EINPRESSWIRE

ESET Threat Reports social media is flooded with deepfake scams and Formbook is now the No. 1 infostealer

DUBAI, DUBAI, UNITED ARAB EMIRATES, December 30, 2024 /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 June through November 2024.

Infostealers are one of the threat categories to experience a reshuffle, with the long-dominant Agent Tesla malware dethroned by Formbook – a well-established threat designed to steal a wide variety of sensitive data. Lumma Stealer too is becoming increasingly sought after by cybercriminals, appearing in several notable malicious campaigns in H2 2024. Its detections shot up by 369% in ESET telemetry.

Social media saw a flood of new scams cropping up, using deepfake videos and company-branded posts to lure victims into fraudulent investment schemes. These scams, tracked by ESET as HTML/Nomani, saw a 335% increase in detections between reporting periods. Countries with the most detections were Japan, Slovakia, Canada, Spain, and Czechia.

“The second half of 2024 seems to have kept cybercriminals busy finding security loopholes and innovative ways to expand their victim pool, in the usual cat-and-mouse game with defenders. As a result, we’ve seen new attack vectors and social engineering methods, new threats skyrocketing in our telemetry, and takedown operations leading to shake-ups of previously established ranks,” says ESET Director of Threat Detection Jiří Kropáč.

Among infostealers, notorious “infostealer-as-a-service” Redline Stealer was taken down by international authorities in October 2024. But it is expected that Redline Stealer’s demise will lead to the expansion of other similar threats. The ransomware landscape was reshaped by the takedown of former leader LockBit, creating a vacuum to be filled by other actors. RansomHub, a ransomware-as-a-service, stacked up hundreds of victims by the end of H2 2024, establishing itself as the new dominant player. China-aligned, North Korea-aligned, and Iran-aligned APT groups have been getting more involved in ransomware attacks.

With cryptocurrencies reaching record values in H2 2024, cryptocurrency wallet data was one of the prime targets of malicious actors. In our telemetry, this was reflected in a rise in cryptostealer detections across multiple platforms. The increase was the most dramatic on macOS, where so-called Password-Stealing Ware – heavily targeting cryptocurrency wallet credentials – more than doubled compared to H1. AMOS (also known as Atomic Stealer), malware designed to collect and exfiltrate sensitive data from Mac devices, was a significant contributor to this increase. Android financial threats, targeting banking apps as well as cryptocurrency wallets, grew by 20%.

For more information, check out the ESET Threat Report H2 2024 on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) 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 known and emerging cyberthreats — 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. An 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 us on LinkedIn, Facebook, and X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
