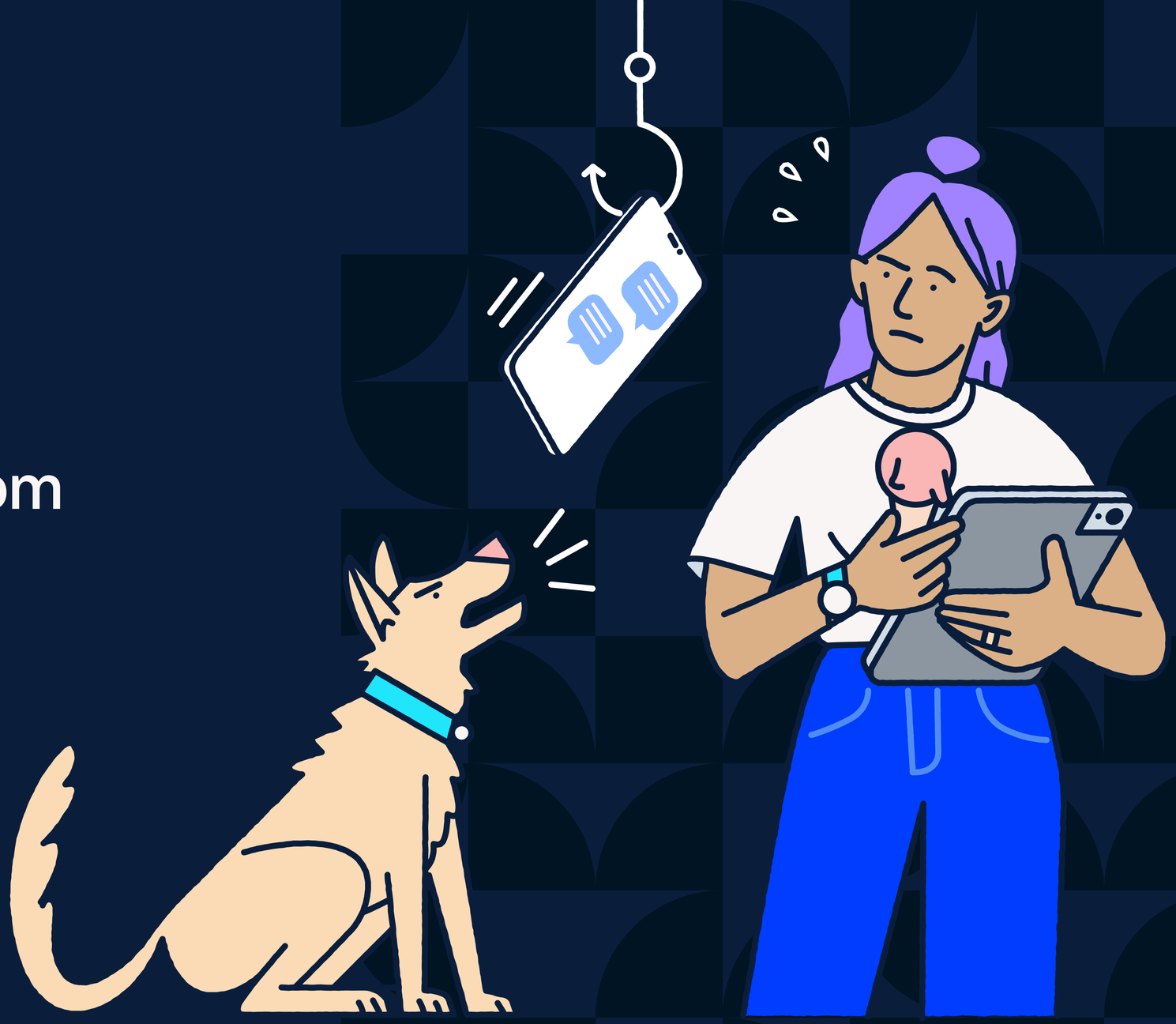
F-Alert

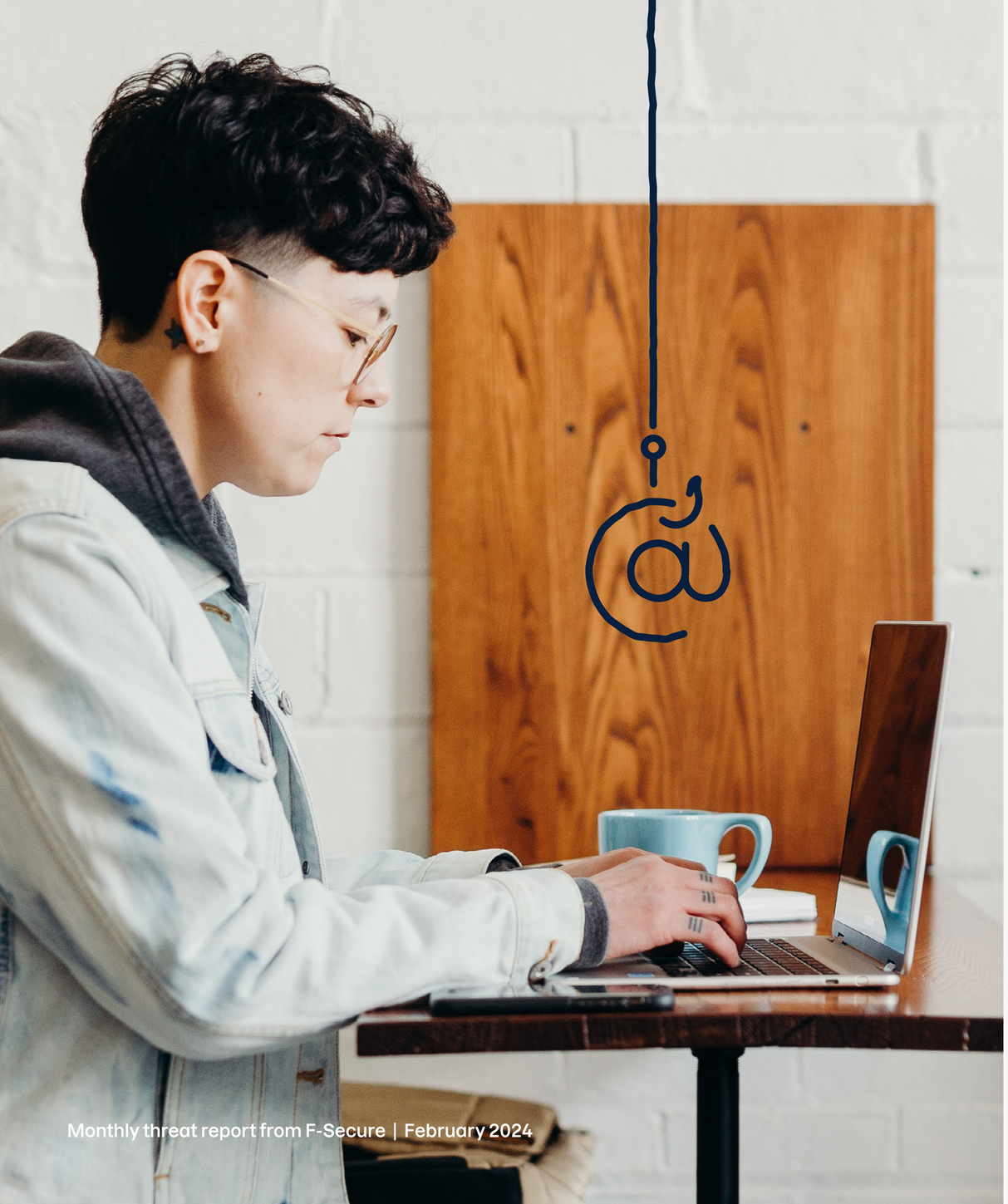
Monthly threat updates from

F-Secure

February 2024



F-Secure



Discover the latest threat updates. Packed with insights from the experts at F-Secure. Delivered every month.

Learn how sellers can outsmart scammers. Find out the hidden threat behind OpenAI's next leap. Know which social networks protect the privacy of your direct messages. And discover how criminals have expanded their pursuit of Google accounts. All this and much more in this month's F-Alert threat report.

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Never accept overpayment. And never share your private information, such as a Google Voice verification code, with any potential buyer. Both of these are common parts of advanced seller scams.

“It's entirely possible to be scammed as a seller.”

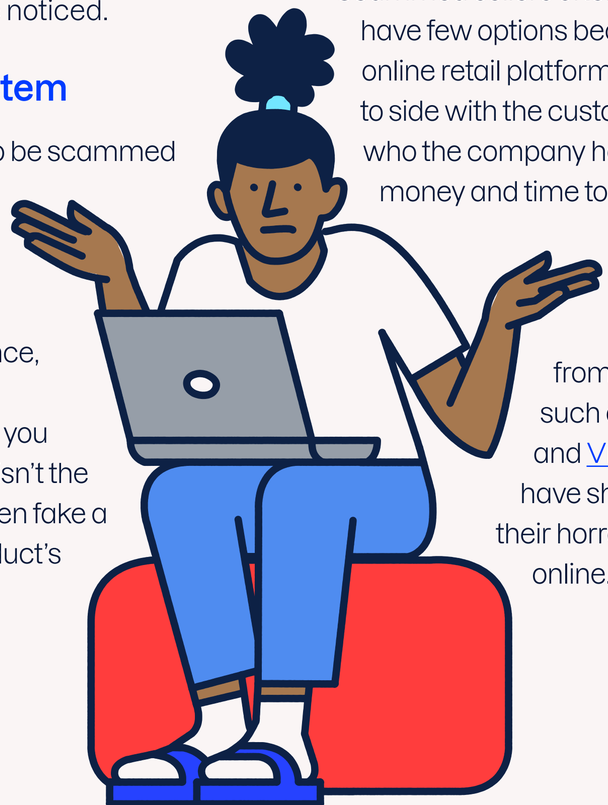
Sellers get scammed, too

Buyers aren't the only ones who need to beware online – sellers also face online shopping fraud.

Ecommerce doesn’t just offer the chance to buy almost anything from anywhere. Individuals can also quickly set up shop to sell their wares in minutes, often through some of the largest shopping platforms on earth. And scammers have noticed.

Abusing the system

“It's entirely possible to be scammed as a seller,” said Laura Kankaala, F-Secure Threat Intelligence Lead. “Buyers can, for instance, abuse the system by claiming that the item you sent is poor quality or isn’t the right size. They can even fake a problem with the product’s delivery.”



The goal of the scam is often to retain the product while avoiding payment.

“In worst-case scenarios, the scammed items are then resold by the scammers themselves,” she said.

“Scammed sellers often feel they have few options because online retail platforms are likely to side with the customers, who the company has spent money and time to acquire.”

"Some wronged sellers from platforms such as Ebay and Vinted have shared their horror stories online. But any victim of fraud should do more than vent," Laura explained.

Reporting shady buyers

“It's imperative to always report shady buyers to the online shopping platforms, no matter how small the loss,” she said. “It’s likely this scammer is not only scamming you but others as well.”

Take screenshots of all contact with the potential scammer and any other type of evidence you can gather. Some platforms may require to you report a fraud in a specific amount of time for the complaint to proceed.

“Finally, consider also filing a police report,” she concluded.

OpenAI deals with growing pains

New GPT Store and phishing attacks reveal the promise and peril of custom AI bots.

OpenAI has seen astonishing success in just a little over a year since it launched ChatGPT, offering the world a masterclass in the opportunities and challenges that come with being the leader in the hottest industry on earth.

With the launch of the delayed GPT Store, the security world is closely watching how OpenAI will handle both moderation and threats like phishing.

Like any digital marketplace

The GPT Store allows users to create and sell custom versions of ChatGPT, called GPTs, that offer useful services from finding hiking trails to creating websites.

"But, just like any digital marketplace, such as Google Play, the GPT Store is not immune to the lurking shadows of security threats and malicious actors," explained Khalid Alnajjar, a Senior Threat Data Researcher at F-Secure.

Just days after the launch of the store, several GPTs seemed to be offering "AI girlfriends," which are in direct violation of OpenAI's policies.

But GPT fans have more to worry about than just amorous robots.

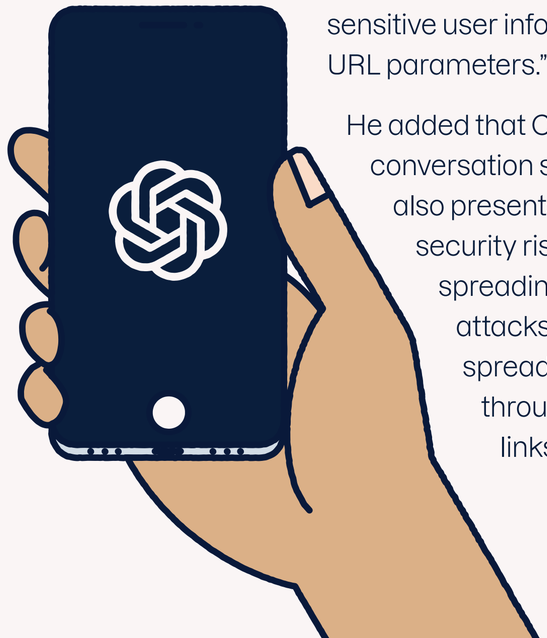
A hidden threat

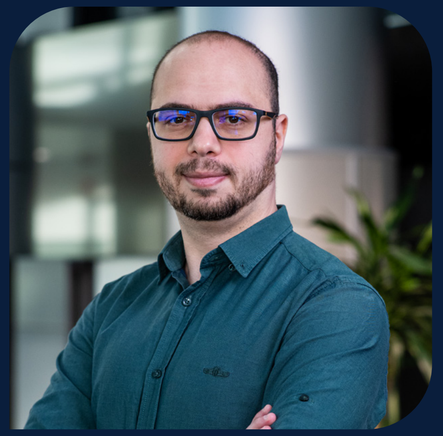
"Beneath the waves of OpenAI's bustling GPT Store lies a hidden threat," Khalid said.

He noted that phishing attacks cleverly disguised to extract user credentials can target ChatGPT users. And the researchers who discovered this security weakness noted that attacks can work from the GPT Store.

"The prompt injection attack works by making the ChatGPT interface render an external image," he said. "While this use case is a legitimate one, attackers can abuse the feature by loading an invisible tiny pixel or passing sensitive user information as URL parameters."

He added that ChatGPT's conversation sharing feature also presents numerous security risks – from spreading phishing attacks to directly spreading malware through malicious links or downloads.





Khalid Alnajjar
Senior Threat Data Researcher
Helsinki, Finland

expert tip

Be mindful of the information you share with any AI interface. Before you hit enter, pause, and think: "Do I really need to share this? Is this safe?"

"Beneath the waves of OpenAI's bustling GPT Store lies a hidden threat."

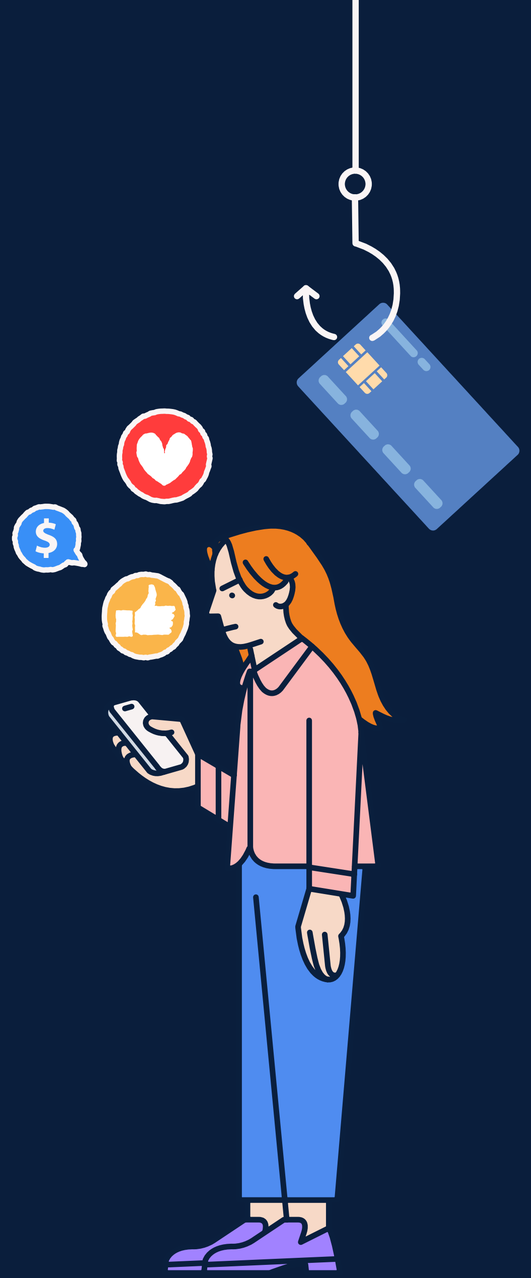
Trending Scam

Adding insult to romance scams

WHAT:
Romance scams are literally a billion-dollar business, but the criminals behind them still want more. A Massachusetts woman, who lost over $150,000 to a romance scammer, was also harassed by scammers pretending to be law enforcement agencies handling her case.

HOW:
An email with the subject "THE CIA IN COLLABORATION WITH THE FBI" threatened the woman. The message warned that if she spoke to law enforcement or her lawyer about a months-long scam with a man alleging to be a pipeline worker needing emergency funds, she would never get her money back. Even worse, she could face criminal charges.

PREPARE:
If you're reading this, you probably know to be suspicious of any plea for money from a stranger. You also know that you should reach out to a trusted friend or relative the moment you feel you may be scammed. Be sure to share these precautionswith any of your loved ones who might be looking for love online.



Breach that matters

Naz.api dump of credentials from Yahoo, eBay, Facebook and more

WHY IT MATTERS:
Since October of last year, we have been alerting our customers who were affected by this massive data leak that has only recently made the headlines. The leak, known as the Naz.api dataset, consists of hundreds of millions of records from various online platforms, such as Roblox, Coinbase, and Yammer. Among these records are 71 million unique credentials, of which 25 million are not found anywhere else online. The source of the leak is likely an infostealer malware, as all the passwords are in plaintext. No major site stores passwords without some form of encryption.

BREACHED DATA:
The data includes usernames, passwords, email addresses and a variety of other personally identifiable information for hundreds of millions of internet users.

WHAT SHOULD YOU DO:
A leak this large could impact nearly any average internet user or one of their loved ones. If you haven't done a check on whether your data has been leaked online before, now is the perfect time. Also be sure that all your accounts have an extra layer of security: activate two-factor authentication or passkeys wherever they are available.

Has your data been exposed as part of Naz.api? Check with our F-Secure Identity Theft Checker!

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

No matter how well encrypted your messages are, they're only as secure as your account. This is another reason to use strong, unique passwords and two-factor authentication, whenever possible, to prevent account takeovers.

"End-to-end encryption turns a direct message into a private message."

Are your DMs really private?

Meta has finally rolled out end-to-end encryption for Instagram and Messenger. How do other social networks compare?

After seven years, Meta has finally fulfilled CEO Mark Zuckerberg's promise to fully encrypt all direct messages on Instagram and Facebook.

End-to-end encryption often puts tech companies in conflict with governments and law enforcement agencies that want access to any information deemed necessary for their aims.

But the issue is pretty simple for consumers.

Encrypted messages offer the confidence that the contents of your communications are only accessible to you and the receiver. No one else—not the platform, telecommunication providers, or anyone trying to snoop—should be able to see them.

"Just because a service calls them 'private messages' is no guarantee that the content is encrypted," explained Joel Latto, Threat Advisor at F-Secure. "End-to-end encryption is what turns a direct message into a private message."

You need to know if you can expect privacy from the direct communications on your favorite social media platform. That's why we've prepared this chart.

Message encryption by social network

Platform	Encryption	Direct or private
Meta (Facebook, Instagram, Messenger, WhatsApp)	End-to-end encryption by default	Private
TikTok	"End-to-end encryption is not currently available."	Direct
LinkedIn	"We encrypt data in transit. Certain sensitive data is also encrypted at rest, including credit card information and passwords."	Unclear, but assume direct.
X	Encrypted Direct Messages are available for verified users and verified organizations' affiliated users.	Can be private but not by default.
Mastodon	Posts on Mastodon are not end-to-end encrypted.	Direct
Youtube, Threads, Bluesky	No messaging available	n/a

Malware targets Google accounts

Criminals take advantage of newer methods to access everything from Gmail accounts to YouTube channels.

You may have never considered the value of your Google account, but you can be sure attackers have.

Almost 2 billion people use Gmail, which is used by countless people as a skeleton key for access to all their key accounts as a backup email. Of the 2.5 billion active YouTube users, 114 million run their own channels.

The tech giant has made impressive progress in improving account security lately by joining the FIDO alliance to roll out passkeys, and introducing a new way for account verification. But criminals seem to be adjusting with malware specifically designed to take over a Google account and gain access to all the Google services linked to that account, including Calendar, Photos, and Meet.

Passwordless hack

"Information stealing malware has been able to take advantage of a known exploit that uses a specific Google API to 'revive' stolen session cookies and gain unauthorized access to Google accounts" said Ash Shatrieh, Threat Intelligence Researcher at F-Secure. "What's new here is criminals can retain access even if the password is changed. The API allows cookies to be regenerated once more even after a password reset."

A post on Telegram in October of 2023 explained how Google Authentication cookies could be used to bypass two-factor authentication, which generally offers excellent account security.

"Lumma infostealer quickly began to take advantage of the security hole, which Google has said that it doesn't plan to fix," Ash added. "Very quickly, several other infostealers also added the same exploit."

Tricks upon tricks

The massive growth of infostealers has been fueled by the constant innovations used to manipulate potential victims.

"One of the advantages of spreading malware through cracked software is that users often don't think twice when ignoring their security software's warnings about installing the downloads," explained Joel Latto, Threat Advisor at F-Secure.

The Lumma stealer uses a variation on another common trick to spread even further.

"Using compromised YouTube accounts, the criminals post videos for cracked software to seed infected files, much in the same way cracked software is often advertised in Discord Forums," he concluded.

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

If you think you've been infected by an infostealer, you need to do more than just scan your computer this time. You need to log out of all Google sessions, change your Google password, and log in again to regenerate cookies. Reviewing and revoking any odd connections is also a good idea.

"Very quickly, several other infostealers also added the same exploit."

About F-Secure

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 200 partners.

For more than 30 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit f-secure.com today!

F-Secure