September 2025

F-Alert

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

F-Secure.

F-Secure Spotlights Human-Centered Security Research

WHERE: United States

WHAT: F-Secure cyber security researchers traveled to Las Vegas last month to present their latest human-centered findings at two of the world's largest cyber security events: Black Hat USA 2025 and the DEF CON 33 hacking conference.

KEY FACTS:

- DEF CON: Megan Squire, F-Secure Threat Intelligence Researcher, hosted a workshop titled 'From Prey to Playbook'—exploring what infostealer logs reveal about human behavior and how red teamers can leverage this information.
- Black Hat: Amel Bourdoucen, F-Secure User and Impact Researcher, shared insights into how some users are excluded from passwordless authentication.
- Advocating for a more human-centered approach to security, Amel highlighted an overlooked challenge: people who fall seriously ill can be failed by biometrics. Weight loss, tremors, and facial changes can cause fingerprint and facial recognition to stop working reliably, locking people out of their own accounts.

Read more: Designing a Passwordless Future That Won't Leave Users Behind

EXPERT INSIGHT:

"The future of authentication can't just be about removing passwords. For passwordless authentication to succeed, it must also enable quick, secure recovery when things go wrong and work for everyone—not just the tech-savvy or physically able. Password managers can play a pivotal role by serving as secure passkey vaults, helping users regain access without resorting to weak or exclusionary recovery flows."

Amel Bourdoucen
User and Impact Researcher
Helsinki, Finland

Online Safety Act Triggers Surge in VPN Downloads

WHERE: United Kingdom

WHAT: In July, the latest iteration of the UK's Online Safety Act came into effect, requiring platforms to enforce age verification for restricted content through measures such as ID checks and facial recognition. Free and paid VPN downloads in the UK have since surged.

KEY FACTS:

- As of 25 July 2025, the Online Safety Act legally requires digital platforms to protect children from harmful or age-inappropriate content by implementing age assurance technology. Platforms that fail to comply can be fined up to £18 million or 10% of their qualifying worldwide revenue.
- Many critics view age verification checks as an invasion of privacy, and VPN downloads in the UK spiked immediately—becoming the most downloaded apps in Apple's App Store within days.
- VPNs encrypt users' internet connections, masking their IP address and location—and, in this case, allowing them to bypass the Act's age verification requirements

EXPERT INSIGHT:

"These identity checks are intended to improve safety, but they may inadvertently drive some people to unsafe downloads. Consumers shouldn't trust free VPNs—there are no free lunches on the internet. Scammers and cyber criminals will capitalize on this trend, so we can expect a spike in SEO poisoning and fake ads for free VPNs carrying malware like infostealers."

Joel Latto
Threat Advisor
Helsinki, Finland

Trending Scam

Scammers Are Flooding Discord with Gaming Scams

WHERE: Global

WHAT'S HAPPENING:

- Ads for fake online gaming websites are spreading across social platforms, luring users with promises of free credits and fabricated celebrity endorsements.
- In one example, a fraudulent wagering site falsely claims a partnership with MrBeast—who recently launched the legitimate Beast Games. Capitalizing on this, scammers promote a "special" promo code offering $2,500 in free credit.
- To claim the credit, users create a free account and gain access to seemingly real betting games. When they attempt to cash out their winnings, they're told to make a "verification deposit"—money they never see again. 'Recovery experts' may then approach, promising to recover the lost funds, but these are scammers as well.

WHAT TO DO:

- Consumers should be extremely cautious of bold offers promising anything for free—particularly those involving cryptocurrency or credits. Any site that requires a payment in order to release money is almost certainly a scam.
- Scammers also frequently re-target victims by posing as recovery services. Service Providers should advise consumers to avoid anyone offering to retrieve lost funds, as such operations are simply another attempt to steal more money.

Breach That Matters

HR Powerhouse Workday Confirms Data Breach

WHERE: Global

WHAT'S HAPPENING:

- In a recent social engineering attack, threat actors targeted Workday and gained access to information through the third-party CRM platform Salesforce. The exposed data included business contact details, however, Workday stated that "there is no indication of access to customer tenants or the data within them."
- Workday employs more than 20,000 people worldwide and serves over 11,000 organizations across industries—including more than 60% of the Fortune 500.
- This incident is part of a broader wave of breaches exploiting Salesforce CRM through social engineering. Other affected companies include Adidas, Chanel, Dior, Google, Louis Vuitton, and Tiffany & Co.

WHAT TO DO:

Attackers impersonate HR or IT in phishing emails and calls to trick employees into linking a malicious OAuth app to their company's Salesforce instance. To protect against this:

- Never approve unknown or suspicious app connection requests.
- Verify unusual requests with IT or security teams before granting access.
- Review app permissions—broad or unusual access requests are a red flag.

The BadBox Botnet is a Bad Deal for US Consumers

WHERE: United States

WHAT: The FBI has issued a warning about the BadBox 2.0 botnet, which has transformed over 1 million consumer devices into digital proxies for criminal operations. This incident reveals how low-cost Internet of Things (IoT) devices are being infected with malware before they even reach stores, essentially weaponizing the global supply chain.

KEY FACTS:

- Unlike traditional malware, BadBox 2.0 is factory-installed in device firmware, meaning victims are compromised the moment they plug in their new purchase.
- The infected devices span everything from streaming boxes to digital picture frames, with most manufactured in China.
- The malware includes persistent backdoors that survive reboots and factory resets, using native libraries embedded deep in the device's operating system.

EXPERT INSIGHT:

"When malware comes pre-installed from the factory, it fundamentally breaks the trust and economic models of consumer electronics. Consumers may save money upfront, but they pay for it by inviting a criminal enterprise into their living room. To stay safe, they should avoid devices with prices that seem too good to be true, have disabled safety features, or require downloads from non-standard marketplaces."

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, US

Is 'Vibe Hacking' the Next AI Threat to Watch?

WHERE: Global

WHAT: The rise of AI-powered hacking—known as vibe hacking—is lowering the barrier to entry for cyber crime. While LLMs and other AI tools make hacking easier, they largely exploit already known vulnerabilities. Their main impact lies in extending threat actors' capabilities, making it easier to generate code, validate ideas, and even analyze data.

KEY FACTS:

- Vibe hacking is the use of LLMs and AI tools to assist in hacking activities. Just as vibe coding uses AI to generate software, vibe hacking applies it to identifying, exploiting, or testing vulnerabilities in digital systems.
- It can enable novice threat actors with no prior experience to attempt hacking—but, like vibe coding, it often produces flawed or non-functional code that requires expertise to fix.
- Most AI-driven hacking exploits known vulnerabilities, which remain the most common weakness in technology today. Tools like XBOW can expose these flaws, which is useful if they're fixed before criminals exploit them. Cases of AI finding previously unknown zero-day vulnerabilities exist, but they are rare.

EXPERT INSIGHT:

"LLMs and AI tools are changing the landscape of both software development and cyber crime. While they make hacking more accessible, the greater danger is how criminals weaponize AI to scale scams, fraud, and disinformation. AI tools already supercharge threat actors with vibe scamming capabilities—from multilingual phishing to deepfake video, audio, and images designed to deceive and disrupt."

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

illuminate

By F-Secure

> “Illuminate, F-Secure’s research function, brings together experts to explore the human, social, and technical aspects of security. We identify emerging threats, prototype new protection systems, and anticipate future risks to keep consumers safe. By staying ahead of the curve, we navigate a constantly evolving digital world and ensure F-Secure delivers trusted, reliable, and innovative cyber security solutions.”

Laura James

Vice President, Research

F-Secure

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 | illuminate