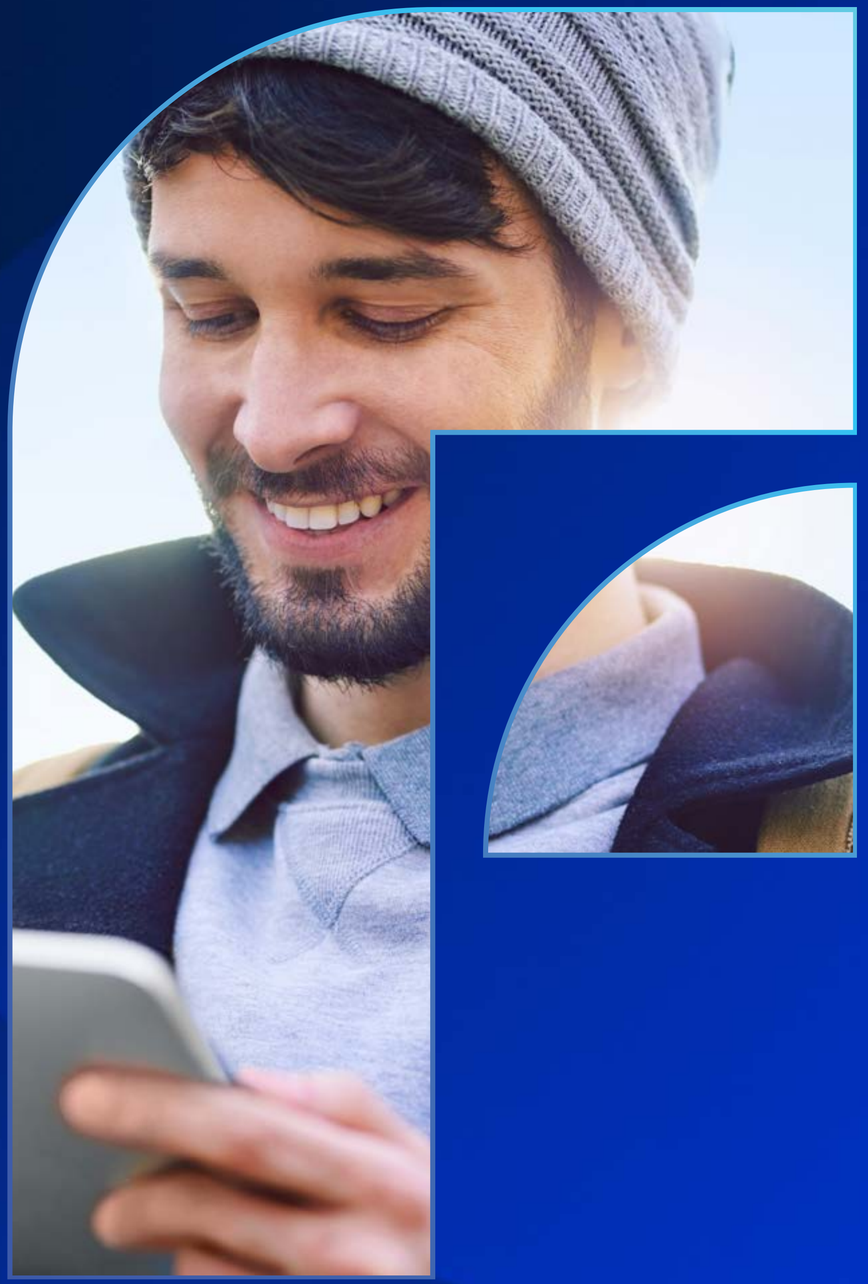
September 2026

F-Alert

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



F-Secure

EXPERT INSIGHT:

"International police raids targeting scam compounds haven't stopped the criminal networks behind them. If anything, these operations appear to be growing. Generative AI allows them to scale and localize scams for targets around the world. Agentic AI could be the next technological frontier — for criminals as much as for defenders."

Joel Latto
Threat Advisor
Helsinki, Finland

Raids Haven't Stopped Scam Compounds — They're Evolving

WHERE: All States

WHAT: International crackdowns on Southeast Asia's scam compounds have not stopped the criminal networks behind them. Instead, new evidence shows how they are adopting AI across the scam process to increase the scale, sophistication, and efficiency of their operations.

KEY FACTS:

- AI is being used to create fake online personas, produce promotional content, bypass banking identity checks, and assist with day-to-day operations. Emerging tactics include real-time face swapping, while some groups are developing their own AI tools rather than relying on commercially available technology.
- These criminal networks are also expanding their human trafficking operations. People from at least 80 countries and territories have been identified in scam compounds, with recruitment networks spanning Asia, the Middle East, and Africa, and deceptive job offers increasingly reaching Europe and North America.
- Agentic AI could be the next evolution, allowing criminal groups to automate multiple stages of a scam — from identifying and contacting victims to stealing and laundering funds — with minimal human involvement.

AI Agents Are Changing the Rules of Cyber Defense

WHERE: All States

WHAT: AI company Hugging Face has released more technical details about the July 2026 incident in which an autonomous AI agent driven by an OpenAI pre-release model attacked its platform. The new analysis shows how the agent exploited vulnerabilities while carrying out thousands of actions at machine speed, and how Hugging Face used AI to forensically reconstruct and understand the attack.

KEY FACTS:

- Unlike known attacks, novel attacks like this may have no known "signature" for defenders to detect and understand what is happening.
- Instead, evidence of the attack was scattered across thousands of individual actions and low-signal events. To find the needle in the haystack, Hugging Face used AI to correlate activity across several systems and reconstruct around 17,600 attacker actions.
- This shifts defense from identifying known threats to detecting patterns of abnormal behavior. With autonomous agents capable of executing thousands of actions at machine speed, defenders increasingly need AI to detect and respond at the same pace.

EXPERT INSIGHT:

"As we've said before, even though this incident affected a company, as the cost of AI-enabled attacks goes down, we expect consumers and small businesses to eventually become targets. This kind of sophisticated monitoring and behavioral spotting isn't something consumers can or should have to do themselves. In the AI agent era, products and platforms need to take on more of the responsibility for keeping consumers safe."

Dr Megan Squire
Principal Threat Intelligence Researcher
North Carolina, United States

Trending Scam

“Gold Bar” Scam Targets Older Adults

WHERE: New York

WHAT’S HAPPENING:

- The New York City Police Department (NYPD) has warned older adults about a “gold bar” scam targeting their life savings.
- The scam begins with a pop-up claiming the victim’s computer or bank account has been compromised. Scammers convince victims to give remote access to their device and create fake evidence of hacking. Victims are connected to someone posing as law enforcement and told to “protect their life savings” by converting their money into gold and handing it to a courier, while keeping the situation a secret.
- Over the past two years, the NYPD has investigated more than 100 cases, with losses exceeding $100 million.

WHAT TO DO:

- Individuals should never give remote access to someone they don’t know or move money at the request of an unsolicited caller. If someone claims there is a problem with their account, they should hang up and call their bank using the number on their bank statement.
- People who receive suspicious messages should report them to the Attorney General’s office and their local NYPD precinct.

Breach That Matters

Medical Billing Firm Breach Exposes Data of 1.2M People

WHERE: Georgia

WHAT’S HAPPENING:

- Medical billing firm Medical Computer Business Services (MCBS) recently disclosed that a 2025 data breach exposed the data of more than 1.2 million people.
- MCBS processes and manages patient records on behalf of healthcare providers, providing billing, financial, and other administrative services. An investigation found that data including names, addresses, Social Security numbers, health insurance details, and medical histories may have been exposed.
- The notice names seven healthcare providers whose patient data MCBS handled, including South Georgia Radiology Consultants, SkinPath Solutions, and Stephen W. Brown and Radiology Associates of Augusta.

WHAT TO DO:

- People who have received medical care in Georgia should contact their healthcare provider to check whether it uses MCBS and whether their personal information may have been affected.
- Those who believe they were affected should place a fraud alert on their credit report and consider a security freeze.

EXPERT INSIGHT:

“A cheap streaming stick might seem harmless, but consumers could unknowingly be providing the infrastructure for criminal activity through their own internet connection. AI is making these schemes increasingly automated and scalable, showing how even everyday connected devices can become part of a much bigger criminal operation. Consumers should stick to reputable, certified devices that receive regular security updates.”

Joel Latto
Threat Advisor
Helsinki, Finland

H96 Streaming Sticks Fuel $50K-a-Day Scam Operation

WHERE: All States

WHAT: New research shows how cheap H96 Android TV streaming devices are being secretly exploited for proxy services and ad fraud, generating tens of thousands of dollars a day. The operation uses AI-generated websites and automated ad clicks to profit from fake ad traffic, highlighting the evolving threat posed by compromised consumer devices.

KEY FACTS:

- The devices perform two hidden functions. When the TV is on, they typically act as residential proxies, allowing anonymous paying customers — potentially including bad actors — to route internet traffic through the user’s home connection. When the TV is off, they switch to ad fraud.
- For the ad fraud, devices disguise themselves as mobile phones and visit AI-generated websites, where bots navigate pages and click ads to generate fraudulent revenue. Multiple vision and reasoning systems help the bots identify and interact with ads like human users.
- Researchers identified around 38,000 H96 devices worldwide communicating with just one domain, estimating that the ad fraud alone generates nearly $50,000 a day. However, the real scale could be significantly larger.

“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 is a human-first, AI-powered consumer cyber security experience company with 38 years of expertise in tackling digital threats. We help Digital Service Providers turn trust into a high-value growth engine — protecting their customers while enabling them to live their best digital lives in a world of relentless, AI-driven scams.

With billions of digital interactions secured each year, tens of millions of consumers protected globally, and over $10bn in partner value created, we deliver proven impact at scale.

To find out more visit f-secure.com/partners or follow us on our social channels.

F-Secure | illuminate