Phishing campaign targets YouTube creators with cookie theft malware

blog.google/threat-analysis-group/phishing-campaign-targets-youtube-creators-cookie-theft-malware/

Ashley Shen October 20, 2021

Threat Analysis Group

Google's Threat Analysis Group tracks actors involved in disinformation campaigns, government backed hacking, and financially motivated abuse. Since late 2019, our team has disrupted financially motivated phishing campaigns targeting YouTubers with Cookie Theft malware.

The actors behind this campaign, which we attribute to a group of hackers recruited in a Russian-speaking forum, lure their target with fake collaboration opportunities (typically a demo for anti-virus software, VPN, music players, photo editing or online games), hijack their channel, then either sell it to the highest bidder or use it to broadcast cryptocurrency scams.

In collaboration with YouTube, Gmail, Trust & Safety, CyberCrime Investigation Group and Safe Browsing teams, our protections have decreased the volume of related phishing emails on Gmail by 99.6% since May 2021. We blocked 1.6M messages to targets, displayed ~62K Safe Browsing phishing page warnings, blocked 2.4K files, and successfully restored ~4K accounts. With increased detection efforts, we've observed attackers shifting away from Gmail to other email providers (mostly email.cz, seznam.cz, post.cz and aol.com). Moreover, to protect our users, we have referred the below activity to the FBI for further investigation.

In this blog, we share examples of the specific tactics, techniques and procedures (TTPs) used to lure victims, as well as some guidance on how users can further protect themselves.

Tactics, techniques and procedures

Cookie Theft, also known as "pass-the-cookie attack," is a session hijacking technique that enables access to user accounts with session cookies stored in the browser. While the technique has been around for decades, its resurgence as a top security risk could be due to a wider adoption of multi-factor authentication (MFA) making it difficult to conduct abuse, and shifting attacker focus to social engineering tactics.

Social engineering YouTubers with advertisement offer

Many YouTube creators provide an email address on their channel for business opportunities. In this case, the attackers sent forged business emails impersonating an existing company requesting a video advertisement collaboration.

Hello, my name is Jeff Tyler. I am one of the pixprotect managers. Recently, our company created an antivirus called pixprotect, but few people in the United States know about it, so that more people know about it, we need good advertising. You have a channel with a good overview, and we will be happy to order a 30-second or 15-second preview. We can agree on a price, but within the normal range.
How we want to see an advertisement for our service:
You need to demonstrate how you open the program and register in it. The insert must be special.
If this is not difficult, then you can tell us about the reliability of our antivirus.
I hope for cooperation, thanks

Example phishing email message

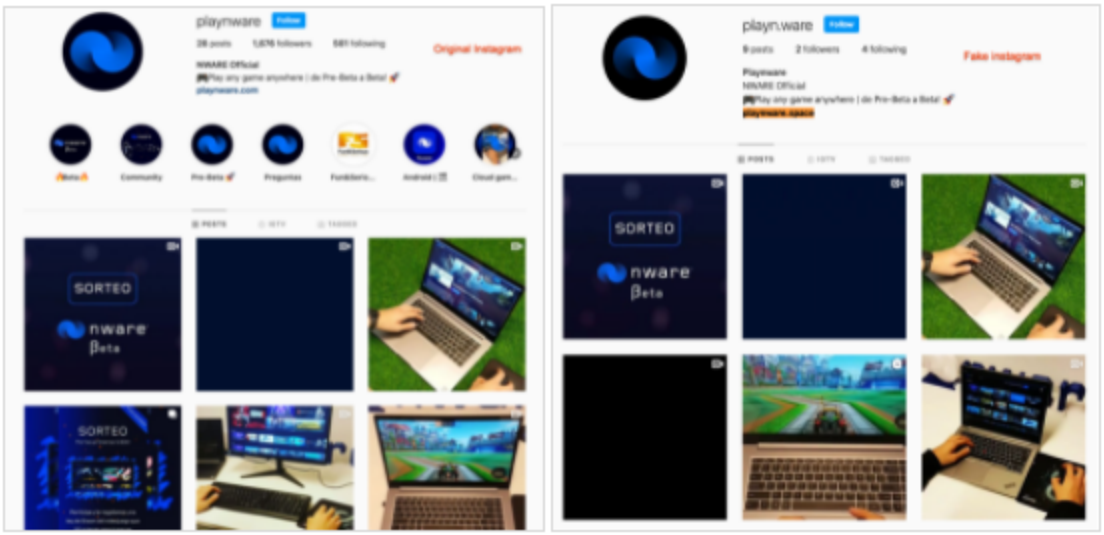
The phishing typically started with a customized email introducing the company and its products. Once the target agreed to the deal, a malware landing page disguised as a software download URL was sent via email or a PDF on Google Drive, and in a few cases, Google documents containing the phishing links. Around 15,000 actor accounts were identified, most of which were created for this campaign specifically.

Fake software landing pages and social media accounts

The attackers registered various domains associated with forged companies and built multiple websites for malware delivery. To date, we've identified at least 1,011 domains created solely for this purpose. Some of the websites impersonated legitimate software sites, such as Luminar, Cisco VPN, games on Steam, and some were generated using online templates. During the pandemic, we also uncovered attackers posing as news providers with a "Covid19 news software."

Lure message and landing pages for the forged covid news software.

In one case, we observed a fake social media page copying content from an existing software company. The following screenshot is an example of a fake page where the original URL is replaced with one leading to a cookie theft malware download.



Original (left) and fake (right) instagram accounts

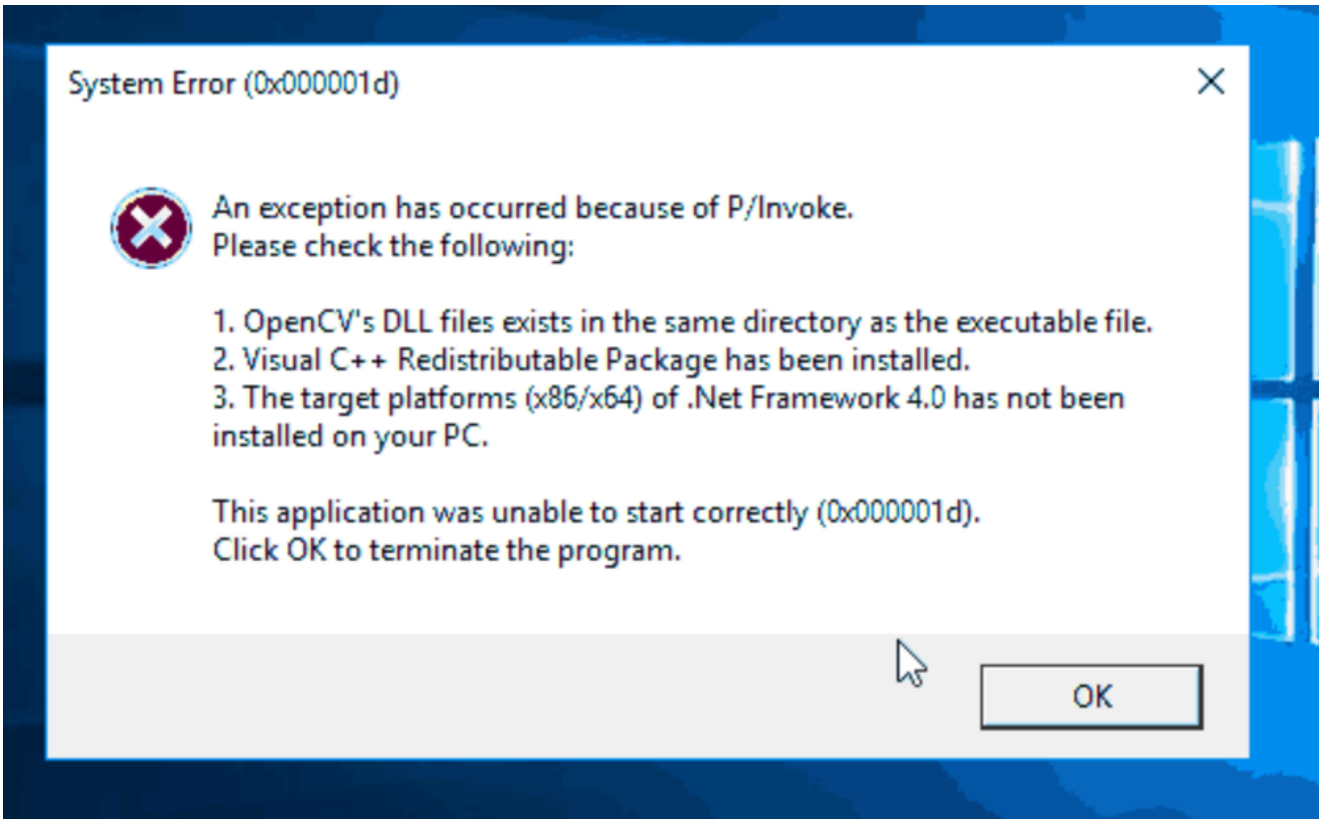
Because Google actively detects and disrupts phishing links sent via Gmail, the actors were observed driving targets to messaging apps like WhatsApp, Telegram or Discord.

Delivering cookie theft malware

Once the target runs the fake software, a cookie stealing malware executes, taking browser cookies from the victim's machine and uploading them to the actor's command & control servers. Although this type of malware can be configured to be persistent on the victim's machine, these actors are running all malware in non-persistent mode as a smash-and-grab technique. This is because if the malicious file is not detected when executed, there are less artifacts on an infected host and therefore security products fail to notify the user of a past compromise.

We have observed that actors use various types of malware based on personal preference, most of which are easily available on Github. Some commodity malware used included RedLine, Vidar, Predator The Thief, Nexus stealer, Azorult, Raccoon, Grand Stealer, Vikro Stealer, Masad (Google's naming), and Kantal (Google's naming) which shares code similarity with Vidar. Open source malware like Sorano and AdamantiumThief were also observed. *Related hashes are listed in the Technical Details section, at the end of this report.*

Most of the observed malware was capable of stealing both user passwords and cookies. Some of the samples employed several anti-sandboxing techniques including enlarged files, encrypted archive and download IP cloaking. A few were observed displaying a fake error message requiring user click-through to continue execution.



Fake error window require user click through

Cryptocurrency scams and channel selling

A large number of hijacked channels were rebranded for cryptocurrency scam live-streaming. The channel name, profile picture and content were all replaced with cryptocurrency branding to impersonate large tech or cryptocurrency exchange firms. The attacker live-streamed videos promising cryptocurrency giveaways in exchange for an initial contribution.

On account-trading markets, hijacked channels ranged from $3 USD to $4,000 USD depending on the number of subscribers.

Hack-for-Hire attackers

These campaigns were carried out by a number of hack-for-hire actors recruited on Russian-speaking forums via the following job description, offering two types of work:

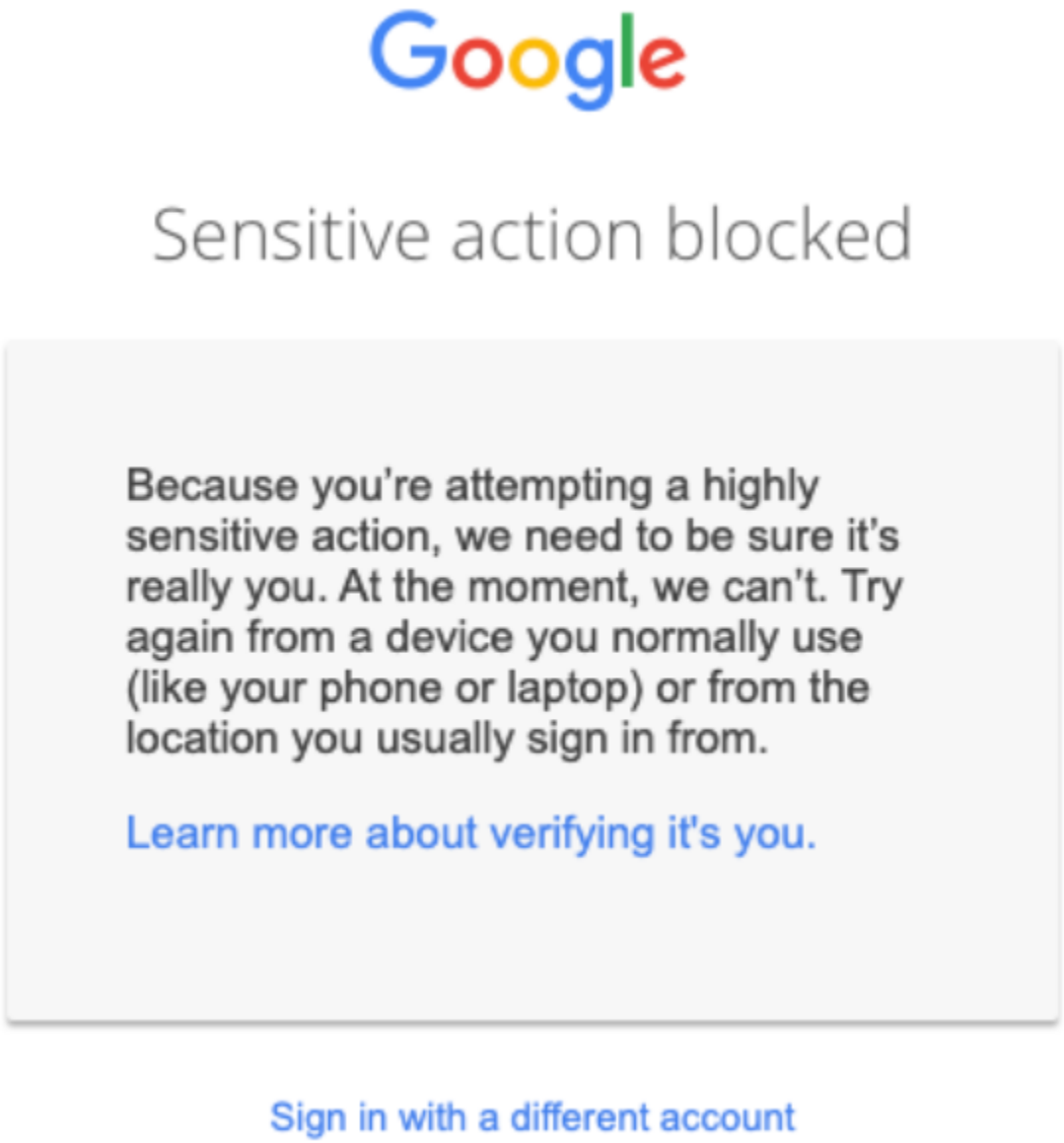
	Light Advertising	Full-stack advertising
Job Description	• Register a Gmail account • Send the account to attacker • Perform social engineering to trick the target into downloading the malware.	• Search and collect YouTube contact email • Register a Gmail account • Send the account to attacker • Prepare and send out initial set of personalised emails to targets • Perform social engineering to trick the target into downloading the malware. • “And everything else”
Revenue Sharing	25% of the revenue from hijacked channel	70% of the revenue from hijacked channel

This recruitment model explains the highly customized social engineering, as well as the varied malware types given each actor's choice of preferred malware.

Protecting our users from attacks

We are continuously improving our detection methods and investing in new tools and features that automatically identify and stop threats like this one. Some of these improvements include:

- Additional heuristic rules to detect and block phishing & social engineering emails, cookie theft hijacking and crypto-scam livestreams.
- Safe Browsing is further detecting and blocking malware landing pages and downloads.
- YouTube has hardened channel transfer workflows, detected and auto-recovered over 99% of hijacked channels.
- Account Security has hardened authentication workflows to block and notify the user on potential sensitive actions.



Sensitive action blocked in account

It is also important that users remain aware of these types of threats and take appropriate action to further protect themselves. Our recommendations:

- **Take Safe Browsing warnings seriously.** To avoid malware triggering antivirus detections, threat actors social engineer users into turning off or ignoring warnings.
- **Before running software, perform virus scanning** using an antivirus or online virus scanning tool like VirusTotal to verify file legitimacy.
- **Enable the "Enhanced Safe Browsing Protection" mode in your Chrome browser**, a feature that increases warnings on potentially suspicious web pages & files.
- **Be aware of encrypted archives** which are often bypassing antivirus detection scans, increasing the risk of running malicious files.

- **Protect your account with 2-Step-verification** (multi-factor authentication) which provides an extra layer of security to your account in case your password is stolen. Starting November 1, monetizing YouTube creators must turn on 2-Step Verification on the Google Account used for their YouTube channel to access YouTube Studio or YouTube Studio Content Manager.

Additional resources: Avoid & Report Phishing Emails.

Technical Details

Related Malware hashes:

- RedLine (commodity)
  - 501fe2509581d43288664f0d2825a6a47102cd614f676bf39f0f80ab2fd43f2c
  - c8b42437ffd8cfbbe568013eaaa707c212a2628232c01d809a3cf864fe24afa8
- Vidar (commodity)
  9afc029ac5aa525e6fdcedf1e93a64980751eeeae3cf073fcbd1d223ab5c96d6
- Kantal (share code similarity with Vidar)
  - F59534e6d9e0559d99d2b3a630672a514dbd105b0d6fc9447d573ebd0053caba (zip archive)
  - Edea528804e505d202351eda0c186d7c200c854c41049d7b06d1971591142358 (unpacked sample)
- Predator The Thief (commodity)
  0d8cfa02515d504ca34273d8cfbe9d1d0f223e5d2cece00533c48a990fd8ce72 (zip archive)
- Sorano (open source)
  c7c8466a66187f78d953c64cbbd2be916328085aa3c5e48fde6767bc9890516b
- Nexus stealer (commodity)
  - ed8b2af133b4144bef2b89dbec1526bf80cc06fe053ece1fa873f6bd1e99f0be
  - efc88a933a8baa6e7521c8d0cf78c52b0e3feb22985de3d35316a8b00c5073b3
- Azorult (commodity)
  8cafd480ac2a6018a4e716a4f9fd1254c4e93501a84ee1731ed7b98b67ab15dd
- Raccoon (commodity)
  85066962ba1e8a0a8d6989fffe38ff564a6cf6f8a07782b3fbc0dcb19d2497cb
- Grand Stealer (commodity)
  6359d5fa7437164b300abc69c8366f9481cb91b7558d68c9e3b0c2a535ddc243
- Vikro Stealer (commodity)
  04deb8d8aee87b24c7ba0db55610bb12f7d8ec1e75765650e5b2b4f933b18f6d
- Masad (commodity)
  6235573d8d178341dbfbead7c18a2f419808dc8c7c302ac61e4f9645d024ed85
- AdamantiumThief (open source)
  Db45bb99c44a96118bc5673a7ad65dc2a451ea70d406671500610 7f65d906715

Top Phishing Domains:

- pro-swapper[.]com
- downloadnature[.]space
- downloadnature[.]com
- fast-redirect[.]host
- bragi-studio[.]com
- plplme[.]site
- fenzor[.]com
- universe-photo[.]com
- rainway-gaming[.]com
- awaken1337[.]xyz
- pixelka[.]fun
- vortex-cloudgaming[.]com
- vontex[.]tech
- user52406.majorcore[.]space
- voneditor[.]tech
- spaceditor[.]space
- roudar[.]com
- peoplep[.]site
- anypon[.]online
- zeneditor[.]tech
- yourworld[.]site
- playerupbo[.]xyz
- dizzify[.]me

POSTED IN:

Threat Analysis Group