F-Alert

Monthly threat updates from

F-Secure

January 2023

F-Secure

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

Find out how you might be affected by the recent massive Twitter data leak. See how scammers exploit Instagram’s mysterious account recovery system. Find out how criminals have hijacked Google’s search results. And learn how the month's biggest leaks might affect you and your data.

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

To hide your identity, Twitter recommends not adding a publicly known phone number or email. But go three steps further. Don't add your phone number at all. Instead, use an authenticator app or hardware key for two-factor authentication. And uncheck both "Discoverability" boxes in Twitter's settings.

> **"This leak is good reminder to always use two-factor authentication whenever it's available."**

Majority of Twitter users exposed

A leak of 200 million email addresses puts some users' privacy at risk and could lead to targeted attacks.

More than 200 million Twitter users appear to have had their personal data posted on a hacker forum, where it is being sold for just $2.

A pretty worthless dataset

"The low price makes sense because it's a pretty worth less as a dataset," said Joel Latto, F-Secure Threat Advisor. "However, that doesn't mean there aren't any worries for the affected users."

Reports suggest that a now-patched vulnerability in Twitter's API (application programming interface) during 2021 made it possible to collect email addresses, phone numbers, and usernames from just over half of the site's users (around 400m). However, Twitter has denied that this vulnerability was exploited.

The biggest risk

"The biggest risk here is for 'pseudonymous' users or who hide their identity," Latto explained. By connecting these accounts to publicly known emails, the identities of these cloaked accounts could be exposed with severe implications for activists and other previously anonymous users.

This breach ranks among the largest of all-time, and appears to be the biggest leak in Twitter's history (although there was a bug that left 330 million users' passwords potentially exposed in 2018, but without any evidence of misuse). And with just a username and email address, threat actors could try to take over an account by attempting to reset the password.

"Unfortunately, almost every service or site gets breached eventually," Latto said. "While the information exposed here is minimal for most users, the need to be careful about securing your key accounts and monitoring your information just keeps growing. This leak is good reminder to always use two-factor authentication whenever it's available."

Instagram influencers exploited

Some Instagram users locked out of their accounts have been forced to turn to the black market for help, but new tools may provide some support.

When an Instagram accounts has been hacked, or shut down by Meta (Instagram's parent company) it can be an uphill struggle for the legitimate owner to reclaim their account, and this has led some influencers into compromising situations.

It can be overwhelming

"Users who have been locked out of their accounts often spend months trying to get help from the site," said Laura Kankaala, F-Secure's Threat Intelligence Lead.

Users report issues with buggy user interfaces, along with dead-end conversations with Meta.

"The account recovery process includes submitting pictures or videos of yourself – which creates opportunities for people looking to exploit the recovery mechanism by using photoshopped, or even deepfaked content, to take over others' accounts," Kankaala said.

The odd thing

Unfortunately, the difficulty of recovering accounts has created a black market.

"Shady characters offer help for substantial payments, and there have been reports of desperate influencers taking desperate measures. The odd thing is these efforts occasionally seem to work," Kankaala explained.

Kankaala believes these successes come from tricks learned via trial and error, whilst helping multiple people who have lost their accounts with their recovery process. She notes some claim to use hacking techniques, but there's no evidence that this is true.

"If you come across someone claiming to have hacked Instagram, most likely they are bamboozling victims into paying for nothing," Kankaala said.

Finally, some help

However, at the end of 2022, Instagram finally took significant steps to address the issue.

"The mystery of the process has been a godsend for scammers," Kankaala said. "Hopefully, this is the beginning of the end of this weird little economy."

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Secure your account. It's not only about strong passwords. It's also about enabling two-factor authentication, activating login requests so you know when a new device tries to access your account, and being mindful which 3rd-party applications, such as Tinder, have access to your Instagram.

> **"It can be overwhelming for someone looking to restore their account and their livelihood."**

Breach reports

A selection of the month's biggest breaches, where confidential or protected information have been exposed.

Deezer

Discovered: 6/1/2023

Affected people:
Almost 335 million

Breach severity: ⚡⚡⚡

Data from the online music streaming service Deezer from 2019 was leaked to hacking forum in early 2023. This breach containing names, email addresses, IPs, and usernames offers a reminder that monitoring your identity and applying strong account security are necessary even if you do not believe your data has ever been exposed. Victims of this breach should expect targeted phishing attacks and refrain from clicking on links or attachments in emails.

Gemini

Discovered: 22/12/2022

Affected people:
More than 5 million

Breach severity: ⚡⚡⚡

Email addresses of users of Gemini, a cryptocurrency exchange, were leaked on a hacking forum in late 2022. While this leak only involves emails, users should take the steps anyone should take whenever data from a financial institution they use has been compromised. File a fraud alert with either Equifax, Experian, or Trans Union. Then check your credit to make sure your personal information has not been used to open any card you did not apply for yourself.

Empowrd Apps

Discovered: 12/1/2023

Affected people:
Almost 165,000

Breach severity: ⚡⚡

Names, email addresses, usernames, passwords, and phone numbers of the civic engagement tool EmpowrdApps have been leaked and are being privately shared on the internet. The primary worry for victims of this leak is password security. Consider the password you used for this app is compromised as it's being shared across the dark web. Change it and any variations of this password that you've ever used and never use them again.

Andersen Corporation

Discovered: 10/1/2023

Affected people:
Over 1.2 million

Breach severity: ⚡⚡

Names, addresses, email addresses, phone numbers and additional personal information were leaked on a hacking forum in January 2023. This dataset belongs to the U.S.-based home improvement company Andersen Corporation. This kind of combination information could be used for very convincing phishing campaigns, by both email and traditional mail.

Want to know if you were affected by a breach? Check out our **F-Secure Identity Theft Checker!**

Google Ads hijacked

Criminals are abusing Google's targeted ad platform to pump out malware.

Users searching for software packages on Google have been served ads that lead to a "malware cocktail."

Weaponizing ads

"Google has generally eliminated search engine poisoning, where criminals abused the site's algorithm to push malicious sites to the top of search results," said Yik Han, a researcher at F-Secure. "However, cyber criminals always adapt."

A new threat combines search engine poisoning with typosquatting—a trick that uses misspellings of popular sites to steal web traffic—to exploit Google's ad platform.

"Threats actors have found a way to weaponize Google's results by creating malicious ads that redirect users to fake websites that mimic trusted brands that deliver malware straight to your computer," Yik Han explained.

Hundreds of companies that offer software downloads have been impersonated, including TikTok, SnapChat, and MetaMask.

"For example, when you search for Brave Browser Download, the real search result should redirect you to brave.com, but a malicious ad will bring you to bravesoftware[.]com, a fake website that hosts malware," Said Yik Han.

Making users less suspicious

Yik Han noted that these malicious sites serve up "malware cocktails," often an information stealer bundled with a software installer, so the victim won't know stealer is running in the background. "Another technique used by these threats to prevent detection is 'pumping,'" he said. "This is done by inserting junk data into the malware until it reaches a large file size, in hopes of making antivirus engines stop scanning the file."

F-Secure created the detection "Trojan: W32/GenInflated.B" for these pumped up infostealers.

"It's quite new, but detections are rising steadily," Yik Han concluded.

Yik Han
Researcher
Puchong, Malaysia

expert tip

When it comes to using search engines, threats will strike where least expect them, so we need to be careful whenever we click on a link, and always check the URL of the site we've been sent to. Additionally, use internet security, like F-Secure TOTAL, that not only secures your computer, but also protects your online activity by blocking malicious websites.

> **"It's quite new, but detections are rising steadily."**

Leaked code spikes infections

Several variants of Spynote have spread widely after the author of the threat leaked the source code for this Android malware.

Since the code behind SpyNote was released in October of 2022, the spyware has infected more devices and evolved to threaten bank accounts.

Doom for its victims

“Apparently, the author of SpyNote became frustrated by scammers impersonating him in hacker forums and published the code on GitHub,” Amit Tambe, a researcher at F-Secure said. “Leaking source code of malware always spells doom for its victims, invariably leading to an infection surge.”

Bad actors continue to add more malicious features and tactics to the original app, which was designed to secretly monitor and manage devices.

“Attackers have impersonated apps—such as Google, Alipay, and even erotic video apps—and spread them through third-party Android app sites, tricking users into downloading and installing those apps,” Tambe explained.

More countries, more infections

The latest variant targets banking apps, aiming to loot users’ accounts.

“The apps use a variety of techniques to gain free rein on the victim’s device,” Tambe said. “Once access to the device is obtained, the spyware then does its job of exfiltrating sensitive information such as audio or video call data and account credentials.”

Infections have spread across multiple borders since the source code leak. And based on the number of infections, the countries most impacted by the leak were Germany and Poland, followed by other countries such as Iran, the UK, and India.

“At F-Secure, we observed that the attacks which were initially present in nine countries in the third quarter of 2022. That has now grown to 13 countries,” Tambe explained. “We also saw a rise in the number of infections by about 28.5% from the beginning of the last quarter of 2022.”

Amit Tambe
Researcher
Helsinki, Finland

expert tip

Downloading of apps from outside of official sources should be avoided. Care must be taken to find out the names of real apps—especially for banks or credit card companies—before downloading similar-sounding alternatives.

“The apps use a variety of techniques to gain free rein on the victim’s device.”

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 170 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 today!