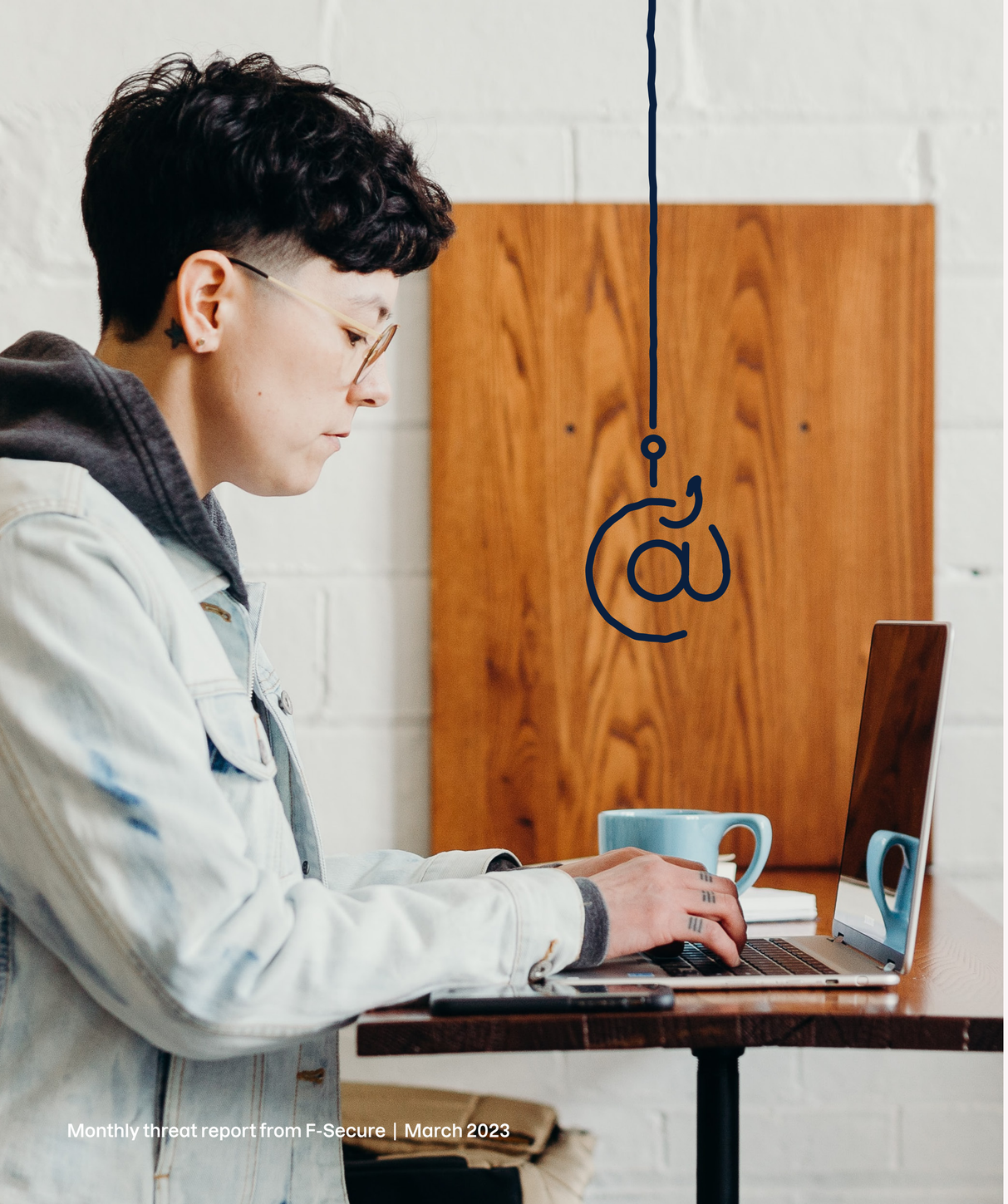
F-Alert

Monthly threat updates from

F-Secure

March 2023

F-Secure



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

Find out how parents may pay when criminals target gamers. Discover how “pig butchering” scams are breaking hearts and emptying bank accounts. Learn how proposed legislation to fight child abusethreatens the integrity of the internet. And read how the month's biggest leaks might affect you and your data.

Yik Han
Researcher
Puchong, Malaysia

expert tip

The Internet is filled with traps and frauds related to cryptocurrency and decentralized finance (DeFi). Click with extreme caution and make sure you're using internet security with both browsing and banking protection, like F-Secure Total, if you access a crypto wallet through any of your devices. Otherwise you could download malware straight into your computer designed to steal everything in your wallet.

Bank failures fuel rising threats

The collapse of Silicon Valley Bank and Signature Bank have triggered the sort of "fear, uncertainty, and doubt" that cyber criminals love to prey upon.

The failure of two prominent mid-sized American banks in early March has unleashed new worries about the global banking system, and online crooks have immediately seized on the chaos.

A false sense of urgency

"The combination of fear, uncertainty, and doubt in the news combined with a false sense of urgency creates a perfect opportunity for malicious threat actors," said Yik Han, a researcher at F-Secure. And soon after the failures multiple cyber security firms issued warnings about how criminals had responded, by crafting attacks that seized upon the narrative of shaky financial institutions threatening global economic security.

Researchers have also uncovered the registration of multiple domain names related to the failed banks now linked to malicious websites and phishing scams. And this trend follows a familiar pattern.

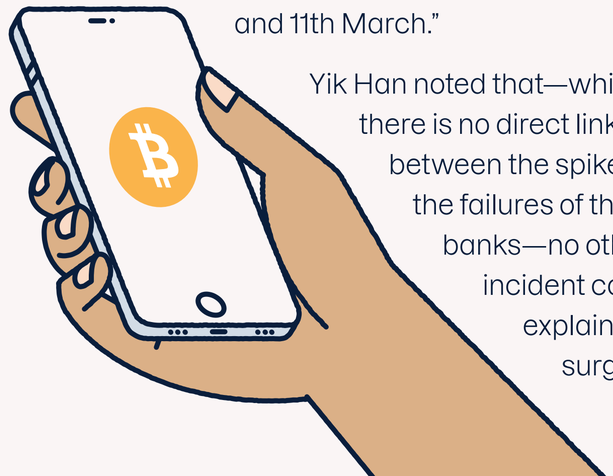
"When cryptocurrency exchange FTX collapsed last year, phishing websites started popping up left and right trying to scam FTX's users under the pretense of helping them recover their losses," Yik Han explained.

A surge in crypto-related threats

Yik Han added that as people lose confidence in banks, they often seek alternative means for holding their assets—Including cryptocurrencies like Bitcoin. And criminals are always ready.

"F-Secure detects and blocks malware spread by crypto scams and malicious web3 projects," he said. "We noticed a big spike in these crypto-related threats on the 10th and 11th March."

Yik Han noted that—while there is no direct link between the spike and the failures of the two banks—no other incident could explain the surge.



"We noticed a big spike in these crypto-related threats on the 10th and 11th March."

Cyber criminals target gamers

The rise of the video game industry combined with the explosion of remote work have created new opportunities for cyber criminals.

Scams targeting video game players can lead to cyber crimes ranging from credential theft to targeting the employers of the parents of younger gamers with financially motivated attacks, a new report finds.

Everyone can be a steppingstone

"Gaming is massive. A recent F-Secure survey found that it's even more popular among kids than social media," said Joel Latto, F-Secure Threat Advisor. "Because games aren't usually associated with high financial risk, gamers tend to not take their security very seriously. And kids usually aren't security conscious at all."

With the vast number of parents doing work on devices that may also be used by their kids to play games, Latto feels that criminals are simply doing what they do best—being opportunists.

"Everyone can be a steppingstone toward something else, but most attacks are automated and simple," Latto noted. "Criminals probably aren't targeting your employer's network specifically. But they might do so by chance—if they're lucky and sophisticated enough."

Exploiting gamers' bad habits

Latto suggested that parents should talk to their kids about security hygiene. This would include using strong unique passwords and two-factor authentication for all their gaming accounts, especially accounts that are connected in any way to credit cards.

He also noted that gaming may give parents a chance to talk about cheating, without much moralizing.

"One of the most common ways for gamers to infect their devices is to look for cracked games or other types of cheats that may be found through Discord channels," he explained. "And cheaters rarely prosper because the cracks may not even work. But they often deliver malware, such as infostealers."

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

Parents can do more than have discussions about online security. They can also provide their kids with a good example. And it should go without saying that devices used for work should be used only for work.

"Criminals probably aren't targeting your employer's network specifically. But they might do so by chance."

Breach reports

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

BeenVerified

Discovered: 14/3/2023

Affected people:
Nearly 147 million

Breach severity: ⚡⚡

Data leaked in August of 2020, which allegedly belongs to BeenVerified, a U.S-based background check company that offers personal searches of public records, has been found on the internet. The data contains names, emails, phone numbers, addresses, and other personal information. Affected users should be most worried about spear phishing attacks that target them through either email or SMS messages. Skepticism of all email or SMS links in general is advised.

Major League Baseball (MLB)

Discovered: 14/3/2023

Affected people:
More than 3 million

Breach severity: ⚡⚡⚡

Data that allegedly belongs to Major League Baseball (MLB), which includes names, email addresses, and phone numbers, is being shared on the internet. Give that MLB is one of the most prominent professional sports leagues in the world, this leak offers a prime opportunity for targeted phishing attacks that use trust in the league to provoke victims into offering up private data clicking on malicious links.

BidenCash

Discovered: 9/3/2023

Affected people:
More than 2 million

Breach severity: ⚡⚡⚡⚡

BidenCash, a dark web credit card marketplace, has apparently leaked millions of credit card numbers online to "celebrate" its first anniversary. The data contains names, addresses, credit card information, emails, and phone numbers, and is being shared across the internet. If your information has been included in this leak, call your bank's fraud department immediately to report your card as stolen.

AT&T

Discovered: 14/3/2023

Affected people:
Nearly 5 million

Breach severity: ⚡⚡

Data that appears to belong to AT&T has leaked online. Email addresses, device information, phone numbers, and names from this leak are being publicly shared in online hacker forums. The major concern for affected victims here is also targeted phishing scams. And when such attacks are connected to a company that users may rely on for services, they can be especially potent. Avoid all clicking on links in communications that allege to be from AT&T. Instead, speak to the company directly if contacted.

Is your data being exposed online? Check out our **F-Secure Identity Theft Checker!**

Tom Gaffney
Principal Consultant
London, United Kingdom

expert tip

While you still can, use apps that use end-to-end encryption in addition to a quality VPN that encrypts your data, like the one included in F-Secure Total, to protect your privacy. Do this even if you don't think you have anything to hide. Because even if you don't, someone probably thinks you do.

'Chat control' risks online safety

Plans to scan devices to fight child abuse pose a material threat to encryption standards that protect all internet users, experts say.

Proposed legislation in the UK and the EU aims to help law enforcement fight child sexual abuse materials (CSAM) and terrorism by granting broad new powers to automatically search citizens' devices.

Critics call this ability to conduct client-side scanning "chat control." They argue that the proposals constitute a power grab that allows governments to freely access private communications, which have been protected except in the most extreme circumstances.

A material threat

"We applaud efforts to fight CSAM," said Tom Gaffney, Principal Consultant at F-Secure. "But the reality of what's being proposed would fundamentally change the internet forever."

Gaffney says that the idea is "terrible", both from privacy perspective and as a material threat to encryption standards, which affects online safety for all. He says end-to-end encryption is the "gold standard" of private digital communications, which protects the online ecosystem that transformed billions of lives.

"Once you put a backdoor into the encryption, you've invited snoopers to find it and violate the privacy of every single person in Europe and, frankly, anyone who uses the internet," Gaffney added.

Magical thinking

A research paper by Ross Anderson of the Department of Computer Science and Technology at the University of Cambridge argues that these proposals epitomize "the sort of magical thinking that leads to bad policy."

He notes that neither local nor national law enforcement agencies have effective ways of dealing with "false positives" that lead to unlawful surveillance of innocent individuals as allowed by current UK law.

He says until that's fixed no-one should even think about expanding police powers into more device scanning.

"The reality of what's being proposed would fundamentally change the internet forever."

‘Pig butchering’ fuels fraud

Schemes that combine the worst of romance and financial scams have helped make fake investments the costliest cyber crime reported to the FBI.

The Internet Crime Report for 2022 from the FBI has found that investment fraud has cost internet users over $3 billion, with over $2.5 billion of that coming from scams related to cryptocurrency. And a con unsympathetically known as “pig butchering” has helped fuel these losses from investment fraud.

Weaponizing trust

In these scams, lonely people seeking romantic connections or friends are systematically “fattened” to increase the money they dump into fake investments. The key to these “pig butchering scams” is trust, said Laura Kankaala, F-Secure’s Threat Intelligence Lead. “The trust can be obtained by texting the victim, or even connecting with them over social or dating platforms,” she said. “After a brief discussion, the victim is lured into an investment platform—which is actually the core of the scam.”

Victims are lured into investing money, generally involving cryptocurrency. The criminals are leveraging fake websites, or mobile apps, which they have managed to slip into official app stores for iOS and Android devices.

“Sometimes victims may take out loans or simply transfer all their money into the phony platform or app controlled by the criminals,” Kankaala explained.

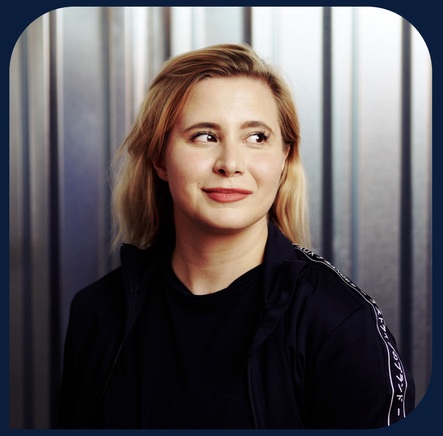
Even the butchers are often victims

The scam often begins with a simple “Hi” from a stranger with an attractive profile picture. These profiles are fake and use stolen pictures.

“It’s likely that message is coming from a building in Southeast Asia filled with people sending out tens of thousands of similar messages every day,” said Kankaala. “They’ve been trained in the exact steps proven to steal as much money as they possibly can.”

Even the perpetrators of these scams themselves are often the victims of horrific crimes.

“It appears that many of the scammers have been tricked by human traffickers into captivity where they have to defraud people or endure beatings, starvation or worse,” Kankaala noted.



Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Online romance and financial entanglements are a dangerous mix. If someone you've never met before in real life starts to talk about cryptocurrency—or any type of investment—be very careful. The criminals may leverage familiar-sounding brands or something similar to existing trading platforms, which make their scams seem legitimate if checked via a Google search.

“Eventually, the perpetrators run away with the money.”

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