August 2024

F-Alert

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

F-Secure

Beware ‘malvertising’ verified by Google

EXPERT INSIGHT:

“The easiest way to avoid these scams is to not click on search ads. This is especially important if you have a habit of using the browser's address bar as a search tool when you’re just looking to go to your bank’s website, for example.”

Joel Latto
Threat Advisor
Helsinki, Finland

WHERE: Global

WHAT: Criminals have used Google ads for years to lure victims to fake websites, often masquerading as popular free software downloads to spread malware. Now, they’re using fake Google Authenticator ads to lure users into downloading malware from GitHub.

KEY FACTS:

- Ads are listed prominently on search result pages to drive clicks.
- AI has enhanced the scale, sophistication, and effectiveness of malware ads.
- Criminals are hosting malware files such as infostealers on GitHub – a trusted software repository unlikely to get blocked via traditional methods.
- Google has been tricked into adding verification badges to some malicious ads.
- This ongoing ‘cat-and-mouse' game between criminals and search engines demonstrates how consumers could be lulled into a false sense of security.

Global IT outages: lessons from chaos

WHERE: Global

WHAT: Last month, mass IT outages were reported all over the world affecting everything from banks to airlines – and impacting vital everyday services that consumers rely on.

KEY FACTS:

- Healthcare, payment and banking systems were affected, thousands of flights were cancelled, doctors struggled to access records, and TV channels were taken off air.
- The cause was a faulty CrowdStrike software security update for Microsoft Windows devices.
- According to CrowdStrike's latest status, "99% of Windows sensors are online compared to before the update".
- Microsoft has offered help by producing a tool that makes recovery easier.
- Consumers should be wary of emails and calls related to the outages as they could have malicious intent.

EXPERT INSIGHT:

"Incidents such as these provide a stark reminder for companies to continuously plan and iterate a robust business continuity and disaster recovery plan. And when they do occur, it becomes a question of how fast companies can recover and resume operation, especially for critical services that impact the everyday person."

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

Exposing stalkerware's hidden dangers

EXPERT INSIGHT:

“Many stalkerware apps claim to be ‘parental control’ apps, but they’re not. They’re incredibly invasive, powerful, and notoriously lack security measures. Victims’ data is unwittingly compromised because people are misled by marketing – even the data of children, whose parents probably have no idea that these apps lack security features.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

WHERE: Global

WHAT: Not only is stalkerware extremely intrusive and unethical, it’s also a popular target for hackers to obtain, leak, and sell highly sensitive data. And it’s a significant issue – there have already been at least four major stalkerware app hacks this year, affecting millions.

KEY FACTS:

- Stalkerware apps are hidden malicious programs installed on victims’ devices to access everything – from viewing their location to recording their phone calls.
- At least 21 stalkerware companies have been hacked or had data leaked since 2017. The latest breach, which occurred in July 2024, exposed activity logs from Spytech spyware monitored devices.
- This history demonstrates just how little concern stalkerware companies have for protecting their consumers and safeguarding the data of their unwitting victims.

Watch Laura’s TEDx Talk on the dangers of stalkerware here.

Taylor Swift ticket scams surge

WHERE: Global

WHAT: Consumers are more likely to take risks when they deeply desire something – in this case, tickets to a Taylor Swift concert – which is why high-demand events are targeted by scammers. UK consumers alone have lost over £1m to Eras Tour scams so far this year.

KEY FACTS:

- Lloyds Bank issued a warning after more than 600 consumers fell for Taylor Swift ticket scams, while California's Attorney General issued an alert last year after receiving 16,884 complaints.
- Some events only sell official tickets through a dedicated website, while others sell through several vendors. Consumers should always refer to the event's official website to confirm legitimate sources.
- New Ticketmaster anti-touting measures mean that people must pre-register by a certain date, but scammers can capitalize on those who miss the deadline.

Read more insights from Ash about ticket scams here.

EXPERT INSIGHT:

"Access to ticket sales doesn't guarantee a ticket, so these events are more likely to attract scammers. When buying online, always use a platform which offers protection in the event of tickets not arriving. When buying from another person, always request an in-app ticket transfer."

Ash Shatrieh
Senior Threat Intelligence Researcher
Helsinki, Finland

Businesses targeted in infostealer breaches

EXPERT INSIGHT:

“The majority of modern malware focuses on collecting information or directly stealing money. Imagine sharing everything you do on your computer with cyber criminals – your banking credentials, passwords, personal information, and everything else. The long-term implications can be extremely severe.”

Timo Salmi
Senior Solution Marketing Manager
Oulu, Finland

WHERE: Global

WHAT: Hundreds of millions of customer records from large companies including Santander Bank and Ticketmaster have recently been listed for sale, compromised through cloud data storage firm, Snowflake. But this was no sophisticated hack – the attackers logged into each victim’s account using credentials stolen through an infostealer.

KEY FACTS:

- Infostealers steal everything from web browser data to usernames and passwords and are more frequently being used by cyber criminals to breach businesses.
- This is the most common form of malware, making up 89% of all Windows threats. However, last year we observed a steep rise in infostealers targeting macOS too.
- According to our 2024 study, only 5% of consumers have experienced a malware infection during the past year – and while it's less common for consumers, even a single malware infection can cause significant damage.

Is your domain a Sitting Duck?

WHERE: Global

WHAT: Millions of domain names are vulnerable to hijacking without detection, thanks to a powerful attack vector in the domain name system (DNS) across many DNS providers. Dubbed the 'Sitting Ducks' attack, it's easy to execute and hard to detect, but preventable.

KEY FACTS:

- More than a million domains are exploitable, with hundreds hijacked every day.
- In this attack, an inactive domain registered with a DNS service is taken over by the attacker without needing to log into the owner's account. Once they control the domain, they can carry out malicious activities while pretending to be the owner.
- Harmful actions can include malware delivery, data exfiltration, and phishing or spam campaigns impersonating the domain owner.

EXPERT INSIGHT:

"Sitting Ducks attacks happen because of mistakes in domain setup and weak security measures at the DNS provider. However, they can be prevented with action from all involved – registrars, DNS providers, web hosting companies, standards bodies, and government regulators. Domain owners should review and identify any inactive domains and ensure they use DNS providers with protections against this type of attack."

Amit Tambe
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 more information visit f-secure.com today.

F-Secure