

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

 cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware

Pavan Karthick M



Malware Intelligence

7

mins read

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.



Pavan Karthick M

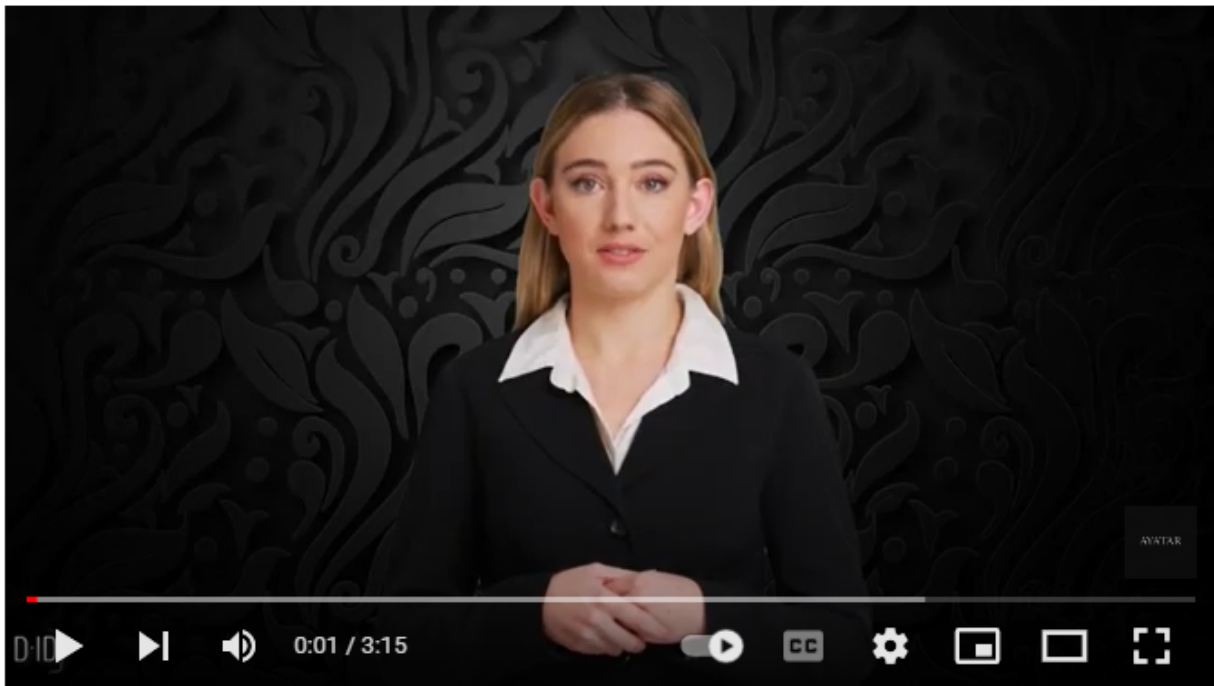
March 13, 2023

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.



Adobe Photoshop Crack 2023 | New Photoshop Crack | Free Download For Pc



184K subscribers

Subscribe

10



Share



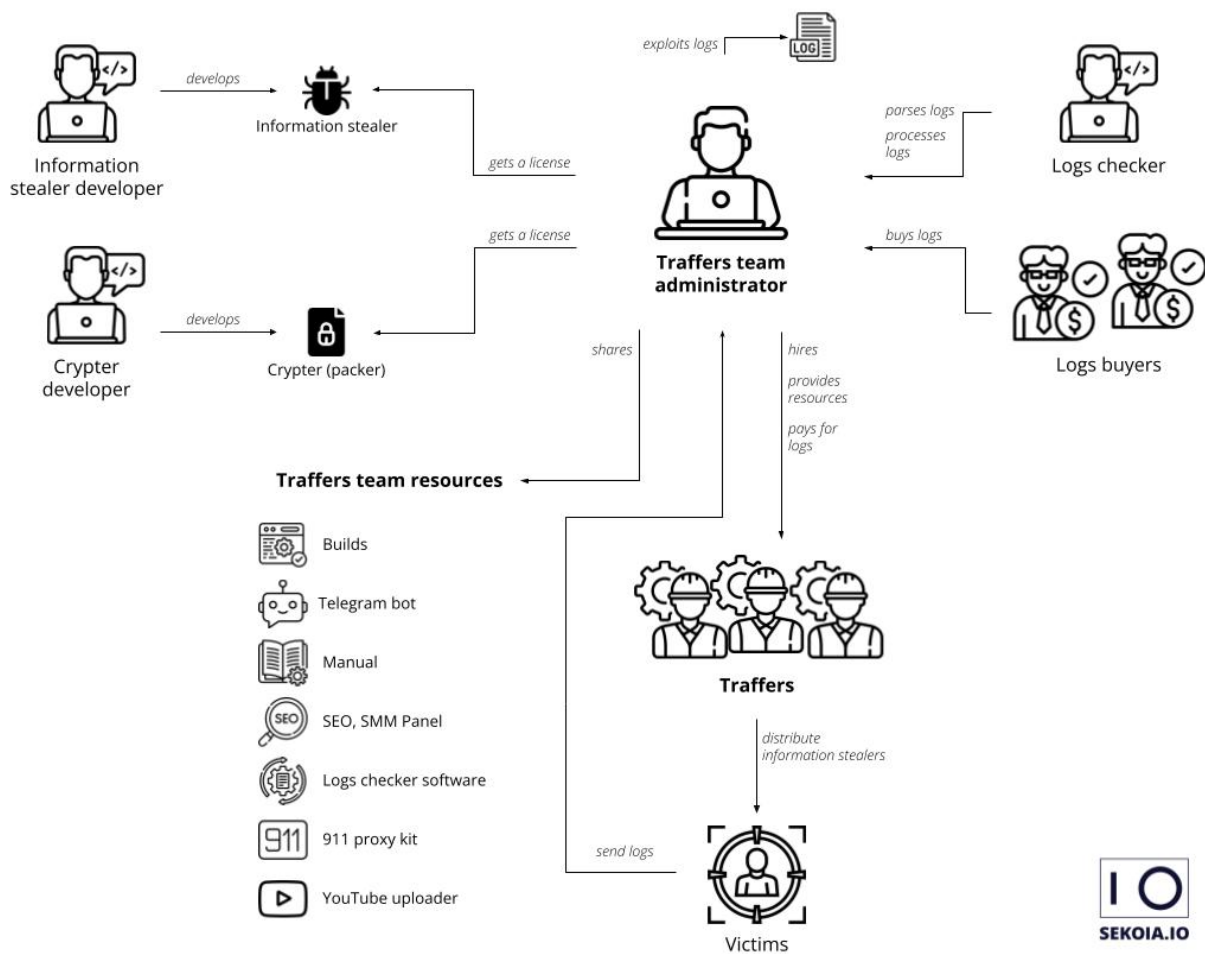
AI-generated video from studio.d-id.com

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

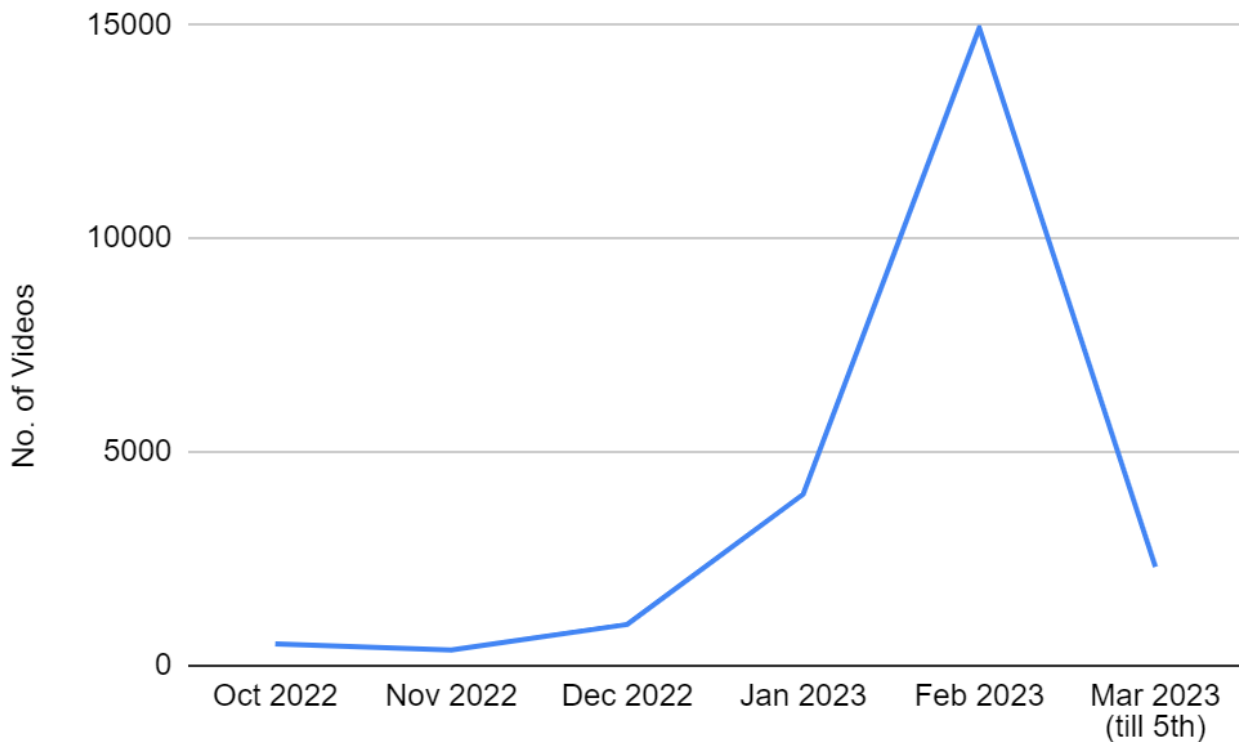
Information stealer developers recruit/ partner with other threat actors, commonly known as traffers, to:

- 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:

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.



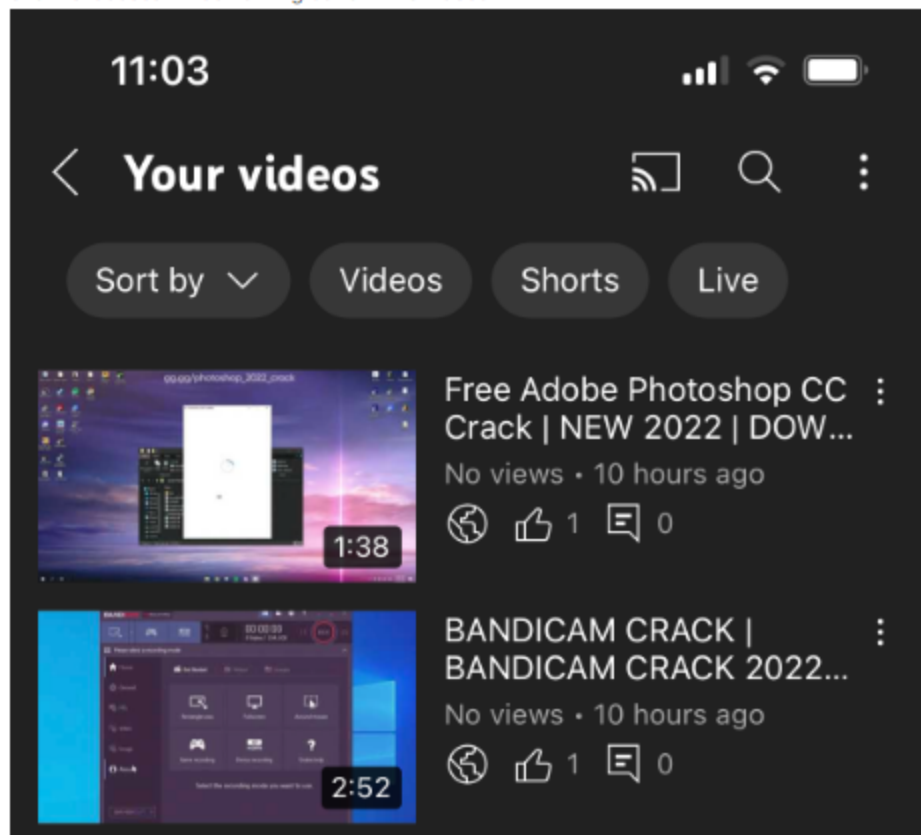
Account Takeover

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.

My YouTube channel has been hacked by someone called [REDACTED]

I've seen my email and I've seen that I got strikes YouTube channel and suddenly I found many videos that I haven't uploaded. When I saw the videos it started with [REDACTED] When I searched about it I've seen many people having same issue. I have protected my account with the two step verification and much more and I have changed my pw and I checked my channel access it was nothing but still the videos



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.

Search

184K subscribers 117 videos

ชีวิตในญี่ปุ่นโดยสามมิตรไทยกับภรรยาญี่ปุ่น ชีวิตคู่ต่างวัฒนธรรมเป็นอย่างไร ใช้ชีวิต... >

HOME VIDEOS SHORTS PLAYLISTS COMMUNITY CHANNELS ABOUT

Recently uploaded Popular

Microsoft Office Crack 2023 | New Microsoft Office Crack | Free Download For Pc 3:16
20 views • 4 minutes ago

Adobe Photoshop Crack 2023 | New Photoshop Crack | Free Download For Pc 3:16
120 views • 5 minutes ago

Adobe Illustrator Crack 2023 | New Illustrator Crack | Free Download For Pc 3:16
89 views • 5 minutes ago

HOGWARTS LEGACY CRACK FREE DOWNLOAD | FULL GAME FOR FREE [...] 3:16
128 views • 6 minutes ago

“สิ่งของที่ญี่ปุ่นไปสิบ 10,000” 11:33
คนญี่ปุ่นมีปัญหากับการไม่มีของญี่ปุ่นที่อยากได้ใน

สาวญี่ปุ่นผัดผัดปรุงไฟแดงแซ่บเป็นแกลโตน้ำมัน 9:04
สาวญี่ปุ่นผัดผัดปรุงไฟแดงแซ่บเป็นแกลโตน้ำมัน

ย่างทะลุ 9:53
คนญี่ปุ่นต้องเข็ดรถไฟเป็นใจได้ เพราะอยู่เมือง

บ้านใหม่ 17:11
สาวญี่ปุ่นดีใจมากที่เห็นคนไทยสร้างโครงการบ้าน

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.



5 subscribers 20 videos
قناة الالعاب خصوصا ماين كرافت >

Subscribe

HOME VIDEOS LIVE PLAYLISTS COMMUNITY CHANNELS ABOUT

Recently uploaded Popular



NEW VALORANT SKIN CHANGER 2022 | FULL TUTORIAL | ALL SKINS | SWAPPER...
6 views · 3 months ago



Marvel's Spider-Man Remastered Crack | FREE DOWNLOAD SPIDER-MAN...
1 view · 3 months ago



AUTODESK MAYA 2022 FULL ACTIVATION | TUTORIAL + FREE DOWNLOAD | NEW...
No views · 3 months ago



CINEMA 4D FREE DOWNLOAD | CRACK 2022 | FREE FULL VERSION
1 view · 3 months ago



FiveM Mod Menu Free | FiveM Hack Download | Eulen mod menu, Bypass v2 |...
2 views · 3 months ago



Free Adobe Photoshop CC Crack | NEW 2022 | DOWNLOAD PHOTOSHOP + CRACK | WOR...
13 views · 3 months ago



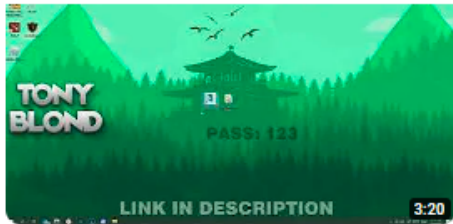
HOW TO INSTALL AND ACTIVATE ESET NOD32 ANTI VIRUS WITH LICENSE
No views · 3 months ago



Wondershare Recoverit Ultimate Full Version
2 views · 3 months ago

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

Automated & Frequent Video Uploads



No views • 4 minutes ago

S [channel name]

Download Links: <https://bit.ly/3IP4mp1> Password: 1896 Autodesk 3dsMax is professional 3D modeling, complexity and ...

New



voicemeeter banana PRO 2022 / FREE DOWNLOAD voicemeeter banana PRO CRACK

80 views • 28 minutes ago

J [channel name]

VOICEMETER BANANA FREE DOWNLOAD How To Download VoiceMeeter DOWNLOAD: <https://bit.ly/3ZjJQnN> PASSWORD: ...

New



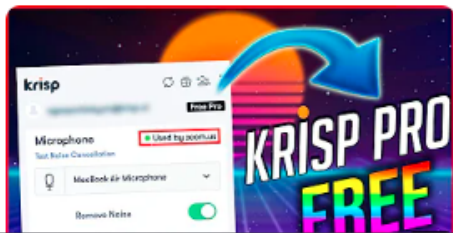
FIGMA CRACK DOWNLOAD 2022 + TUTORIAL

92 views • 29 minutes ago

J [channel name]

DOWNLOAD: <https://bit.ly/3SOBBv4> PASSWORD: 1896 Description tags are needed for global search and video promotion in ...

New



Krisp Crack | Install Tutorial | Unlimited | Free Download (2022)

93 views • 33 minutes ago

[channel name]

Welcome, This is new free crack for you Link: <https://bit.ly/3IP8s0n> Password: 1896 Everything you need is already is ...

New

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.

SEO Optimization Using Region-Specific Tags

Threat actors add an exhaustive list of tags that will deceive the Youtube algorithm to recommend the video and ensure it appears as one of the top results. While the tags include keywords relevant to the software, it also includes random keywords in different languages.

IGNORE TAGS:

blender, blender tutorial, blender guru, blender 3d, blender crack, blender cracked glass, blender crack tutorial, how to download and install blender, how to download blender 3d, how to install blender, install blender, how to download blender, download blender, blender 2.8, blender animation, procedural, how to create cracks in blender, download blender 3d, how to download blender for windows 10, download blender, blender download windows 10, blender 2.9, quad remesher, quad remesher for blender, download quad

Example of tags used in YouTube for SEO purposes

In the example below, the tags include keywords related to **Indian and Pakistani TV channels, TV programs, and phrases in local languages.**

latest, blender 3d, techniques, maya 2022 bonus tools, easy, instructions, 2016, maya 2017, maya 2018, vfx, autodesk maya 2020, learn to, system requirements, chamfer, normals, pakistani drama, maya 2020, stylized, top pakistani dramas, ary digital drama, gratis, espanol, substance designer, workflow, bake, perfect, fix, pbr, physically based, pipeline, animation, controls, startup, mesh, particles, vr for maya, how to download autodesk maya 2022 free, where to get maya 2022, vr for maya 2022, fundamental, water, patreon, maya 2022 free, maya modelling, bifrost, fluids, dynamics, how to install maya 2022, video, rig, rigging in maya, download, uv, gamedev, game rig, game development, #autodesk, get maya for free, maya3d, how do i, game rigging, sun marathi serial episodes, autodesk maya price in india, abhalachi maya serial, organic modeling in maya, polygon modeling, modeling an alligator, autodesk maya price, sant gajanan shegaviche, abhalachi maya marathi serial, modeling in maya, nandini serial, nandhini serial, autodesk maya system requirements, sun marathi nandini, autodesk maya student, marathi channel serial, nandini marathi serial, autodesk cad

Example of tags used in YouTube for SEO purposes

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

929 views Mar 7, 2023

How To Download "4K Video Downloader" For FREE | Crack

Link to download: <https://github.com/federicoTheGoAnima...>

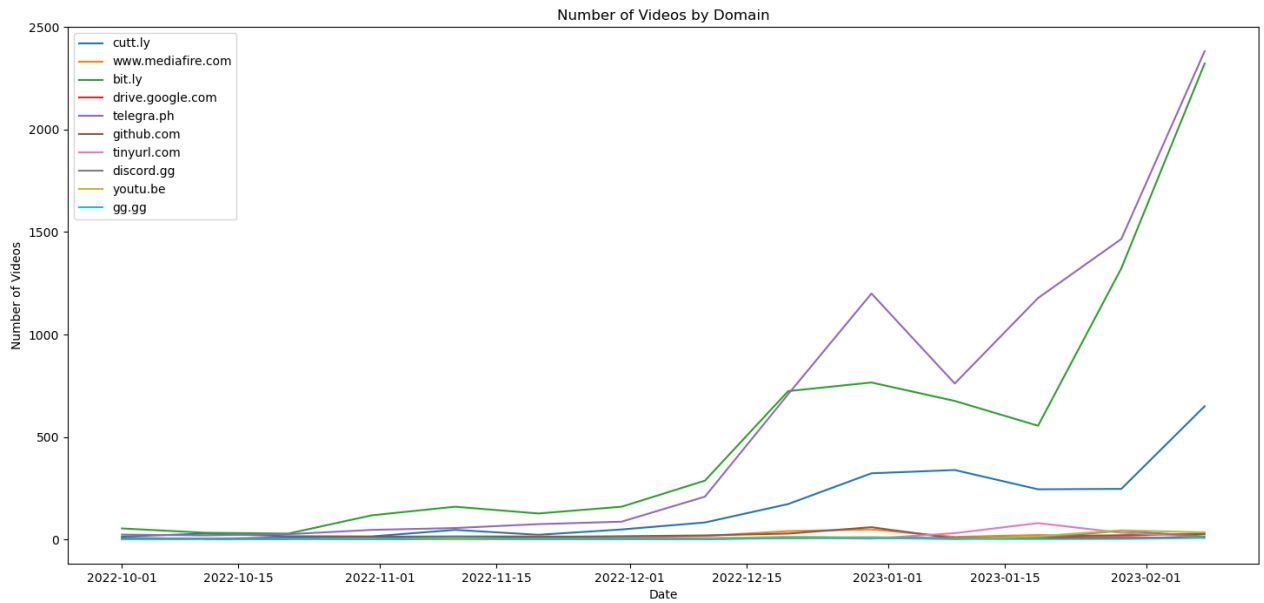
Password:2022

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.



Using Fake Comments to Give the Videos Legitimacy

Threat actors add several comments claiming that the cracked software worked for them. This lends the videos an air of legitimacy and misleads users into believing that the malicious download is legitimate. As seen in the examples below, several videos have identical comments within an hour of being posted, which indicates that the threat actors have automated the process of adding fake comments to videos.

Cubase 12 Pro Crack \ Free download 2022 \ Crack 2022



451 subscribers

Subscribe

284 views 1 hour ago

🔗 **DOWNLOAD:** <https://bit.ly/3yigJoH>

🔗 **PASSWORD:** 1896

Show more

7 Comments Sort by



Add a comment...



1 hour ago

Thank you so much Sense!! You are a blessing!

👍 Reply



1 hour ago

thank you straight to the point

👍 Reply



1 hour ago

thank you soo much very direct link n works for me love the way you expressed the installation .

👍 Reply



1 hour ago

BROTHER, YOU ARE THE BEST!!! You oooh really helped me!! THANK YOU VERY MUCH!This is cool, well done!

👍 Reply



1 hour ago

THANKS FOR THIS IV BEEN SEARCHING FO SOOO LONG

👍 Reply



1 hour ago

Nice tutorial.... Very helpful

👍 Reply

HOW TO DOWNLOAD VIDIQ BOOST CRACK 2022



25.4K subscribers

Subscribe

277 views 1 hour ago
DOWNLOAD - <https://bit.ly/3mwLCDx>
pass-1896
Show more

6 Comments Sort by



Add a comment...



1 hour ago
Thank you so much Sensei! You are a blessing!

Reply



1 hour ago
thank you straight to the point

Reply



1 hour ago
man I missed this kind of tutorials lol. Great work here, thanks!!!

Reply



1 hour ago
BROTHER, YOU ARE THE BEST!!! You ooh really helped me!! THANK YOU VERY MUCH!This is cool, well done!

Reply



1 hour ago
THANKS FOR THIS IV BEEN SEARCHING FO SOOO LONG

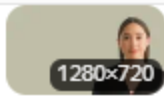
Reply



1 hour ago
thank you soo much very direct link n works for me love the way you expressed the installation .

Reply

AI-Generated Videos



SNS Recruitment (@snsrecruitment) / Twitter

twitter.com

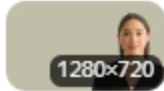
Please click the link below to view our current vacancies.View all jobs.



Welcome to FISBO - YouTube

youtube.com

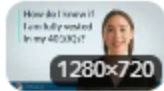
Welcome to FISBO - YouTube



SNS Recruitment on Twitter: "Calling all chefs. Please click the link below to view our current vacancies.View all jobs: https://

twitter.com

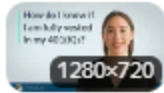
#jobs. #chef. snsrecruitment.co.uk/job-search. #chefjobs. #cheflife.



How do I know if I am fully vested in my 401(K)s? - YouTube

youtube.com

Learn more about this topic at https://meetbeagle.com/resources/post/how-do-i-know-if-i-am-fully-vested-in-my-401-k-sLeave us a comment if you have any quest...



Marguerite menace unité fully vested Rond Ville Paysage

skoolmatte.com



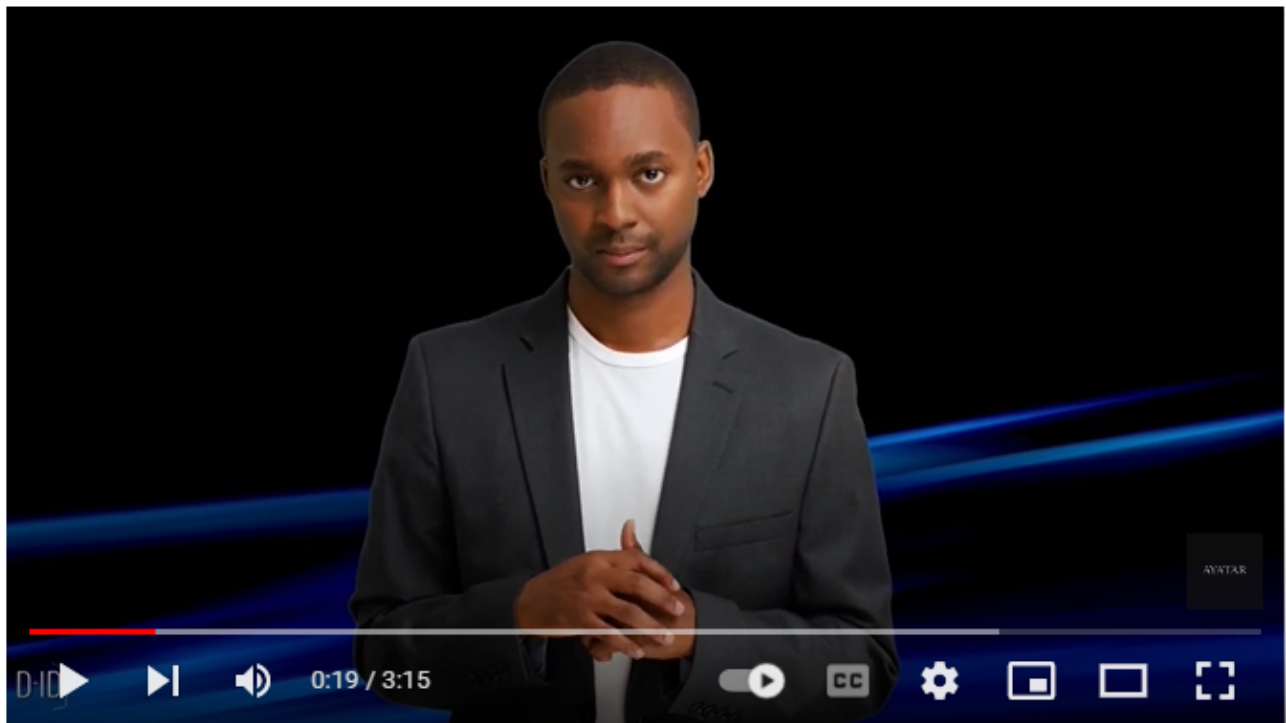
SNS Recruitment (@snsrecruitment) / Twitter

twitter.com

What everybody should know about Clinical Trials!Without clinical trials, we wouldn't have any vaccines, treatments for cancer, heart disease, diabetes and m. youtube.com.

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.



HOGWARTS LEGACY CRACK FREE DOWNLOAD | FULL GAME FOR FREE |
HOGWARTS LEGACY CRACK 2023 | FULL FREE



184K subscribers

Subscribe

9 | | Share | ...

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.

Author



Pavan Karthick M

Threat Intelligence Researcher at CloudSEK

Predict Cyber threats against your organization

Schedule a Demo



Malware Intelligence

★
7

min read

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.

Authors



Pavan Karthick M

Threat Intelligence Researcher at CloudSEK

Co-Authors

Deepanjli Paulraj

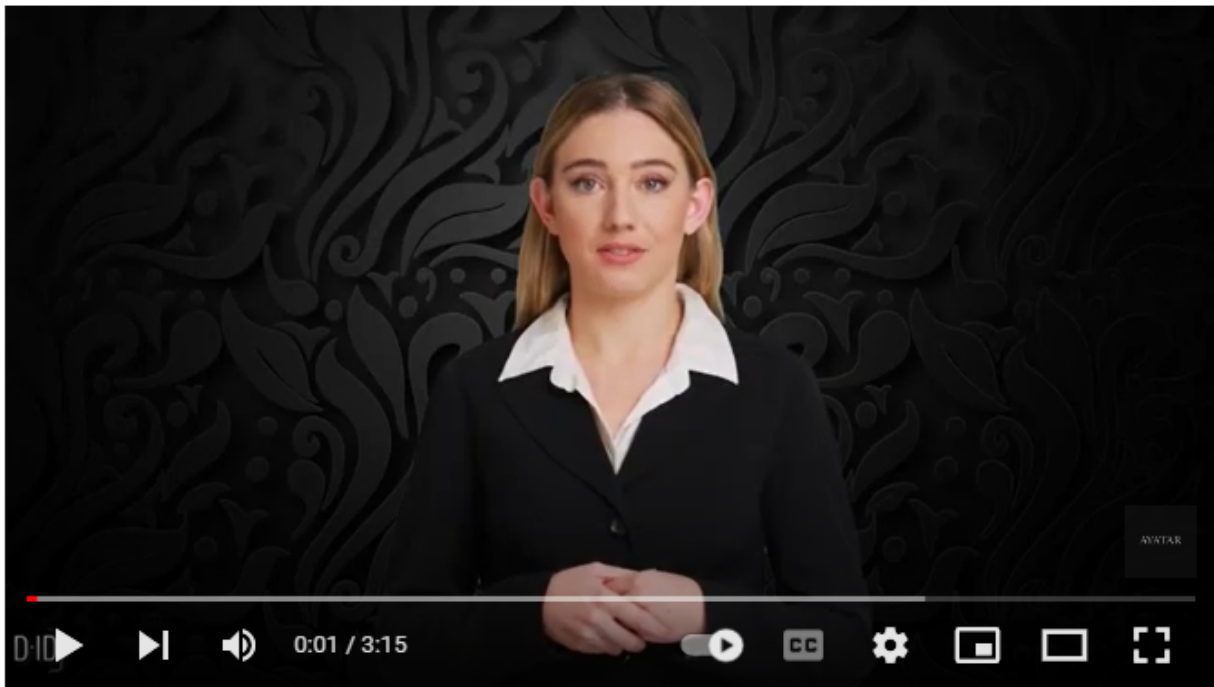


Authors: Pavan Karthick M, Deepanjli Paulraj

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.



Adobe Photoshop Crack 2023 | New Photoshop Crack | Free Download For Pc



184K subscribers

Subscribe

10



Share



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

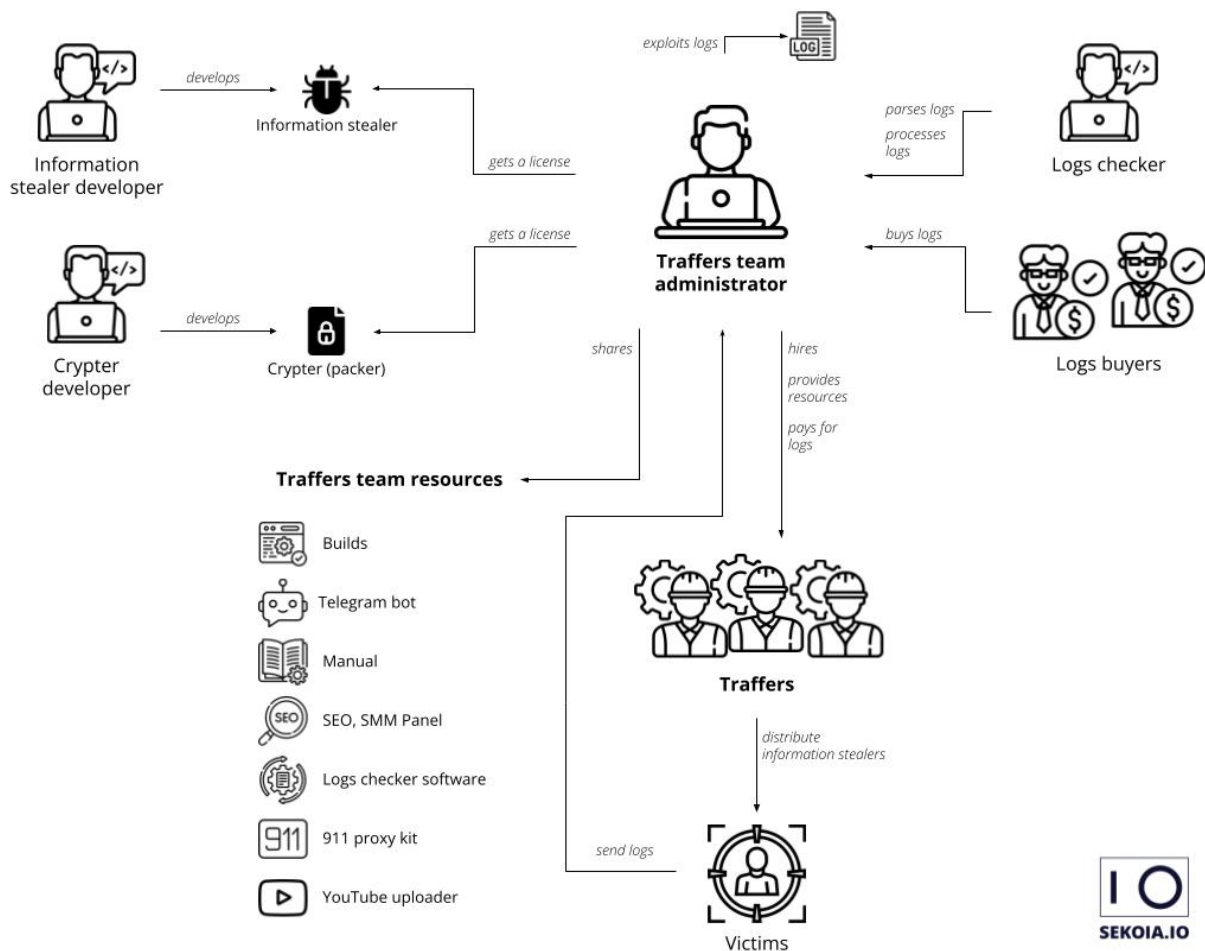
The Burgeoning Information Stealer Ecosystem

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.

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:

1 2 3

Glad to announce the revival of the good old project! Formerly **The Partnership Club** .

At your disposal:

- 3 Stillers: **Meta** , **Redline** , **Aurora** .
- 4 Cryptors: **EasyCryptor** , **AliceCrypt** , **MelonCrypt** , **WhiteCrypt** .
- Auto issue, auto build, auto check, auto upload of your logs .
- From 100 Cups, a toolbar is available, in which at the moment: Pamper, access to **AvCheck** .
- Advanced referral system, you not only move up in the rankings, but also **get 3% of the total profit from chills from your referrals** .
- YT Panel which gives you access to such tools as:
 - Checking SEO and keywords.
 - Video autoload (only with cookies from CookieCreator).
- EasyLiker - your best friend in promotion and promotion of your videos (requires personal api service).
 - Ability to request cookies under autofill.
- Issuing access to CookieCreator for top uploaders, I see the result, I give access.
 - Up to \$100 we give a log .
- In the case of a brute 90/10 from pure, you choose the bruter.

- The opportunity to open the doors to crypto scam , on the best and one of a kind panel **CryptoGrab .**


- More than 250 fakes at your disposal
- 2 Logging Methods , Phishing & Drainer .
- Full automation

* You can find more detailed information in the bot, in the corresponding section.

* There are a lot of plans, a number of tools still need to be implemented, all updates and news will be in the news channel.

Glad to be back and hello everyone!

[Terms of use](#) ▾

For applications - 

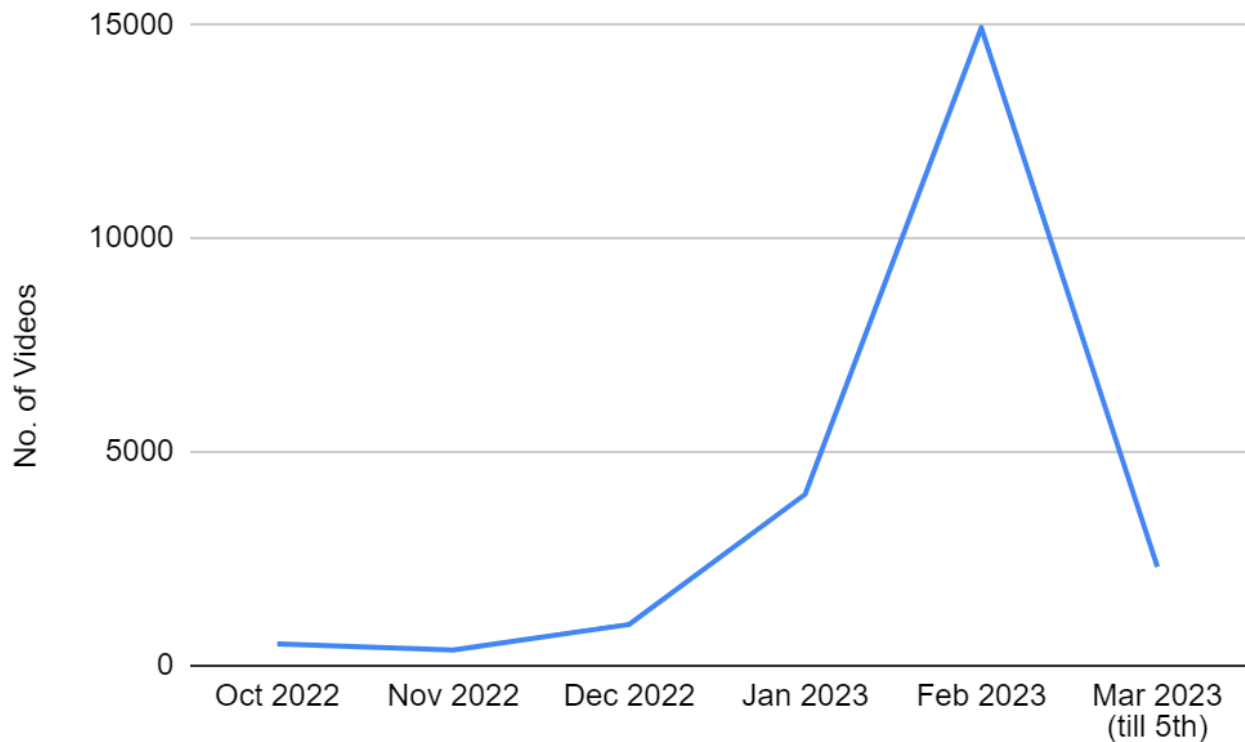
Forum post recruiting Traffers. Claims to have YT panel for 911 infection chain, automated tools for traffic generation

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.



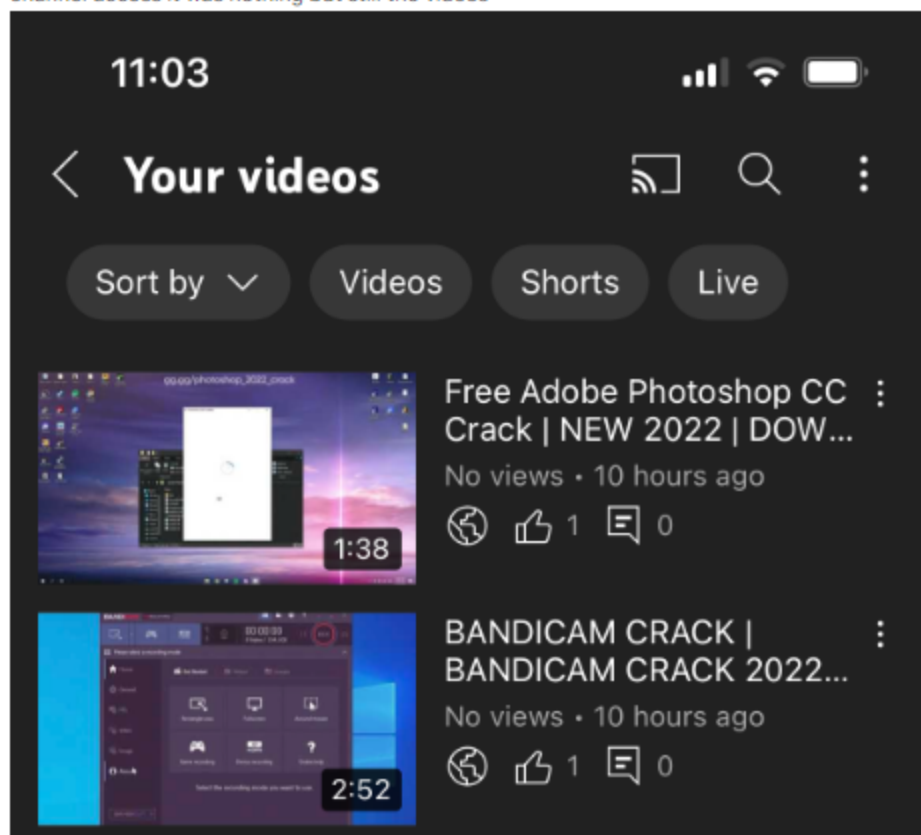
Account Takeover

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.

My YouTube channel has been hacked by someone called [REDACTED]

I've seen my email and I've seen that I got strikes YouTube channel and suddenly I found many videos that I haven't uploaded. When I saw the videos it started with [REDACTED] When I searched about it I've seen many people having same issue. I have protected my account with the two step verification and much more and I have changed my pw and I checked my channel access it was nothing but still the videos



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.

Search

184K subscribers 117 videos

ชีวิตในญี่ปุ่นโดยสามมิตรไทยกับภรรยาญี่ปุ่น ชีวิตคู่ต่างวัฒนธรรมเป็นอย่างไร ใช้ชีวิต... >

HOME VIDEOS SHORTS PLAYLISTS COMMUNITY CHANNELS ABOUT

Recently uploaded Popular

Microsoft Office Crack 2023 | New Microsoft Office Crack | Free Download For Pc
20 views • 4 minutes ago

Adobe Photoshop Crack 2023 | New Photoshop Crack | Free Download For Pc
120 views • 5 minutes ago

Adobe Illustrator Crack 2023 | New Illustrator Crack | Free Download For Pc
89 views • 5 minutes ago

HOGWARTS LEGACY CRACK FREE DOWNLOAD | FULL GAME FOR FREE [...]
128 views • 6 minutes ago

“สิ่งของที่ญี่ปุ่น ไปปีน 10,000”
11:33
คนญี่ปุ่นมีปัญหากับการไม่มีของญี่ปุ่นที่อยากได้ใน

สาวญี่ปุ่นขอลอง ผัดเผ็ดกุ้งไฟแดง
9:04
สาวญี่ปุ่นผัดผัดกุ้งไฟแดงแซ่บเป็นแกลโตน่ามัน

ย่างทะเล
9:53
คนญี่ปุ่นต้องเข็ดรถไฟเป็นใจได้ เพราะอยู่เมือง

บ้านใหม่
17:11
สาวญี่ปุ่นดีใจมากที่เห็นคนไทยสร้างโครงการบ้าน

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.



5 subscribers 20 videos
قناة الالعاب خصوصا ماين كرافت >

Subscribe

HOME VIDEOS LIVE PLAYLISTS COMMUNITY CHANNELS ABOUT

Recently uploaded Popular



NEW VALORANT SKIN CHANGER 2022 | FULL TUTORIAL | ALL SKINS | SWAPPER...
6 views · 3 months ago



Marvel's Spider-Man Remastered Crack | FREE DOWNLOAD SPIDER-MAN...
1 view · 3 months ago



AUTODESK MAYA 2022 FULL ACTIVATION | TUTORIAL + FREE DOWNLOAD | NEW...
No views · 3 months ago



CINEMA 4D FREE DOWNLOAD | CRACK 2022 | FREE FULL VERSION
1 view · 3 months ago



FiveM Mod Menu Free | FiveM Hack Download | Eulen mod menu, Bypass v2 |...
2 views · 3 months ago



Free Adobe Photoshop CC Crack | NEW 2022 | DOWNLOAD PHOTOSHOP + CRACK | WOR...
13 views · 3 months ago



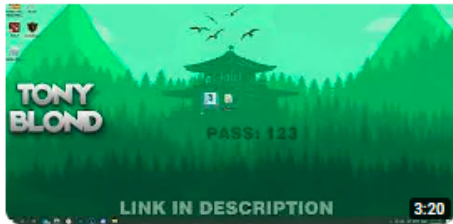
HOW TO INSTALL AND ACTIVATE ESET NOD32 ANTI VIRUS WITH LICENSE
No views · 3 months ago



Wondershare Recoverit Ultimate Full Version
2 views · 3 months ago

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

Automated & Frequent Video Uploads



No views • 4 minutes ago

[S...](#)

Download Links: <https://bit.ly/3IP4mp1> Password: 1896 Autodesk 3dsMax is professional 3D modeling, complexity and ...

New



voicemeeter banana PRO 2022 / FREE DOWNLOAD voicemeeter banana PRO CRACK

80 views • 28 minutes ago

[J...](#)

VOICEMETER BANANA FREE DOWNLOAD How To Download VoiceMeeter DOWNLOAD: <https://bit.ly/3ZjJQnN> PASSWORD: ...

New



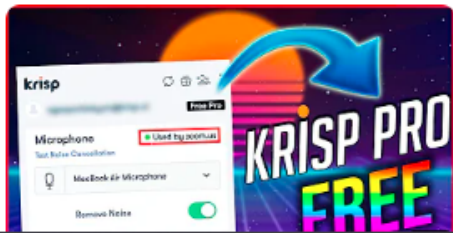
FIGMA CRACK DOWNLOAD 2022 + TUTORIAL

92 views • 29 minutes ago

[J...](#)

DOWNLOAD: <https://bit.ly/3SOB8v4> PASSWORD: 1896 Description tags are needed for global search and video promotion in ...

New



Krisp Crack | Install Tutorial | Unlimited | Free Download (2022)

93 views • 33 minutes ago

[...](#)

Welcome. This is new free crack for you Link: <https://bit.ly/3IP8s0n> Password: 1896 Everything you need is already is ...

New

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.

SEO Optimization Using Region-Specific Tags

Threat actors add an exhaustive list of tags that will deceive the Youtube algorithm to recommend the video and ensure it appears as one of the top results. While the tags include keywords relevant to the software, it also includes random keywords in different languages.

IGNORE TAGS:

blender, blender tutorial, blender guru, blender 3d, blender crack, blender cracked glass, blender crack tutorial, how to download and install blender, how to download blender 3d, how to install blender, install blender, how to download blender, download blender, blender 2.8, blender animation, procedural, how to create cracks in blender, download blender 3d, how to download blender for windows 10, download blender, blender download windows 10, blender 2.9, quad remesher, quad remesher for blender, download quad

Example of tags used in YouTube for SEO purposes

In the example below, the tags include keywords related to **Indian and Pakistani TV channels, TV programs, and phrases in local languages.**

latest, blender 3d, techniques, maya 2022 bonus tools, easy, instructions, 2016, maya 2017, maya 2018, vfx, autodesk maya 2020, learn to, system requirements, chamfer, normals, pakistani drama, maya 2020, stylized, top pakistani dramas, ary digital drama, gratis, espanol, substance designer, workflow, bake, perfect, fix, pbr, physically based, pipeline, animation, controls, startup, mesh, particles, vr for maya, how to download autodesk maya 2022 free, where to get maya 2022, vr for maya 2022, fundamental, water, patreon, maya 2022 free, maya modelling, bifrost, fluids, dynamics, how to install maya 2022, video, rig, rigging in maya, download, uv, gamedev, game rig, game development, #autodesk, get maya for free, maya3d, how do i, game rigging, sun marathi serial episodes, autodesk maya price in india, abhalachi maya serial, organic modeling in maya, polygon modeling, modeling an alligator, autodesk maya price, sant gajanan shegaviche, abhalachi maya marathi serial, modeling in maya, nandini serial, nandhini serial, autodesk maya system requirements, sun marathi nandini, autodesk maya student, marathi channel serial, nandini marathi serial, autodesk cad

Example of tags used in YouTube for SEO purposes

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

929 views Mar 7, 2023

How To Download "4K Video Downloader" For FREE | Crack

Link to download:<https://github.com/federicoTheGoAnima...>

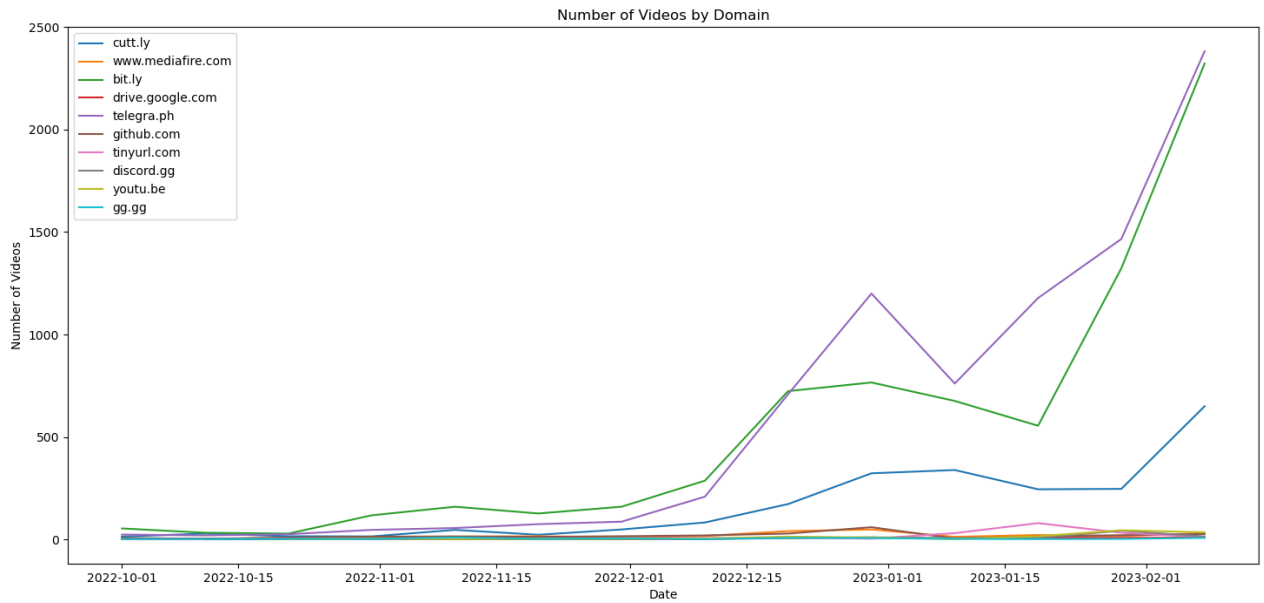
Password:2022

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.



Using Fake Comments to Give the Videos Legitimacy

Threat actors add several comments claiming that the cracked software worked for them. This lends the videos an air of legitimacy and misleads users into believing that the malicious download is legitimate. As seen in the examples below, several videos have identical comments within an hour of being posted, which indicates that the threat actors have automated the process of adding fake comments to videos.

Cubase 12 Pro Crack \ Free download 2022 \ Crack 2022



451 subscribers

Subscribe

284 views 1 hour ago

🔗 **DOWNLOAD:** <https://bit.ly/3yigJoH>

🔗 **PASSWORD:** 1896

Show more

7 Comments Sort by



Add a comment...



1 hour ago

Thank you so much Sense!! You are a blessing!

👍 Reply



1 hour ago

thank you straight to the point

👍 Reply



1 hour ago

thank you soo much very direct link n works for me love the way you expressed the installation .

👍 Reply



1 hour ago

BROTHER, YOU ARE THE BEST!!! You ooh really helped me!! THANK YOU VERY MUCH!This is cool, well done!

👍 Reply



1 hour ago

THANKS FOR THIS IV BEEN SEARCHING FO SOOO LONG

👍 Reply



1 hour ago

Nice tutorial.... Very helpful

👍 Reply

HOW TO DOWNLOAD VIDIQ BOOST CRACK 2022



25.4K subscribers

Subscribe

277 views 1 hour ago
DOWNLOAD - <https://bit.ly/3mwLCDx>
pass-1896
Show more

6 Comments Sort by



Add a comment...



1 hour ago

Thank you so much Sensei! You are a blessing!

Reply



1 hour ago

thank you straight to the point

Reply



1 hour ago

man I missed this kind of tutorials lol. Great work here, thanks!!!

Reply



1 hour ago

BROTHER, YOU ARE THE BEST!!! You ooh really helped me!! THANK YOU VERY MUCH!This is cool, well done!

Reply



1 hour ago

THANKS FOR THIS IV BEEN SEARCHING FO SOOO LONG

Reply

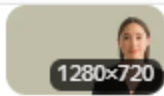


1 hour ago

thank you soo much very direct link n works for me love the way you expressed the installation .

Reply

AI-Generated Videos



SNS Recruitment (@snsrecruitment) / Twitter

twitter.com

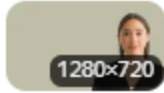
Please click the link below to view our current vacancies.View all jobs.



Welcome to FISBO - YouTube

youtube.com

Welcome to FISBO - YouTube



SNS Recruitment on Twitter: "Calling all chefs. Please click the link below to view our current vacancies.View all jobs: https://

twitter.com

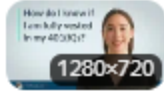
#jobs. #chef. snsrecruitment.co.uk/job-search. #chefjobs. #cheflife.



How do I know if I am fully vested in my 401(K)s? - YouTube

youtube.com

Learn more about this topic at https://meetbeagle.com/resources/post/how-do-i-know-if-i-am-fully-vested-in-my-401-k-sLeave us a comment if you have any quest...



Marguerite menace unité fully vested Rond Ville Paysage

skoolmatte.com



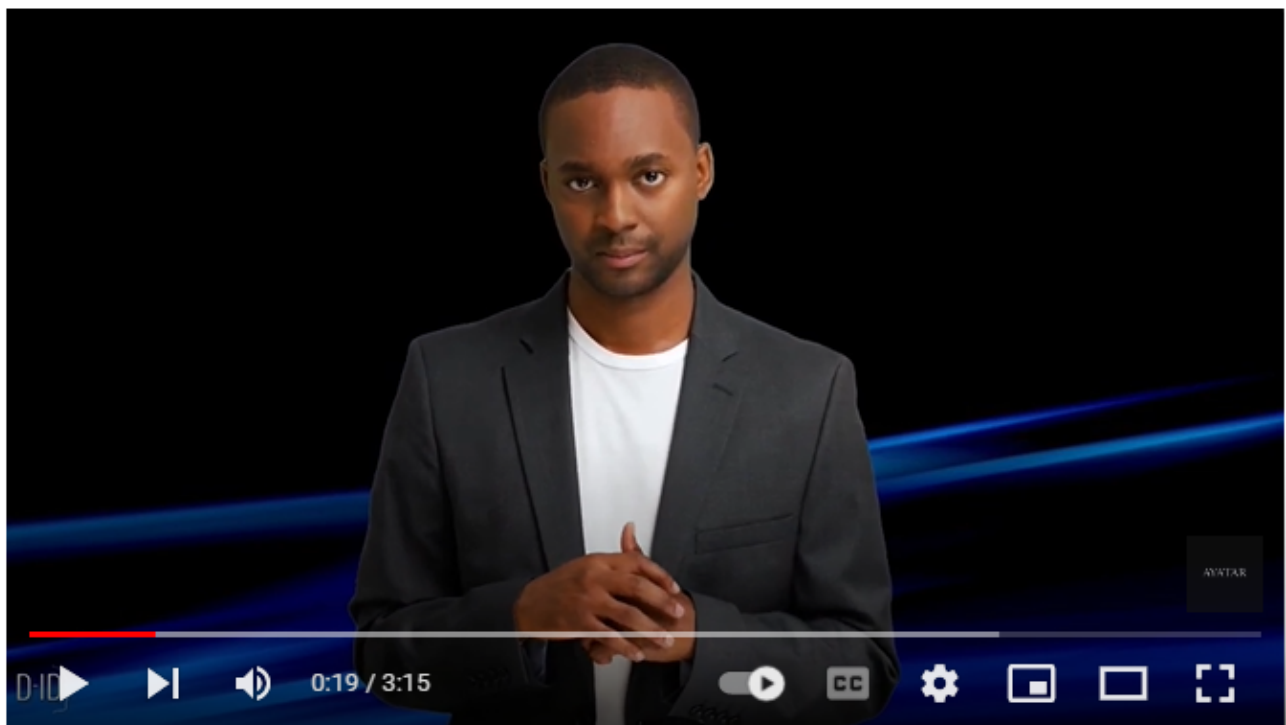
SNS Recruitment (@snsrecruitment) / Twitter

twitter.com

What everybody should know about Clinical Trials!Without clinical trials, we wouldn't have any vaccines, treatments for cancer, heart disease, diabetes and m. youtube.com.

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.



HOGWARTS LEGACY CRACK FREE DOWNLOAD | FULL GAME FOR FREE |
HOGWARTS LEGACY CRACK 2023 | FULL FREE



184K subscribers

Subscribe

9



Share



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.