ESET Threat Report: ClickFix fake error surges, spreads ransomware and other malware

DUBAI , DUBAI, UNITED ARAB EMIRATES, June 30, 2025 /EINPresswire.com/ -- ESET has released its latest Threat Report, which summarizes threat landscape trends seen in ESET telemetry and from the perspective of both ESET threat detection and research experts, from December 2024 through May 2025. One of the most striking developments this period was the emergence of ClickFix, a new, deceptive attack vector that skyrocketed by over 500% compared to H2 2024 in ESET telemetry. This makes it one of the most rapidly rising threats, accounting for nearly 8% of all blocked attacks in H1 2025 and is now the second most common attack vector after phishing.

ClickFix attacks display a fake error that manipulates the victim into copying, pasting, and executing malicious commands on their devices. The attack vector affects all major operating systems including Windows, Linux, and macOS. “The list of threats that ClickFix attacks lead to is growing by the day, including infostealers, ransomware, remote access trojans, cryptominers, post-exploitation tools, and even custom malware from nation-state-aligned threat actors,” says Jiří Kropáč, Director of Threat Prevention Labs at ESET.

The infostealer landscape also saw significant shifts. With Agent Tesla fading into obsolescence, SnakeStealer (also known as Snake Keylogger) surged ahead, becoming the most detected infostealer in our telemetry. SnakeStealer’s capabilities include logging keystrokes, stealing saved credentials, capturing screenshots, and collecting clipboard data. Meanwhile, ESET contributed to major disruption operations targeting Lumma Stealer and Danabot, two prolific malware-as-a-service threats. Before the disruption, Lumma Stealer activity in H1 2025 was higher than in H2 2024 (+21%) and Danabot was up even more, by +52%. This shows that both were prolific threats, making their disruption that much more important.

The ransomware scene further descended into chaos, with fights between rival ransomware

gangs impacting several players, including the top ransomware as a service – RansomHub. Yearly data from 2024 shows that while ransomware attacks and the number of active gangs have grown, ransom payments saw a significant drop. This discrepancy may be the result of takedowns and exit scams that reshuffled the ransomware scene in 2024, but may also be partially due to diminished confidence in the gangs' ability to keep their side of the bargain.

On the Android front, adware detections soared by 160%, driven largely by a sophisticated new threat dubbed Kaleidoscope. This malware uses a deceptive "evil twin" strategy to distribute malicious apps that bombard users with intrusive ads, degrading device performance. At the same time, NFC-based fraud shot up more than thirty-five-fold, fueled by phishing campaigns and inventive relay techniques. While the overall numbers remain modest, this jump highlights the rapid evolution of the criminals' methods and their continued focus on exploiting NFC technology.

Our research into GhostTap shows how it steals card details so attackers can load victims' cards into their own digital wallets and tap phones for fraudulent contactless payments worldwide. Organized fraud farms use multiple phones to scale these scams. SuperCard X packages NFC theft as a simple, minimalistic malware-as-a-service tool. It presents itself as a harmless NFC-related app, once installed on a victim's device, it quietly captures and relays card data in real time for quick payouts.

"From novel social engineering techniques to sophisticated mobile threats and major infostealer disruptions, the threat landscape in the first half of 2025 was anything but boring," summarizes Kropáč about the contents of the latest ESET Threat Report.

For more information, check out the ESET Threat Report H1 2025 on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown— securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts and blogs.

Sanjeev Kant

Vistar Communications
+971 55 972 4623
email us here