F-Alert

Monthly threat updates from

F-Secure

December 2022

F-Secure

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

In this year-end edition of F-Alert, we review the latest cyber security threats and data breaches from December. Discover how cyber criminals see new Artificial Intelligence tools. Find out why our data is worth billions on dark web marketplaces. And learn how the month's biggest breaches might affect you and your data.

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

As always, be on the lookout for scams. No matter what's the context or how well the scam messages have been written, criminals want you to act. Don't give out your credentials, install malware or transfer money or cryptocurrency to suspicious destinations.

New bot previews AI risks

A remarkable new chatbot from OpenAI could foreshadow how cyber criminals can weaponize artificial intelligence in the future.

More than a million people have already sampled the power of a computer delivering intelligent, crafted human-like text at incredible speeds thanks to [a new chatbot] released in early December by the research laboratory OpenAI.

With the increasing prevalence of AI, concerns about robots taking our jobs—or just taking over—continue to gain momentum. But the reality is more prosaic, as AI is already being used in multiple ways, affecting many of our digital moments.

"Moderation of our social media feeds and our recommendations for music and shopping are already leveraging AI," said Laura Kankaala, F-Secure's Threat Intelligence Lead." Even industrial optimizations are already leveraging the technology."

AI and cyber crime

ChatGPT has already been used for a variety of impressive tasks, including personalized education, drafting newspaper articles, and writing computer code. And the question of whether it could be employed by cyber criminals is attracting more interest.

"When it comes to cyber crime, the benefits of AI have not yet been realized," Kankaala said. "But that could change with the availability of models like ChatGPT, which is quite good at generating text and participating in conversations."

AI is everywhere

Fully automated attacks generated by ChatGPT are not yet feasible. But, as with other emerging technologies, Kankaala only sees it as a matter of time before cyber criminals get on the AI bandwagon.

"We know that an easy-to-use tool that automates scams and phishing emails are bound to appear," Kankaala said. "Because it's too good of an opportunity to pass up." But for now, the overall 'killchain,' or how the attack plays out, will not change. "The scams may look fancier, but — fortunately—defending against these threats is nothing new," Kankaala concludes.

> **"When it comes to cyber crime, the benefits of AI have not yet been realized."**

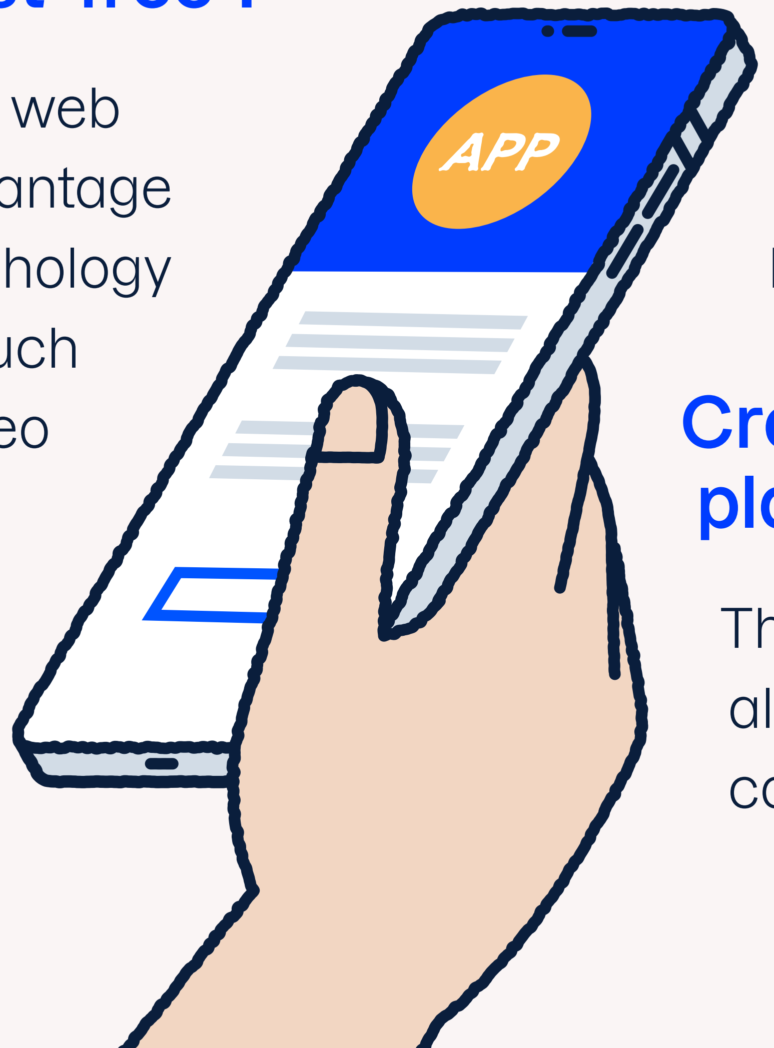
Good apps glued to bad

Dark web service hides infostealers in real apps to infect Android or Windows users.

A new cyber crime campaign, identified as Zombinder, attaches malware to legitimate Android apps to entice victims into installing the malicious payload on their devices or PCs. According to reports, security analysts found the platform on the darknet during investigations into a campaign promoting different types of malware that focused on Android and Windows users.

Who can resist ‘free’?

Zombinder, a dark web service, takes advantage of this simple psychology by offering lures such as “free” Wi-Fi, video downloads, or sports streaming services.



“The temptation of ‘free stuff’ is irresistible for many internet users. Especially those in search of a Wi-Fi connection,” said Amit Tambe, a researcher at F-Secure. “And the threat actors take the con one step further, they actually deliver the promised functionality,” Tambe added. “However, the real app comes with a malicious app ‘glued’ to it by Zombinder.”

During installation, the user is presented with a prompt for a plugin, which installs an infostealer in the background.

Crossing apps and platforms

This campaign’s marketing also seeks to make the corrupted apps appeal to the largest possible audience. And this has helped the campaign infect thousands of users with a variety of stealers since the binding technique first appeared in March 2022.

“Some of the malicious sites from the campaign offer the option to download the apps on either Android or Windows platforms,” Tambe said. “This sort of malware targets victims’ personal information and accounts. It could go after cryptocurrency wallets, emails from the Gmail app, or even two-factor authentication codes.”

Amit Tambe
Researcher
Helsinki, Finland

expert tip

The Internet is filled with cracked software, modded APKs, and application hacks. Often, these sorts of riskware are fake and may contain malicious trojans or malware that will infect your computer. Always download from trusted websites and avoid shady websites.

> **“The threat actors take the con one step further, they actually deliver the promised functionality.”**

Breach reports

Bookcrossing

Discovered: 10/11/2022

Affected people:
Nearly 1.9 million

Breach severity: ⚡ ⚡

Data from Bookcrossing, an online book club, was leaked to a hacker forum. The data being privately shared on the internet contains IPs, passwords, usernames, email addresses and additional personally identifiable information. Breaches like this fuel criminals' attempts to carry out automated account takeovers. Affected users should change any account that uses the password, or any variation of the password used for this site.

Football Guys

Discovered: 1/12/2022

Affected people:
More than 500,000

Breach severity: ⚡

Data from this U.S. fantasy football site was leaked on a hacker site. While this dataset only includes usernames and passwords, it is still useful to criminals due to password reuse. If Internet users used strong, unique credentials for all their accounts, this would eliminate countless acts of cyber crime.

Cointracker

Discovered: 15/12/2022

Affected people:
More than 1.5 million

Breach severity: ⚡ ⚡ ⚡

In November 2022, data belonging to this cryptocurrency tax and portfolio management software service was leaked on a hacking forum. Affected users, and all consumers who have had their financial data leaked, should contact their financial institutions to check for fraudulent transactions and monitor their credit report continuously.

Washington State Food Worker Course

Discovered: 15/12/2022

Affected people:
Nearly 1.9 million

Breach severity: ⚡ ⚡ ⚡

User data leaked from this virtual education platform includes names, email addresses, passwords, phone numbers, and driver's license numbers. While this breached data will typically result in account takeover attempts or spearphishing attacks, affected users should also be mindful of the risks that come from exposed driver's license numbers, which can be used to apply for other services and are extremely difficult, if not impossible, to replace.

Want to know if you were affected by any of these breaches?
Check out our **F-Secure Identity Theft Checker!**

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

Time between initial data breach and criminals abusing stolen data seems to be shortening. That's why you need a service like F-Secure ID PROTECTION to scour through dark web marketplaces and alert you as soon as your data shows up there. Then you can take steps to secure your data immediately.

Dark web marketplaces thrive

New research explains how criminals make big bucks selling stolen data with little fear of the law.

New research has found that dark web marketplaces raked in more than $140 million in just eight months, selling stolen data across a "highly connected" ecosystem.

Where stolen data goes

The study outlines the "supply chain" that keeps dark web marketplaces stocked with an abundance of personally identifiable information.

"We all hear about breaches leading to data being stolen from corporate servers," said Joel Latto, F-Secure Threat Advisor. "But we rarely hear about what happens to your data next."

Breached files are given to brokers to sell in dark web marketplaces. Other criminals buy the data for fraudulent credit card transactions, identity theft, and phishing attacks.

"The revenue of the top marketplaces is comparable to those from midsize American companies, many of which have valuations of billions of dollars," said Latto. "Remember that next time you think your data has no value."

> "The revenue of the top marketplaces is comparable to those from midsize American companies."

Beyond the law's grasp

In the eight months studied, over 2,000 vendors registered more than 600,000 sales across 30 marketplaces, with many of the vendors appearing on multiple marketplaces.

"Buyers and sellers all use cloaking software like Tor to reach the marketplaces," he said. "In addition, these sites use authorization codes to try to vet buyers and only take cryptocurrency."

Since identifying these criminals and shutting down these marketplaces is so difficult, the researchers suggest making stolen data worthless by making it extremely difficult to commit fraud.

"Their idea is to use artificial intelligence to provide law enforcement with the tools to prevent identity crimes—but at this point, that's just science fiction."

Scammers exploit TikTok trend

Cyber criminals used the titillation of a TikTok challenge to spread malware that steals credentials, crypto, and credit cards.

TikTok users were tricked into installing malware by the false promise of a tool that would reveal nude bodies blurred for the app's popular "invisible challenge."

Down the rabbit hole

TikTok users participate in this challenge, which began in April 2020, by filming themselves undressed and applying a filter that blends their silhouettes into a neutral background for an "invisible" effect. And the initial 'lure' was a TikTok post promising filter removal.

"Cyber criminals weaponized users' curiosity to create a multi-layer social engineering scam that led victims to infecting their own devices," explained Yik Han, a researcher at F-Secure. "The victim was told to join a Discord server, where they received a message from a bot pointing them to GitHub for the download along with instructions in a YouTube video."

But once installed, the tool does not remove any filter.

"However, the executed malware will steal personal files—Including Discord credentials, crypto wallet passwords, and credit card details."

Seems legit

Before all the content was removed from their respective platforms, the TikTok videos racked up more than 1 million views, more than 35,000 people have joined the Discord server, the GitHub repository has 103 stars, and the YouTube video was viewed 2,000 times. And this scam shows how social media can be weaponized to fool users into making bad decisions.

"The criminals used multiple tricks to make their GitHub repository seem legitimate," Han said. "These big numbers made it hard for a user to realize that each element was part of a trap to spread malware."

Yik Han
Researcher
Puchong, Malaysia

expert tip

Don't be fooled by big numbers on social media. Cyber criminals are figuring out how to game platforms to build up the views, likes, and shares that make their content seem credible. Always research an app when you download with a search and look through the reviews.

> **"Cyber criminals weaponized users' curiosity ... that led victims to infecting their own devices."**

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!

F-Secure