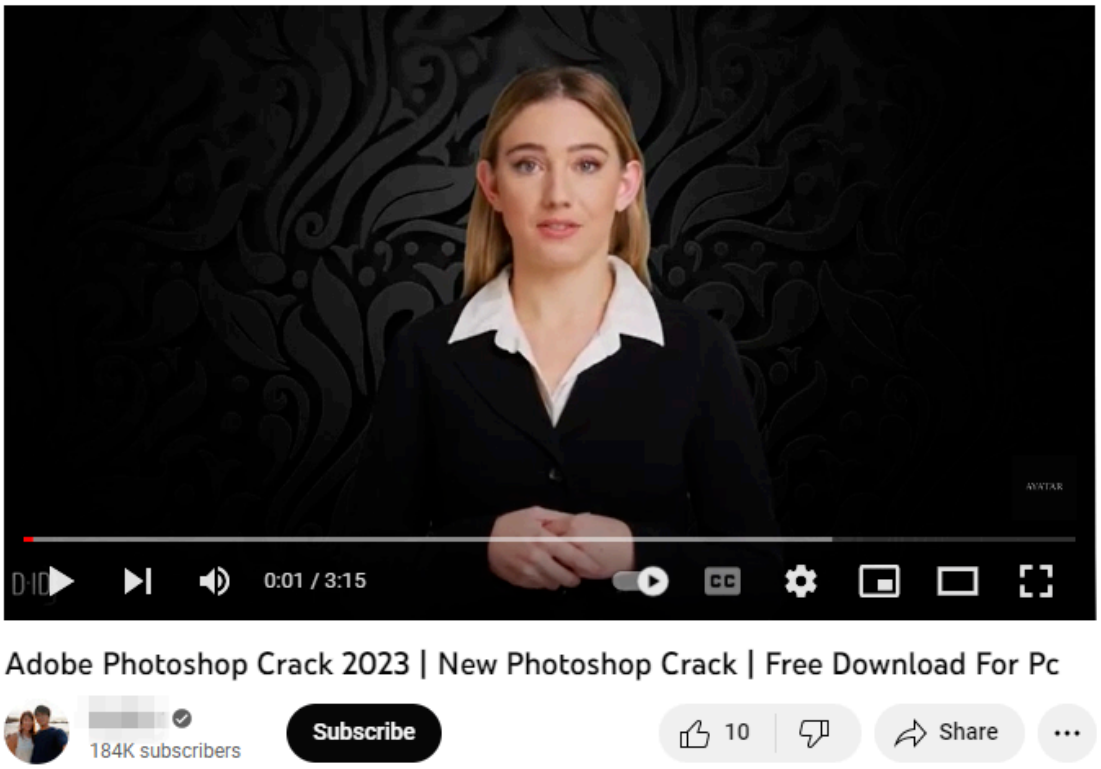
March 13, 2023

Authors: Pavan Karthick M, Deepanjli Paulraj

Rise in Threat Actors Using AI-Generated Youtube Videos

Since November 2022 there has been a **200-300%** month-on-month increase in Youtube videos containing links to stealer malware such as Vidar, RedLine, and Raccoon in their descriptions. The videos lure users by pretending to be tutorials on how to download cracked versions of software such as Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD, and other products that are licensed products available only to paid users.

Usually, the videos use a screen recording or audio walkthrough of the steps to download and install the software. However, there has recently been an increase in the use of AI-generated videos from platforms such as Synthesia and D-ID, being used in the videos. It is well known that videos featuring humans, especially those with certain facial features, appear more familiar and trustworthy. Hence, there has been a recent trend of videos featuring AI-generated personas, across languages and platforms (Twitter, Youtube, Instagram), providing recruitment details, educational training, promotional material, etc. And threat actors have also now adopted this tactic.



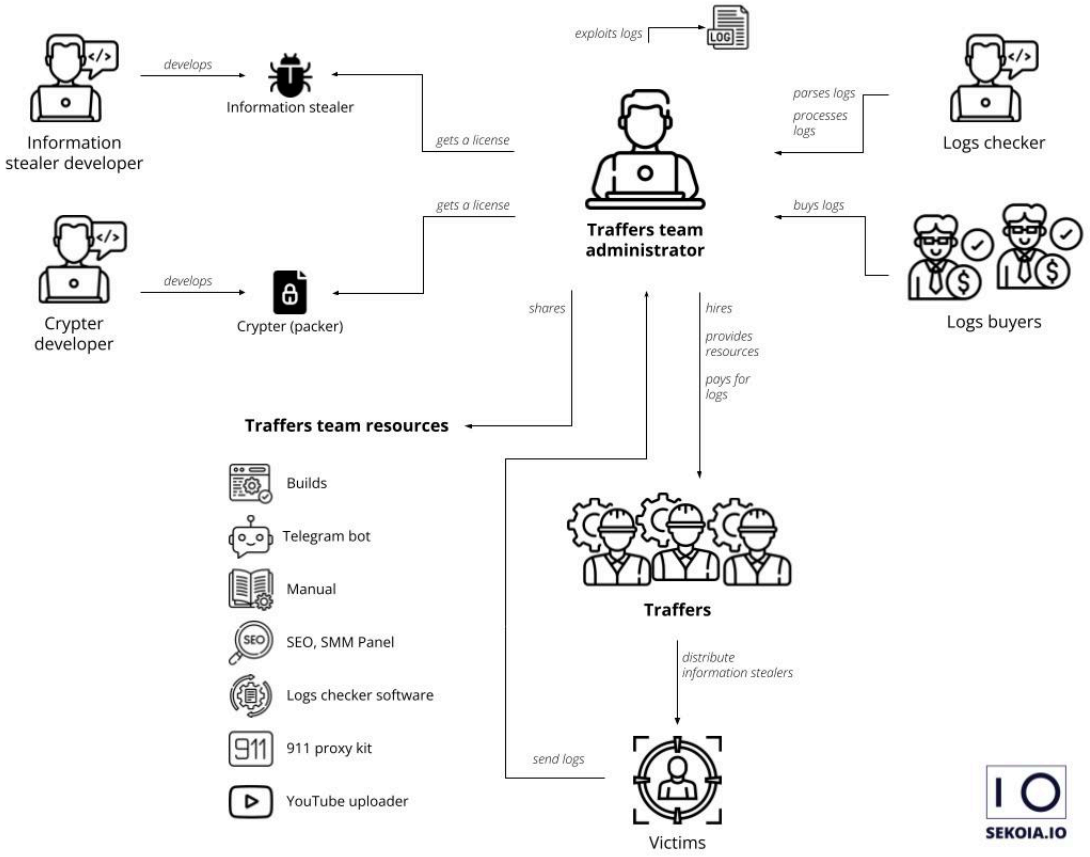
AI-generated video from studio.d-id.com

The Burgeoning Information Stealer Ecosystem

Infostealers are malicious software designed to steal sensitive information from computers. They can steal passwords, credit card information, bank account numbers, and other confidential data. They are usually spread through malicious software downloads, fake websites, and Youtube tutorials. Once installed on a system, they steal information from the computer and upload it to the attacker's Command and Control server.

Information stealers typically collect a victim’s:

- Browser data, including passwords, cookies, extension data, auto-fills, credit card details, etc.
- Crypto wallet data and credentials
- Telegram data and credentials
- Files such as .txt, documents, excel sheets, PowerPoint presentations, etc, using a File Grabber.
- System information such as IP address, malware path (Redline and Vidar only), Timezone, location, system specifications, etc.



Organization of the information stealer ecosystem (Source sekoia.com)

Information Stealer Developers

The developers are responsible for developing and updating the malware code to ensure that antivirus and other endpoint detection systems do not detect the stealer when it is downloaded to a computer. They also work on expanding the scope of the stealer by adding new browsers, wallets, and other applications that the malware can steal information from. Even as EDRs are updated with new IoCs to detect malware, developers continue to iteratively upgrade the malware to evade detection. Hence, EDRs and IoCs are valid only for a short period of time.

> Related Report : Information Stealer Targets Crypto Wallets Via Fake Windows 11 Update

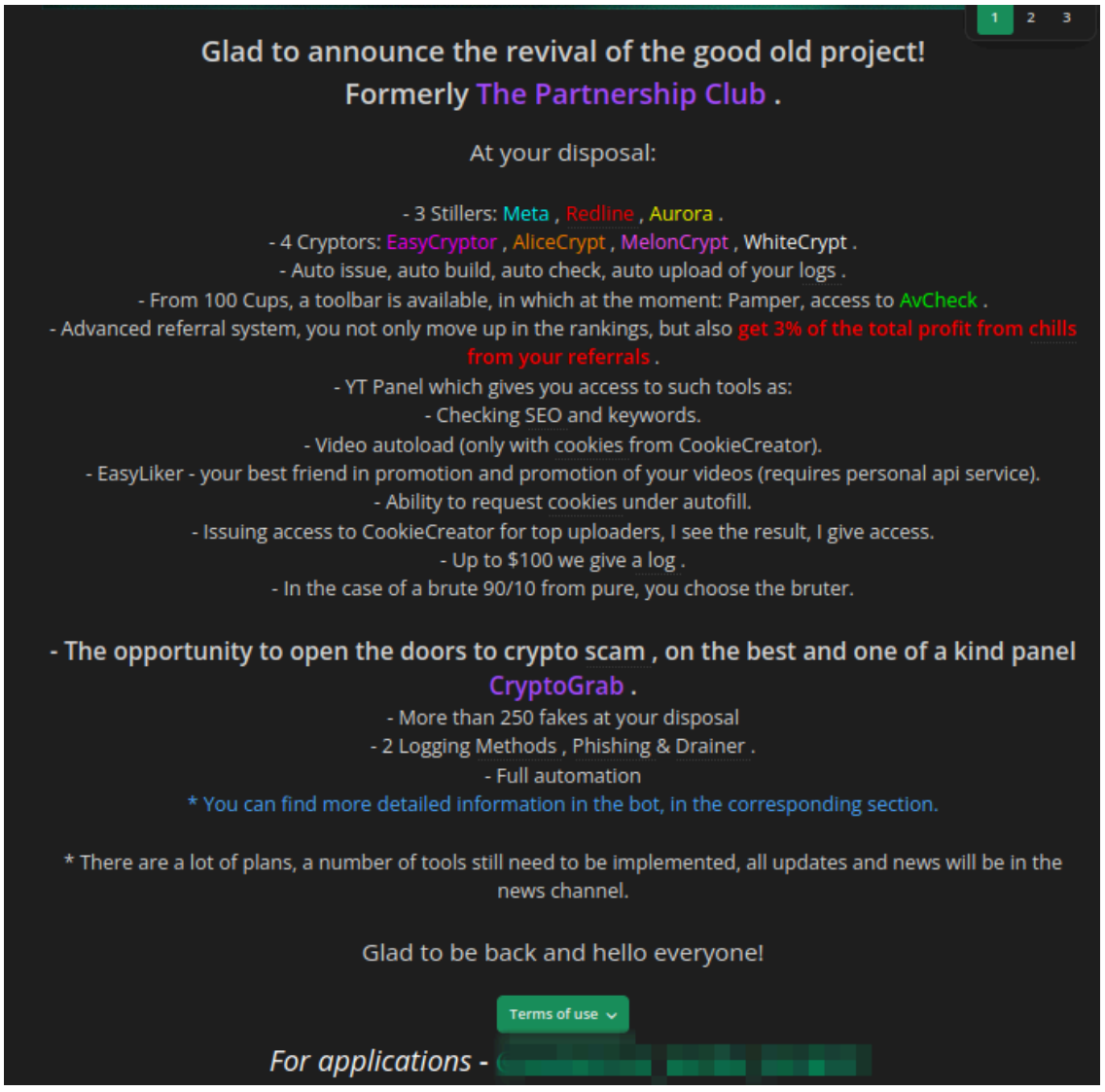
Traffers

Information stealer developers recruit/ partner with other threat actors, commonly known as traffers, to:

- Identify victims via stealer logs, compromised credentials, etc., from underground marketplaces, Telegram channels, and from other traffers.

- Spread the stealer via fake websites, phishing emails, Youtube tutorials, Social media posts, etc.
- Use SEO optimization to ensure the sources of infection are easily visible and available to potential victims.
- Collect, organize, and sell the exfiltrated information on underground forums, Telegram channels, and to other groups that spread stealer malware.

Traffers are recruited via posts and advertisements across various underground forums:



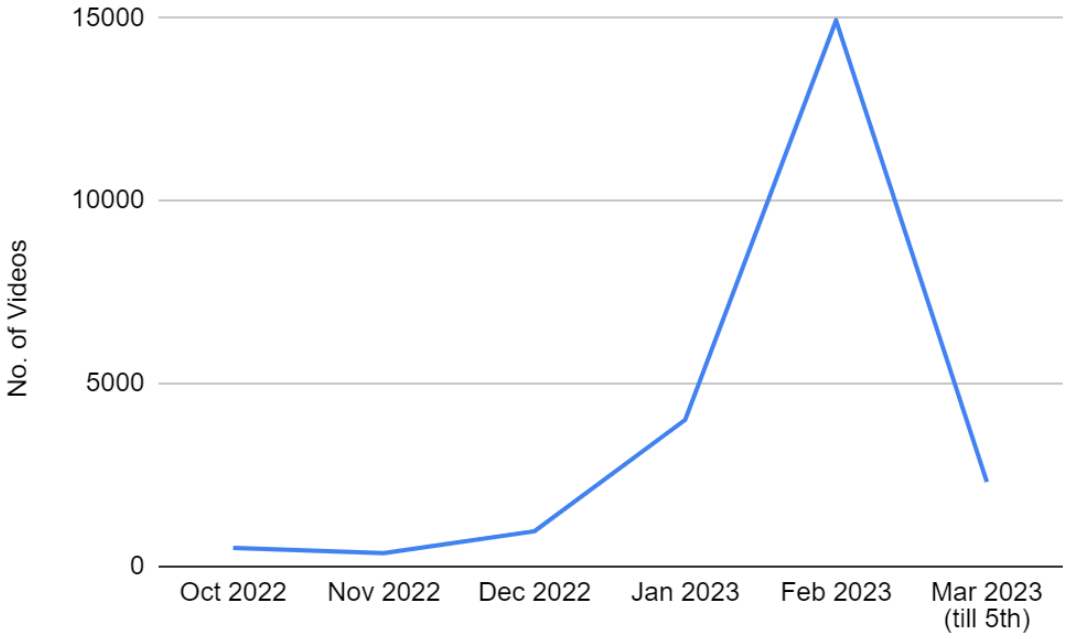
Forum post recruiting Traffers. Claims to have YT panel for 911 infection chain, automated tools for traffic generation

Youtube as a Malware Distribution Channel

With over 2.5 billion active monthly users, Youtube is a popular and versatile platform. From entertainment and reviews to recipes and educational material, Youtube is used by a wide range of users across demographics.

While Youtube is an easy way to reach millions of users, the platform's regulations and review process make it difficult for threat actors to have long-term active accounts on the platform. Once a few users have been affected, the video is usually taken down and the account is banned. Hence threat actors are always looking for new ways to circumvent the platform's algorithm and review process.

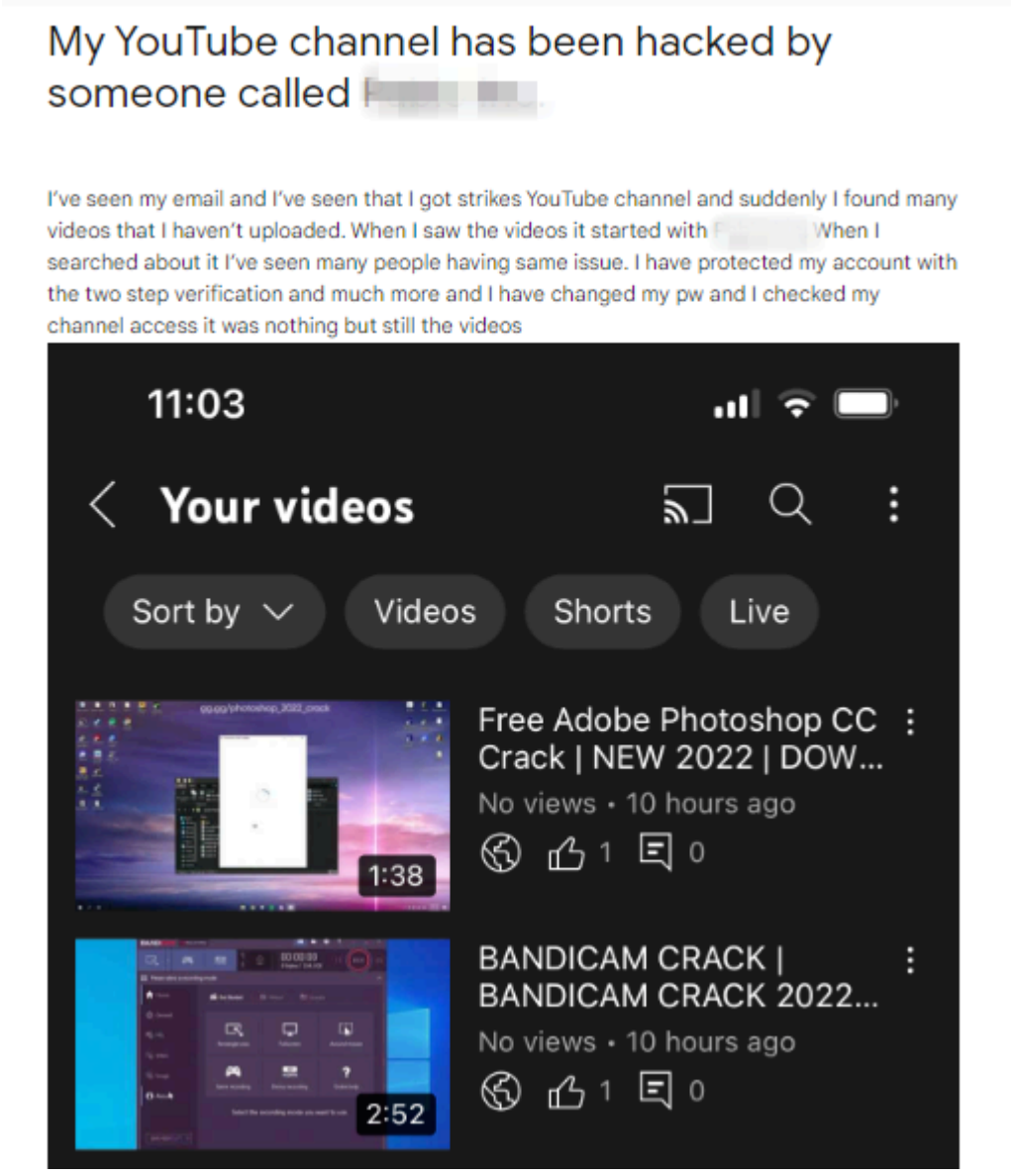
Since November 2022, CloudSEK has observed a 2 to 3 times month-on-month increase in the number of videos spreading stealer malware.



Account Takeover

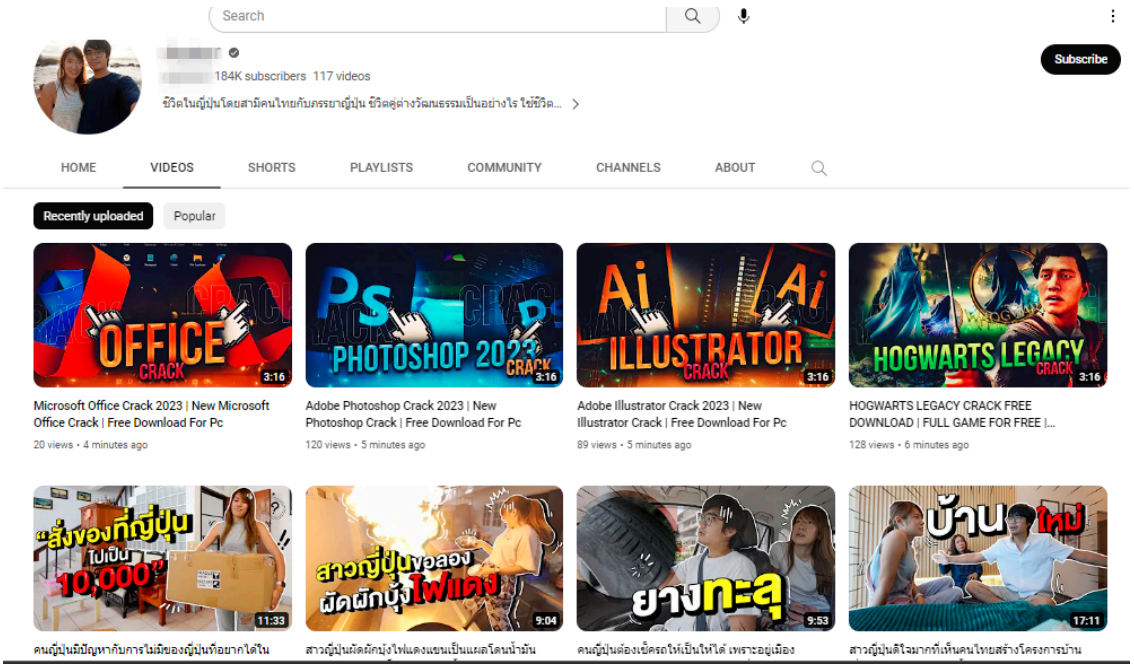
Threat actors use previous data leaks, phishing techniques, and stealer logs to take over existing Youtube accounts. They target both educated and active users (with a significant number of subscribers and uploads) and less educated users.

There have been several reports and complaints regarding Youtube account takeovers. The threat actors immediately upload 5-6 videos to the account.



Taking Over Popular Accounts

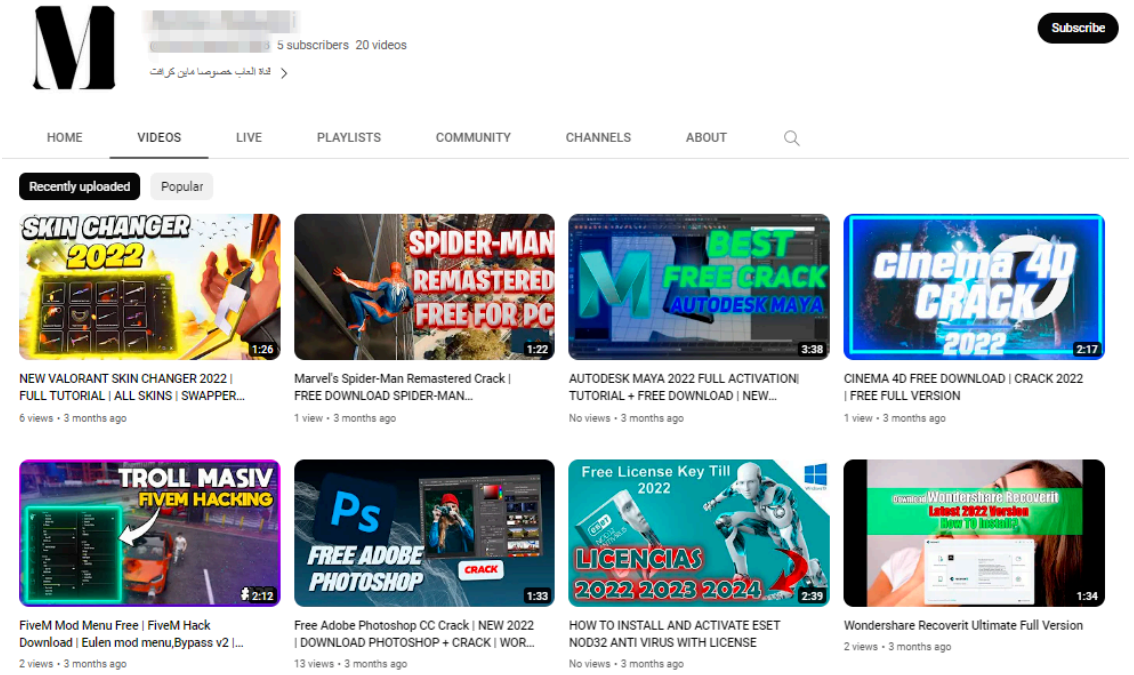
Threat actors target popular accounts with 100K+ subscribers, in an attempt to reach a large audience in a short period of time. Usually, the subscribers of popular accounts will be notified about a new upload. Uploading to such accounts lends video legitimacy as well. However, such Youtubers will report their account taker to Youtube and gain access back to their accounts within a few hours. But in a few hours, hundreds of users could have fallen prey.



A popular Youtuber whose account was flooded with crack download videos

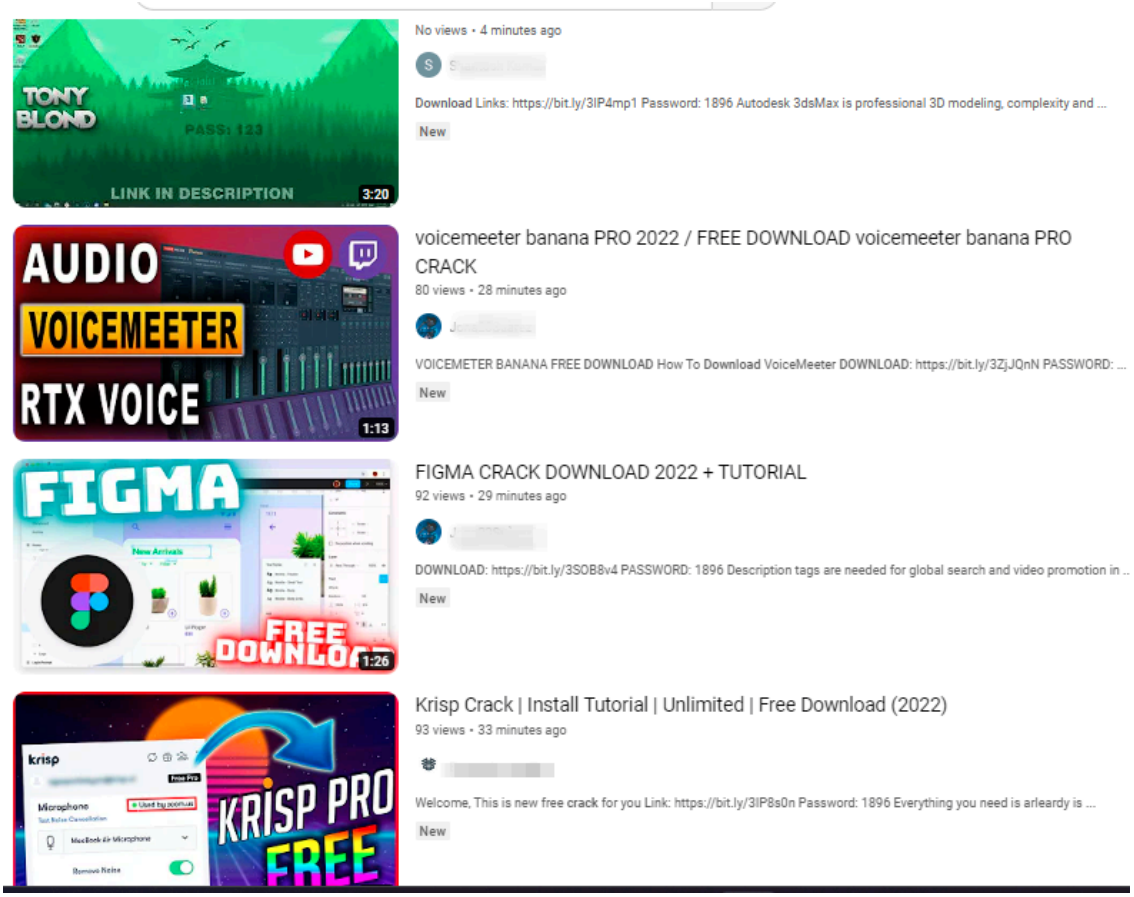
Taking Over Less Popular Accounts

General users, who don't upload videos on a regular basis, may not notice that their account has been taken over for a significant period of time. And even if they lose access to their accounts, they may not have the incentive to report it. As seen in the example below, the malicious videos are available even after 3 months. Despite the limited reach of these accounts, threat actors target them because videos uploaded to them remain available for an extended period of time.



A not-so-popular YouTube account flooded with crack download videos

Automated & Frequent Video Uploads

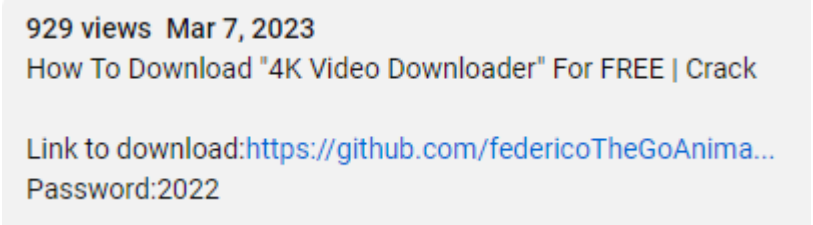


We have observed that every hour 5-10 crack software download videos, containing malicious links, are uploaded to Youtube. This frequent addition of videos compensates for the videos that are deleted or taken down and ensures that at any given time, if a user searches for a tutorial on how to download a cracked software, these malicious videos will be available.

Obfuscated Links

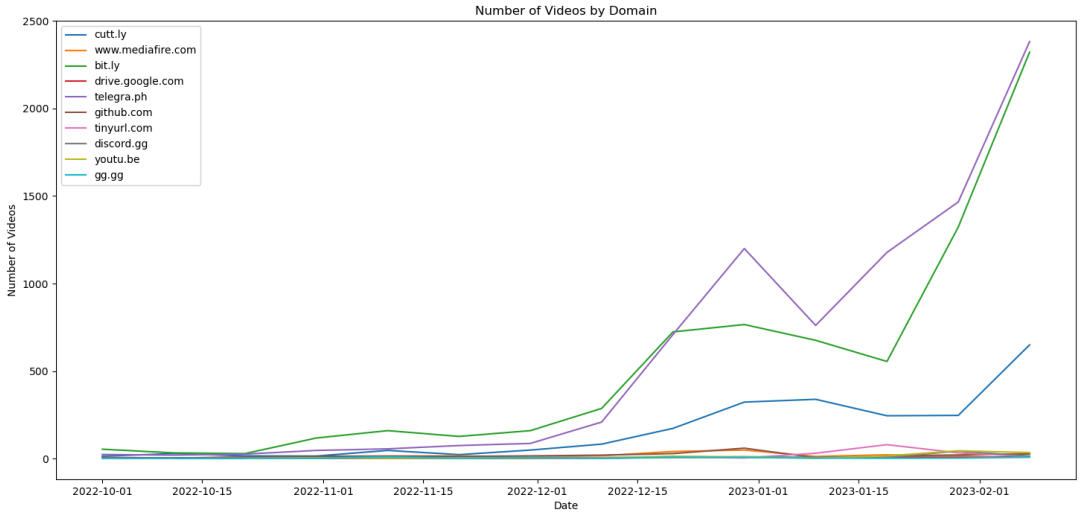
The malicious link to download the malware-laced file is usually included in the description of the video. However, these links don't appear suspicious because the threat actors use:

- URL shorteners such as bit.ly and cutt.ly
- Links to file hosting platforms such as mediafire.com
- Links that directly download the malicious zip file

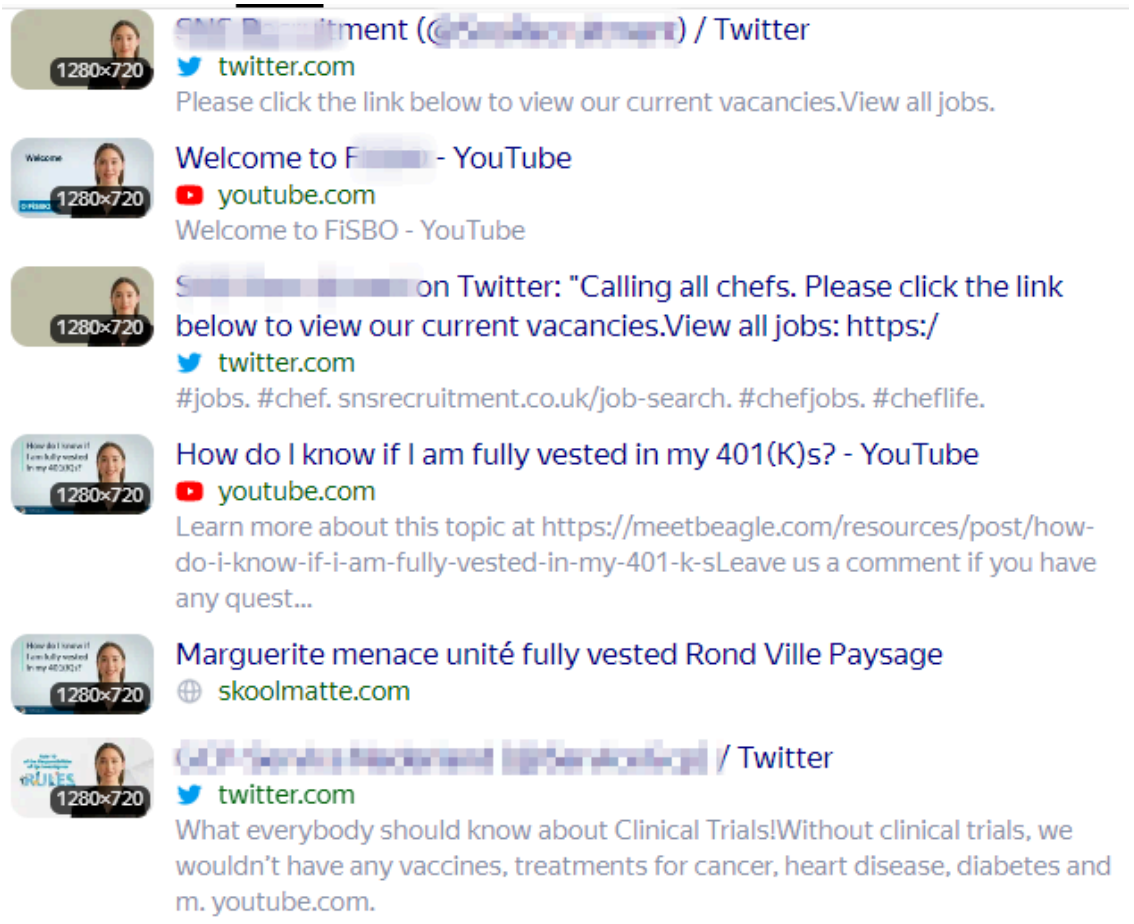


No views Feb 24, 2023 #autodeskmaya #autodesk
Download: https://bit.ly/3IMiGQA
Password: 1896

Commonly seen websites that are used in infection chain are listed in the chart below.

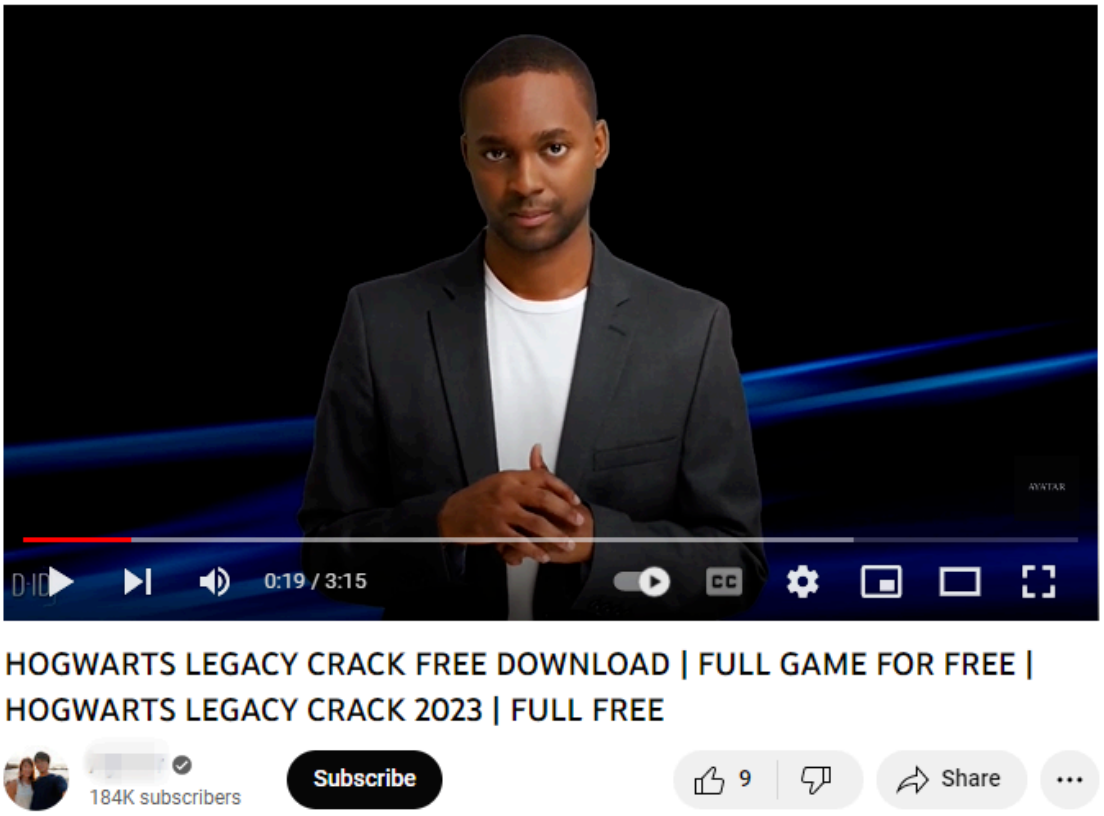


AI-Generated Videos



It is well known that videos featuring humans, especially those certain facial features, appear more familiar and trustworthy. Hence, there has been a recent trend of videos featuring AI generated personas, across languages and platforms (Twitter, Youtube, Instagram), providing recruitment details, educational training, promotional material, etc. And threat actors have also now adopted this tactic.

As seen in the example below, a Hogwarts crack download video generated using d-id.com was uploaded to a Youtube channel with 184K subscribers. And within a few minutes of being uploaded, the video had 9 likes and 120+ views.



The Way Forward

Limitations of String-Based Rules

String-based rules will prove ineffective against malware that dynamically generates strings and/or uses encrypted strings. Encryption and encoding methods differ from sample to sample (eg- new versions of Vidar, Raccoon, etc). In addition, they will only be able to detect the malware family when the sample is unpacked, which is almost never used in a malware campaign.

Real-time Adaptive Threat Monitoring

To address constantly changing threats, organizations need to adopt adaptive threat monitoring. This can only be done by closely monitoring threat actors' changing Tactics, Techniques, and Procedures. It is also important to conduct awareness campaigns and to equip users to identify potential threats.

Apart from this, it is recommended that users enable multi-factor authentication and refrain from clicking on unknown links and emails. Additionally, avoid downloading or using pirated software because the risks greatly outweigh the benefits.

Threat Researcher at CloudSEK, building threat intelligence and automation systems for malware tracking, dark web intelligence, and vulnerability monitoring. He researches stealer ecosystems and cybercrime networks, and speaks at BSides, Null/OWASP, and HITB on AI-driven security automation.

Deepanjli is CloudSEK's Lead Technical Content Writer and Editor. She is a pen wielding pedant with an insatiable appetite for books, Sudoku, and epistemology.

Subscribe to CloudSEK Resources

Get the latest industry news, threats and resources.

Related Blogs

Predict Cyber Threats against your organization
