F-Alert

Monthly threat updates from

F-Secure

November 2022

F-Secure

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

In this inaugural issue of F-Alert, we review the latest cyber security threats and data breaches from November. Discover Facebook scammers' new trick. See how criminals spread a malicious Android app. And learn how the month's biggest breaches might affect you and your data.

Scammers target Facebook

Malicious Facebook pages use notifications to drive victims to phishing sites

A new wave of scams utilizes Facebook's tagging feature to trick Page owners into believing they've violated Facebook's terms and conditions. Several variations of the attack exist, but all lead to phishing sites designed to steal Page owner's credentials.

The scammers make it personal

"After the Post is published on the malicious Page, victims receive notification that action must be taken quickly to prevent their pages being 'permanently disabled,'" explained Joel Latto, F-Secure Threat Advisor.

This tactic creates both confusion and a sense of urgency. "The source of the notification is unclear," Latto said. "And since victims may believe this is an official notification that requires quick action, they are less likely to spot the red flags that suggest the message is fraudulent."

Stolen accounts can be used for several malicious purposes—such as promoting scams, running questionable ads, impersonating businesses, or reselling access to other criminals.

Slipping through Facebook's detection

F-Secure observed one scam page publishing a new Post every couple of minutes, totaling roughly 47 posts in an hour, with each post tagging 25-30 pages. This resulted in over 1,000 Pages being targeted each hour for several days before Facebook shut it down.

"This type of spamming seems to be able to evade Facebook's inauthentic behavior detection systems surprisingly well," Latto said.

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

The first line of defense for Page owners is to secure your personal account with a strong, unique password and turning 2FA (two-factor authentication) on. You should also periodically review which apps, agencies or ex-employees have access to your Page.

> **"F-Secure observed one scam page published a new post every couple of minutes."**

Sarogini
Manager of Threat Protection Engineering Team
Kirkkonummi, Finland

expert tip

A reputable mobile security product such as F-Secure TOTAL will do a regular scanning of your device to make sure no known malware has been detected. If an infection is found, uninstall the malicious app and stop using the device for any financial transactions.

> **“Check an app's reviews for fake comments and overly positive 5-star evaluations.”**

Sharkbot reappears

The malicious Android app has been spotted in the Google Play store and it continues to spread by other means

Just when you thought it was safe to go back in the water, two versions of the Android malware Sharkbot have been spotted inside Google Play, again.

Tens of thousands of users appear to have downloaded the most recent versions of the malicious software posing as an antivirus app.

Sharkbot has fierce features

F-Secure has been detecting Sharkbot since early 2022, says Sarogini, who leads F-Secure’s Threat Protection Engineering team.

“Based on our telemetry, victims were mostly from Europe, with the vast majority of infections found in the United Kingdom,” she said.

The fake apps allow criminals to steal victims’ credentials. They include a keylogger to track button clicks and SMS intercept, which reveals all text messages. In addition, remote control functionality allows criminals to bypass security features to make financial transactions without the device owner’s knowledge

“While Sharkbot versions do occasionally appear inside the official Play store, the malware has spread continually this year via text and instant messages.”

Be careful which apps you invite into your device

Taking time before downloading any app is a good rule. “Android users should be very careful when clicking links leading to the installation of ‘Antivirus’ or ‘Cleaner’ apps,” Sarogini said.

“Check an app’s reviews for fake comments and overly positive 5-star evaluations. Likewise, look out for very poor reviews, which could come from victims who have experienced unusual or malicious activities after installation.”

Breach reports

Locally

Discovered: 3/11/2022

Affected people:
Nearly 1.9 million users

Breach severity: ⚡⚡⚡⚡

After Locally.com was breached in October, private data from the shopping site began to be privately shared on the internet. In addition to names, email addresses, and passwords, stolen credit card information is being circulated. Affected users should contact their banks and replace this card with a new card number immediately. Ask your bank to check for fraudulent transactions and file a fraud alert with one of the credit bureaus.

PrivatBank

Discovered: 10/11/2022

Affected people:
Nearly 27 million customers

Breach severity: ⚡⚡⚡⚡

Data belonging to PrivatBank was leaked on a Telegram channel in September. Names, email addresses, phone numbers, passport numbers, and usernames from the Ukrainian financial company are being privately shared on the internet. This information could easily be used to falsify documents. Anyone whose information has been shared as part of this leak could become the victim of a highly targeted spear phishing attack that exploits the stolen data. Extreme caution is advised.

Gmail Combolist

Discovered: 17/11/2022

Affected people:
More than 100,000 Gmail users

Breach severity: ⚡⚡⚡

This collection of Gmail addresses and passwords from previously breached sites was shared on a hacking forum. This data is likely being used for 'credential stuffing,' a technique where criminals automate the work using lists of stolen credentials brute-force tools to try to crack into the accounts on thousands of other websites. All Gmail users should secure their accounts with strong unique passwords and use two-factor authentication for added protection.

US Based Fraud Protection Company

Discovered: 17/11/2022

Affected people:
More than 400,000 consumers

Breach severity: ⚡⚡⚡⚡⚡

Information belonging to a U.S.-based fraud protection software company was leaked on a hacking forum in October of 2022. The data contains names, emails, phone numbers, and credit card numbers. Victims should immediately report their credit cards as stolen. Given that the company breached was in the business of preventing fraud, customers should also expect targeted and convincing phishing attacks. Any email regarding fraud protection should be verified by a phone call to the company that sent it.

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

Emotet returns

The massive malware botnet has returned from vacation to spam users with hundreds of thousands of malicious emails each day

The massive malware operation known behind Emotet has returned from a four-month vacation and is currently blasting out millions of emails each week to spread its malware.

Change is nothing new for Emotet

F-Secure researchers Yik Han and Amit Tambe have tracked Emotet's activity and noted that the malware has regularly taken breaks and returned with new functionalities since it first appeared as a banking trojan in 2014.

"The group has become a successful malware-as-a-service offering, which has been used by a variety of threat actors leading to a variety of attacks, including some ransomware attacks," said Yik Han.

The threat actors utilizing Emotet have also continued to evolve their delivery methods, using a variety types of file attachments in spam campaigns--including malicious documents with macros, PDFs with malicious links, and password-protected zips.

Consumers pay when Emotet plays

"Constant development makes Emotet malware a popular choice of criminal groups that carry out attacks against key industries—including health care, higher education and public sector infrastructure," Yik Han said. "These attacks often lead to the theft of huge amounts of consumer information."

Criminals often sell stolen data on the dark web—leading to identity theft, fraud, and various scams.

Yik Han
Researcher
Puchong, Malaysia

expert tip

A tool like F-Secure's IDENTITY PROTECTION helps you check if your information has been breached. Watch out for any unusual activity related to your data—such as increased spam, unusual calls, or misuse of your email to sign up for services.

> **"Constant development makes Emotet malware a popular choice of criminal groups."**

Patricia Dacuno
Senior Researcher
Helsinki, Finland

expert tip

Information stealers often arrive as fake installers or cheats for gaming apps. That's why your family should only download software from trusted and official websites. Also, avoid opening attachments and clicking links from email messages coming from unknown senders.

StrelaStealer robs emails

New malware goes after users of two popular email clients and shows how infostealers keep expanding their targets

Newly identified malware StrelaStealer goes after email credentials by targeting users of Microsoft Outlook and Mozilla Thunderbird. This infostealer was first spotted targeting Spanish businesses in early November.

Business users of all sizes targeted

"Outlook is the most popular email program for large businesses and enterprises, while many smaller businesses rely on Thunderbird, which is free," said Patricia Dacuno, Senior Researcher at F-Secure.

She noted the decoy document sent as an attachment in the attack claims to come from a vehicle-leasing company that serves mostly corporate clients.

"This suggests businesses, perhaps specific businesses, are the current target of the threat actors," she said.

A new goldmine

By focusing on credentials stored in email clients, StrelaStealer adds to the long list of data types infostealers have targeted.

"Infostealers typically grab data stored in browsers by the autofill feature," Dacuno said. "The data they steal, and then often leak, can include a variety of personal and financial details."

Criminals may follow up the attacks by stealing money or cryptocurrency, selling information on the black market, or using stolen information to carry out additional attacks.

Don't feed the stealers

"To protect your data from being stolen, avoid using the autofill feature of the browser as much as possible—especially for sensitive information, such as usernames, passwords, billing information, or any personal identification," Dacuno.

"Stolen email addresses can make fake messages look more legitimate to lure unsuspecting users."

Huge breach for insurance firm

Medibank customer data has been breached and leaked by a group suspected to be associated with notorious ransomware gang REvil

Criminals have continued to release highly sensitive data for patients covered by Australian insurance giant Medibank after nearly 10 million customers had their data exposed early in November.

Extortion continues to ramp up

“Private information has been compromised, but Medibank has made the right decision by not paying the ransom and therefore funding cyber crime,” said Laura Kankaala, F-Secure’s Threat Intelligence Lead. “When dealing with ransomware gangs, there are no guarantees that paying would actually change anything."

The threat actors—which many experts believe to be associated with REvil, a ransomware gang the Russian government claimed to have shut down in January of this year—started by dumping masses of data on their leak site on dark web.

This has been followed by a gradual release of medical records.

“These records don’t show a patient’s whole medical history, unlike in the case of the Finnish psychotherapy firm Vastaamo where entire case histories were leaked,” she said. “However, there are diagnosis numbers associated with treatments received.”

This has led to patients from the Medibank leak with a history of mental health care being placed on a dark web list entitled “Psychos.”

“Despite the escalation, Medibank has continued to insist it will not pay,” she said. “The attackers said that they are waiting to post more information soon unless their demands are met."

After leaking some more data on the weekend before Black Friday, the attackers' leak site suddenly went offline without any explanation. Days later, the site reappeared just as mysteriously, and the situation continues to evolve.

Laura Kankaala

Threat Intelligence Lead

Helsinki, Finland

expert tip

Protect your online identity with strong and unique passwords and enable multi-factor authentication for services that you use. Furthermore, be cautious for phishing attacks and immediately contact the police in case any extortion attempts are made towards you.

> **“Private information has been compromised, but MediBank has made the right decision.”**

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