September 2024

F-Alert

The latest cyber security threat updates from F-Secure threat intelligence experts

F-Secure

Are platforms like Telegram the new dark web?

EXPERT INSIGHT:

“The dark web is often used as a catch-all term for criminal activity online, typically referring to networks like Tor. But everyday platforms such as Telegram, Discord, and even social media have also become places to buy and sell illegally obtained data or serve as building blocks for the technological infrastructure of attacks. It’s important to stay vigilant on all online platforms as today's ‘dark web’ is closer to us than we might realize.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

WHERE: Global

WHAT: Cyber crime used to be predominantly associated with the dark web. While it remains active there, we are now seeing a growing presence of criminal activity on 'clear web' platforms like Telegram, Discord, and social media platforms such as Facebook.

KEY FACTS:

- Telegram has evolved into more than an instant messaging app – it’s often viewed as an easily accessible gateway to illegal activities that we associate with the term ‘dark web’, thanks to its publicly searchable chat groups and encrypted messages.
- The recent arrest of Telegram’s CEO has only amplified concerns regarding the app’s content moderation – or lack thereof it.
- A recent alleged breach and leak of over 330 million email addresses was falsely attributed to SOCRadar by a threat actor. However, there was no actual breach or leak. Instead, the threat actor collected public Telegram channel names from the platform and scraped publicly available data from these channels.

Exposing Active Listening technology in your phone

WHERE: Global

WHAT: "Is my phone listening to me?" is a question that has been asked for years (we even covered it in a 2019 video). While some say no, a leaked Cox Media Group (CMG) pitch deck reveals that their Active Listening technology, designed for ad targeting based on what people say near their devices, proves otherwise.

KEY FACTS:

- In a recent report exposing CMG's leaked pitch deck, CMG claims its tech listens to device microphones and advertises to users accordingly.
- CMG has also partnered with Google, Amazon, and Facebook – although we can't confirm that Active Listening tech is used by these platforms.
- In a since deleted blog post, CMG said: "It is legal for devices to listen to you. When a new app download or update prompts consumers with a multi-page terms of use agreement somewhere in the fine print, Active Listening is often included."

EXPERT INSIGHT:

"We can now confirm that the technical capabilities to execute this level of pervasive eavesdropping is 100% possible, and similar products are likely offered by other tech companies. While it's nearly impossible for consumers to sift through every Terms of Service to determine if a platform can listen to everything, what they can do is review their device settings and app permissions to limit microphone access."

Joel Latto
Threat Advisor
Helsinki, Finland

Trending Scam

Majority of businesses hit by deepfakes

WHERE: US and UK

WHAT'S HAPPENING:

- A Medius survey reveals that more than half of businesses in the US and UK have faced financial scams involving deepfake technology, with 43% falling victim.
- Criminals are increasingly using deepfakes to impersonate CEOs, CFOs, and other key staff, tricking employees into sending money or sensitive data.
- 85% of those surveyed see deepfake scams as an "existential" threat. Deloitte predicts generative AI could lead to $40 billion in fraud losses in the US by 2027.

WHAT TO DO:

- Train all employees, especially those in high-risk roles, to identify deepfakes and respond appropriately if targeted.
- Prepare for potential attacks by segregating duties for wire transfers and using technology to detect suspicious activity and transactions.

Breach that matters

Millions at risk in data broker breach

WHERE: US

WHAT'S HAPPENING:

- National Public Data, a background-check service, experienced a major data breach this year when a hacker stole personal information, including Social Security numbers (SSN) and contact details, potentially impacting millions of people.
- Initially, the company did not disclose the breach but has now acknowledged it.
- This raises concerns about identity theft and the security practices of data brokers.

WHAT TO DO:

- If your SSN is leaked, freeze your credit and set up financial monitoring.
- Use our free F-Secure Identity Theft Checker to see if your email address has been leaked in any data breaches. You can monitor if your SSN, email address, or other personal information has been leaked with F-Secure ID Protection.

EXPERT INSIGHT:

“While blocking SMS messages with malicious content helps to combat scams, we strongly urge consumers to stay vigilant about suspicious messages, especially those that exploit empathy. To protect iOS users from harmful SMS, F-Secure's AI-powered SMS filters automatically analyze and redirect harmful messages to a junk folder. This feature will also be available for Android users later this year.”

Calvin Gan
Senior Manager, Scam Protection Strategy
Kuala Lumpur, Malaysia

Can blocking URLs in messages stop SMS scams?

WHERE: Malaysia

WHAT: In an effort to combat SMS scams, telecommunications companies nation-wide have blocked the ability to send and receive text messages containing URLs and hyperlinks. While this is a significant step forward, it's important to acknowledge that it won’t completely eradicate the problem.

KEY FACTS:

- This month, the Malaysian Communications and Multimedia Commission (MCMC) directed telcos to block all hyperlinks and requests for personal information sent via SMS.
- Previously, enterprise SMS – such as promotional messages – were exempt from a May 2023 block on URLs in SMS.
- While this directive is a major step toward reducing smishing scams, it doesn't prevent scammers from using other tactics, such as directing victims to call a fraudulent phone number.

Inside Apple's privacy-focused approach to AI

WHERE: Global (except EU countries)

WHAT: Apple's upcoming release, Apple Intelligence (or Apple AI), promises a privacy-first approach for its users. However, with ongoing concerns and complaints about data protection and privacy surrounding generative AI, will Apple AI genuinely be any different?

KEY FACTS:

- Apple AI launches in the US first next month with iOS 18, iPadOS 18, and macOS Sequoia.
- One of Apple's key differentiators is its commitment to user privacy. For example, Apple Photos uses on-device processing for features like text recognition and image classification, keeping data private by ensuring it's not uploaded to Apple's servers.
- Apple employs a "Private Cloud Compute" system that enables devices to handle simpler tasks with on-device AI while offloading more complex processes to secure, advanced servers managed by Apple. Crucially, the servers never store user data.
- However, for tasks that require deeper understanding, like rewriting text or breaking down a complex problem, Siri will offer the option to connect to ChatGPT. This raises huge privacy, security, and factual inaccuracy concerns, if not handled well.

EXPERT INSIGHT:

"In a world where personal data feels increasingly vulnerable, Apple's initiative uniquely balances powerful AI-driven experiences with robust user privacy protections. This could set a new standard for tech giants. I do believe Apple AI is genuinely private, pending rigorous testing, but I probably won't connect my own ChatGPT account just yet."

Ash Shatrieh
Senior Threat Intelligence Researcher
Helsinki, Finland

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 200+ partners.

For more than 35 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 the latest news and updates visit f-secure.com or follow us on our social channels.

F-Secure