March 2025

F-Alert

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

F-Secure

DeepSeek Under Fire: Unpacking its Controversy

WHERE: Global

WHAT: Hyped tech often leads to increased crime and controversy—and DeepSeek, the industry-disrupting Chinese AI chatbot, is no exception. Malware and malicious code libraries are already masquerading as DeepSeek, tricking users into downloading them to their devices, but the biggest controversy centers around its privacy—or lack thereof.

KEY FACTS:

- DeepSeek collects user information, including chat interactions, when the chatbot isn't hosted locally. While most major LLMs offer settings to disable data collection for model training, DeepSeek does not provide this option.
- Users should avoid sharing sensitive personal or company information when using these tools. Some companies now provide isolated AI tools for employees, ensuring that data remains private and isn't shared with the tool's creator.
- Several countries have already banned DeepSeek over spying concerns. Additionally, security researchers recently exposed a vulnerability that allowed external parties to access user chat histories, further escalating security risks.

EXPERT INSIGHT:

"The hype around DeepSeek comes with the same problems as any overhyped technology. In the past, scammers exploited the OpenAI ChatGPT craze by distributing malicious apps, while ChatGPT itself faced scrutiny over privacy concerns. Now, the spotlight is on DeepSeek. The biggest issue, however, is its reluctance to address security and privacy risks. This lack of transparency and accountability raises serious red flags."

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

New FlexibleFerret Malware Targets macOS Users

EXPERT INSIGHT:

“Malware detection and evasion is an ongoing cat-and-mouse game, with threat actors continually evolving their tactics to remain undetected. In this process, even seemingly innocuous job seekers and software developers are no longer safe. Staying alert and cautious of unusual requests and phishing links is more important than ever.”

Amit Tambe
Researcher
Helsinki, Finland

WHERE: Global

WHAT: A new malware strain called ‘FlexibleFerret’ has been discovered, linked to the North Korean ‘Contagious Interview’ campaign. These threat actors are using advanced evasion tactics to target job seekers using macOS devices, as well as directly targeting developers.

KEY FACTS:

- The campaign traditionally uses fake jobs as an infection vector. Victims are tricked into clicking links disguised as missing or outdated software needed for their interview, ultimately leading to the download of malicious droppers.
- FlexibleFerret, the latest variant, operates under various pretexts, such as fake job interviews and bug reports on GitHub. When the victim runs the malicious installer, FlexibleFerret also installs a fake Zoom application that secretly connects to a suspicious domain.
- Although Apple updated XProtect, its built-in anti-malware system for macOS, in January to detect several 'Ferret' family variants, the latest FlexibleFerret variant remains undetected.

Trending Scam

Governments Warn of Scammers Posing as Officials

WHERE: Global

WHAT'S HAPPENING:

- A new wave of government imposter scams is sweeping the globe, with scammers using fake authority to steal money, personal information, and access accounts.
- The UAE recently warned about scammers posing as Ministry of Foreign Affairs officials, while the US Federal Trade Commission cautioned about fraudsters impersonating its Chairman, Andrew Ferguson.
- These scams typically begin with a call or message about an issue—such as suspicious account activity—then transfer victims to a 'government official' who offers to resolve it if they provide sensitive information, transfer funds, or grant remote access.

WHAT TO DO:

- A government official will never ask consumers to transfer money to another account, provide cash, or purchase cryptocurrency.
- If consumers receive an unexpected phone call, email, or text claiming they have an issue, we advise them to verify the claim before acting. They should not use the contact information provided but instead seek out official sources.

Breach That Matters

Healthcare Industry Remains Prime Target for Hackers

WHERE: US

WHAT'S HAPPENING:

- Healthcare providers continue to be top targets for data breaches, with hundreds of cyber attacks reported last year and new breaches occurring this year.
- Last October, UnitedHealth reported 100 million patients had their data stolen in the Change Healthcare ransomware attack. That figure has since nearly doubled to 190 million, making it the largest healthcare breach in US history.
- This year, Connecticut's Community Health Center notified over 1 million patients of a data breach, discovered two months after hackers accessed its network and stole patients' personal and healthcare data.

WHAT TO DO:

- Consumers impacted by healthcare data breaches should regularly monitor their credit and bank statements for unauthorized charges or new accounts opened in their name. They should also be especially cautious of phishing scams.
- Many healthcare providers involved in breaches offer free credit monitoring or identity theft protection to those affected, helping to catch fraudulent activity early.

EXPERT INSIGHT:

“Social media users and those interested in cryptocurrency should exercise caution with unverified crypto platforms, implement strong security measures like multi-factor authentication, and stay informed about emerging scams to avoid falling victim to these organized cyber criminal operations.”

Sarogini Muniyandi
Senior Manager, Scam Protection Engineering
Helsinki, Finland

'Crazy Evil' Gang Linked to Social Media Scams

WHERE: Global

WHAT: Russian-speaking cyber crime group, ‘Crazy Evil’, has been linked to a series of sophisticated scams targeting cryptocurrency users and influencers via social media platforms. Their operations involve multiple subgroups specializing in various fraudulent tactics, including phishing campaigns, fake crypto platforms, and malware distribution.

KEY FACTS:

- Luring victims by posing as legitimate cryptocurrency projects, Crazy Evil tricks them into downloading malware such as StealC, AMOS, and Angel Drainer, which steal sensitive data and digital assets.
- Active since at least 2021, the group uses private Telegram channels to coordinate and expand across platforms. Their fraudulent websites, including TyperDex, Selenium Finance, and Rocket Galaxy, impersonate real services to deceive users into financial transactions or credential theft.
- According to a new report, Crazy Evil has drained millions in illicit revenue and infected thousands of devices, impacting both Windows and macOS. These attacks highlight the growing risks in cryptocurrency and decentralized finance, particularly for influencers and investors.

Why Cross-Border Fraud Remains Hard to Police

WHERE: Global

WHAT: Cross-border fraud is evolving alongside cyber crime, becoming increasingly international, organized, and sophisticated. The ongoing 'scamdemic' is largely driven by organized crime networks, which often exploit low-cost labor in certain regions. Additionally, the growing accessibility of AI has further expanded their reach.

KEY FACTS:

- Thriving on jurisdictional loopholes, legal complexities, and the increasing interconnectedness of global trade, cross-border fraud presents a major challenge for law enforcement in tackling large-scale scams and pyramid schemes.
- Moreover, with rapid advancements in technology—especially AI—now widely accessible, scammers can easily bypass linguistic barriers using machine translation and deepfake audio, making their schemes more convincing than ever.
- A recent study by the Global Anti-Scam Alliance (GASA) calls for a stronger, more coordinated response to this growing issue, with greater collaboration between governments, law enforcement, private companies, and individuals essential to improving intelligence sharing and enforcement efforts.

EXPERT INSIGHT:

"I agree with GASA's call for a more structured global response to cross-border fraud; however, such a framework risks adding bureaucracy rather than streamlining efforts. While coordination is crucial, the real challenge lies in maintaining agility and avoiding administrative bottlenecks. Ultimately, combating fraud requires not just cooperation but continuous innovation—leveraging technology for protection just as criminals use it for deception."

Joel Latto
Threat Advisor
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