ESET Threat Report: Infostealers using AI & banking malware creating deepfake videos to steal money

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 4, 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 December 2023 through May 2024. These past six months painted a dynamic landscape of Android financial threats, malware going after victims' mobile banking funds – be they in the form of "traditional" banking malware or, more recently, cryptostealers. Infostealing malware can now be found impersonating generative AI tools, and new mobile malware GoldPickaxe is capable of stealing facial recognition data to create deepfake videos used by the malware's operators to authenticate fraudulent financial transactions. Video games and cheating tools used in online multiplayer games were recently found to contain infostealer malware such as the RedLine Stealer, which saw several detection spikes in H1 2024 in ESET telemetry.

"GoldPickaxe has both Android and iOS versions and has been targeting victims in Southeast Asia through localized malicious apps. As ESET researchers investigated this malware family, they discovered that an older Android sibling of GoldPickaxe, called GoldDiggerPlus, has also tunneled its way to Latin America and South Africa by actively targeting victims in these regions," explains Jiří Kropáč, Director of ESET Threat Detection.

In recent months Infostealing malware also began to utilize the impersonation of generative AI tools. In H1 2024, Rilide Stealer was spotted misusing the names of generative AI assistants, such as OpenAI's Sora and Google's Gemini, to entice potential victims. In another malicious campaign, the Vidar infostealer was lurking behind a supposed Windows desktop app for AI image generator Midjourney – even though Midjourney's AI model is only accessible via Discord. Since 2023, ESET Research has increasingly seen cybercriminals abusing the AI theme – a trend that is expected to continue.

Gaming enthusiasts who ventured out of the official gaming ecosystem were attacked by infostealers, as some cracked video games and cheating tools used in online multiplayer games were recently found to contain infostealer malware such as Lumma Stealer and RedLine Stealer. RedLine Stealer saw several detection spikes in H1 2024 in ESET telemetry, caused by campaigns in Spain, Japan, and Germany. Its recent waves were so significant that RedLine Stealer detections in H1 2024 surpassed those from H2 2023 by a third.

Balada Injector, a gang notorious for exploiting WordPress plug-in vulnerabilities, continued to run rampant in the first half of 2024, compromising over 20,000 websites and racking up over 400,000 hits in ESET telemetry for the variants used in the gang's recent campaign. On the ransomware scene, former leading player LockBit was knocked off its pedestal by Operation Chronos, a global disruption conducted by law enforcement in February 2024. Although ESET telemetry recorded two notable LockBit campaigns in H1 2024, these were found to be the result of non-LockBit gangs using the leaked LockBit builder.

The ESET Threat Report features news about recently released deep-dive investigation into one of the most advanced server-side malware campaigns, which is still growing – Ebury group, with their malware and botnet. Over the years, Ebury has been deployed as a backdoor to compromise almost 400,000 Linux, FreeBSD, and OpenBSD servers; more than 100,000 were still compromised as of late 2023.

For more information, check out the ESET Threat Report H1 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