ESET, spol. s r. o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
fax: +421 (2) 322 44 109, www.eset.com

Digital Security
Progress. Protected.

GLOBAL PRESS RELEASE
CATEGORY 1 – GLOBAL
EMBARGOED UNTIL JUNE 27, 2024
Bratislava – Slovakia, JUNE 27, 2024; 11:30 CEST

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

- ESET has released its latest Threat Report, which summarizes threat landscape trends seen in ESET telemetry and from the perspective of ESET experts, from December 2023 through May 2024.
- Infostealers started to impersonate generative AI tools such as Midjourney, Sora, and Gemini.
- New mobile malware GoldPickaxe is capable of stealing facial recognition data to create deepfake videos.
- RedLine Stealer saw several detection spikes in ESET H1 2024 telemetry, caused by campaigns in Spain, Japan and Germany.
- Balada Injector, a gang notorious for exploiting WordPress plugin vulnerabilities, continued to run rampant in the first half of 2024, compromising over 20,000 websites as ESET telemetry detected 400,000 hits.

BRATISLAVA — June 27, 2024 — 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, while the 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.

ESET, spol. s r. o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
fax: +421 (2) 322 44 109, www.eset.com

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 that 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 plugin 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

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.