F-Alert

Monthly threat updates from

F-Secure

April 2023

F-Secure

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

Find out about the takedown of one of the biggest criminal marketplaces on the web. Discover how AI can be used to scam you. Get an inside look at Apple's latest security updates. And learn how to charge your phone in public safely.

Hoai Duc Nguyen
Researcher
Helsinki, Finland

expert tip

Reduce the amount of data that criminals can access and make it harder for them to abuse it. For instance, don't save critical login credentials or data to autofill in your web browser. You'll lose a little convenience, but you gain a lot of safety.

"Genesis Market had 80 million sets of credentials and digital fingerprints up for sale."

Cyber crime superstore stopped

An international effort called "Operation Cookie Monster" has seized the Genesis Market, a thriving dark web marketplace.

Law enforcement around the world led by the FBI and the Dutch National Police Corps had arrested more than a hundred people on the 4th of April, bringing down one of the world's biggest marketplaces for stolen data.

80 million!

"Genesis Market had 80 million sets of credentials and digital fingerprints up for sale," said Hoai Duc Nguyen, a researcher at F-Secure. "The marketplace also offered stolen data including browser histories, cookies, form autofills, and IP address locations which allow attackers to log into victims' account without raising suspicion."

Stolen Facebook, PayPal, and Amazon accounts were among those up for sale for as little as a $1 each.

"It's worth noting the number 80 million, which indicates large scale data theft gathered through many cybercrime campaigns," he said.

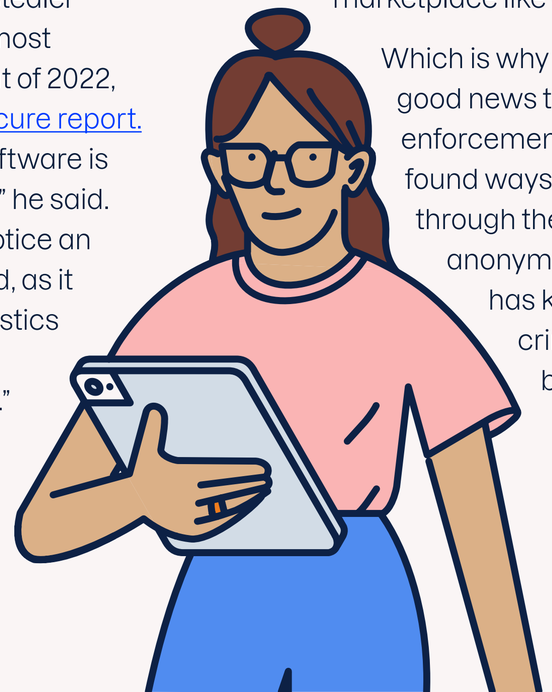
As the name implies...

Nguyen connected that the growth of dark web marketplaces is directly related to the rise of infostealer trojans, which were the most common Windows threat of 2022, according to a new F-Secure report. "This sort of malicious software is both tricky and effective," he said. "Users generally won't notice an infostealer being installed, as it shares a lot of characteristics with legitimate software and often disguises itself."

F-Secure has seen this type of trojan embedded into pirated applications, shipping notices, and unpaid invoices.

"As the name implies, infostealers access private data, such as browser cookies, saved usernames, and passwords, to suck it up," Nguyen added. "And the next thing you know, your credentials end up for sale in a marketplace like Genesis."

Which is why it's very good news that law enforcement has found ways to break through the dark web anonymity that has kept these criminals in business.



AI's risks get real

ChatGPT has alerted the masses to the power of AI, but consumers also need to be aware of its security risks.

The groundbreaking AI chatbot ChatGPT from OpenAI has amassed more than 100 million users since it was opened to the public in December of 2022.

While this and similar generative AI tools are likely to transform fields ranging from software to education to health care, they will also give cyber criminals powerful new advantages.

A new era for phishing attacks

Generative AI is likely already improving the effectiveness of phishing scams, explained Abdullah Al Mazed, F-Secure's Senior Technical Product Manager, whose expertise lies in creating solutions that protect consumers against emerging threats.

"You had probably seen some phishing emails or an SMS where you could instantly detect the attack because of a grammatical or spelling mistake. Those days will be a thing of the past," said Mazed. "ChatGPT demonstrates how far the Natural Language Processing field has already gone and how easy it is to write a very convincing mail or blog post by just giving a few keywords."

And as AI advances, so will the risks. "Phishing attacks will only get more sophisticated," he said. "Soon, you should expect an automated multi-step process where the first communication will have no links to a phishing page, no request to do anything specific but just very convincing texts that initiate a conversation."

Take a pause?

AI tools also come with the same sort of privacy concerns that arise from most online services, along with some unique issues of their own.

A data leak from ChatGPT forced the company behind the chatbot, OpenAI, to take the tool down briefly. And Samsung employees apparently fed confidential company data to the tool. These privacy issues have prompted regulatory concerns from many governments, including an outright ban of the tool from the Italian government that will lift if OpenAI takes "useful steps."

In addition, a group of tech leaders and academics have called for "a pause" in the development of AI tools that build on the existing models available to the public.

But consumers shouldn't expect the development of these tools to slow down in any way. In fact, the power and impact of these tools are likely to increase dramatically.

Abdullah Al Mazed
Senior Technical Product Manager
Oulu, Finland

expert tip

If you aren't among the hundreds of millions that have tried ChatGPT, take the time to try it out. When you experience firsthand how convincing a conversation you can have today with an AI, it will probably help you be more careful when you engage in a chat with an unknown party over the internet and help you avoid potential phishing attacks.

"Phishing attacks will only get more sophisticated."

F Secured: your free 38-page guide to online security in 2023

The F-Secured guide provides a comprehensive overview of the cyber security threats facing consumers in 2023, featuring insight and advice from F-Secure experts.

Whether you're looking to get the lowdown on malware; understand security and the connected home; master your use of passwords; learn about the latest phishing threats; or get the latest cyber security trends for 2023, the F-Secured guide reveals everything you need to know, including how to best protect yourself against emerging threats.

Download it now to find out more about:

- Malware today and how to protect against it
- Security and the smart home
- Cyber security CSI: 5 top threats
- How to master your passwords
- Trends and predictions for 2023

Download F-Secured today

Dylan Tham
Researcher
Kuala Lumpur, Malaysia

expert tip

The days of thinking Apple devices are immune to malware are long gone. Apple users should take these updates as seriously as Apple does. It is crucial to keep your operating system and applications up to date with the latest security patches and updates.

“It is also possible for an attacker to chain both these vulnerabilities together.”

Attackers target holes in Apple

The technology giant has released an update to plug two critical vulnerabilities being exploited by attackers.

Apple released an important security update in early April to address two critical vulnerabilities. These fixes have been pushed to all PCs running macOS and mobile devices using iOS, which powers the iPhone and iPad.

A rare weekend update

“That Apple pushed these updates out over the weekend, something the company rarely does, shows how important they are,” said Dylan Tham, a researcher at F-Secure. “It appears that attackers are actively exploiting both vulnerabilities.”

The first is a vulnerability found in WebKit, an engine used by many popular browsers, including Safari and Google Chrome, across different operating systems such as iOS and macOS.

“The vulnerability in WebKit could allow attackers to create maliciously crafted web pages or HTML emails that can trigger the vulnerability when loaded in a vulnerable browser or email client,” he said.

Tham added that once a victim visits a site with the malicious code, the attacker could potentially take complete control of the device and access sensitive data.

’Highest level’ of access

The second vulnerability was found in a technology used in various applications such as video processing and graphics rendering.

“The exploitation of this vulnerability can lead to an attacker gaining the highest level of privileges on an operating system, allowing direct control over hardware and memory resources,” Tham said. “That’s an attacker’s dream come true.”

Tham noted that both attacks can be introduced to a victim's machine through various methods such as phishing emails, social engineering attacks, or malicious websites.

“It is also possible for an attacker to chain both these vulnerabilities together,” he said.

How to get a safe charge

The FBI has issued a warning about public phone charging stations. But the risks are minimal, and a better solution is obvious.

Avoid public charging stations. That's the gist of a new warning from the US Federal Bureau of Investigation (FBI).

While she agrees with the advice, Laura Kankaala, F-Secure's Threat Intelligence Lead, wants consumers to know the risks that come from a public charging station are relatively minimal.

Trust this device?

Kankaala has demonstrated these sorts of attacks before to different audiences, such as in a Finnish TV documentary and in keynotes. "In general, these USB charging port attacks aim to steal information stored on phones by mounting the internal storage of the phone to a computer they are connected to," she said.

While charging wires do open the possibility of direct access to a device, a full-blown compromise is not likely.

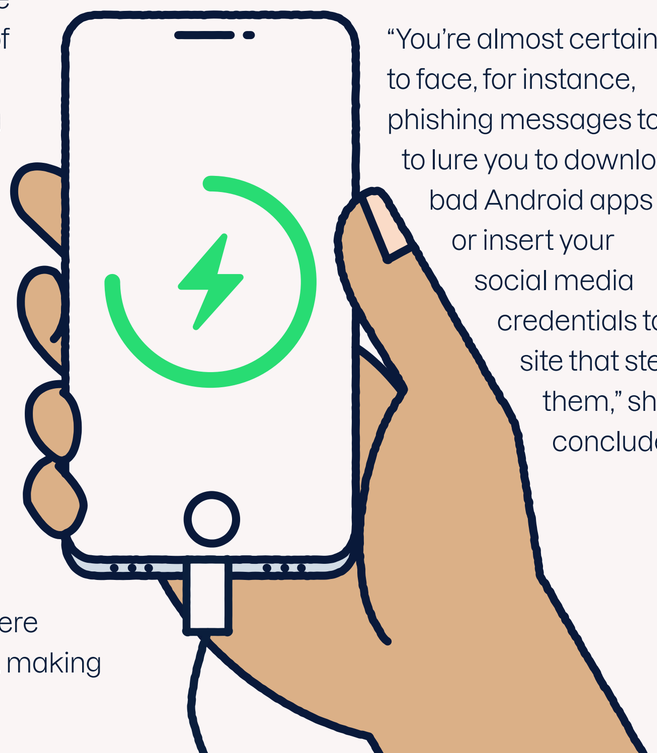
"Modern and up-to-date smartphones prompt users to 'trust' the device upon connection. Something you should never do on a public charging station in case it prompts you for it," she said. "However, if your smartphone is really old, it may lack these security features and be far more susceptible to all kinds of attacks, including those that use a USB charging port."

Not a mainstream problem

"All in all, it is unlikely that these sorts of attacks will become a mainstream problem, because they require someone physically accessing the place where the attack is carried out, making them quite targeted and not very easily scalable," she said.

Using your own charger to charge your phone via a wall socket is the safest option, but Kankaala advises that you are far more likely to encounter far more common threats.

"You're almost certain to face, for instance, phishing messages to try to lure you to download bad Android apps or insert your social media credentials to a site that steals them," she concluded.



Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

If you do need to use a public charging station, you should use a USB data blocker.

"If your smartphone is really old, it may lack these security features and be far more susceptible to all kinds of attacks."

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 180 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