EINPRESSWIRE

The remarkable adaptability of cybercriminals, the comeback of sextortion scams, and a rise in deceptive loan apps

Threat Report

H1 2023

December 2022 - May 2023

(eset):research

eset Digital Security Progress. Protected.

DUBAI, UNITED ARAB EMIRATES, July 12, 2023 /EINPresswire.com/ -- ESET has released its latest Threat Report, which summarizes threat landscape trends seen in ESET telemetry from December 2022 through May 2023. In H1 2023, we observed developments highlighting cybercriminals' remarkable adaptability and pursuit of new avenues of attack: exploiting vulnerabilities, gaining unauthorized access, compromising sensitive information, and defrauding individuals. One of the reasons for shifts in attack patterns is stricter security policies introduced by Microsoft, particularly on opening macro-enabled files. ESET telemetry data also suggests that operators of the once-notorious Emotet botnet have struggled to adapt to the shrinking attack surface, possibly indicating that a different group acquired the botnet. In the ransomware arena, actors increasingly reused previously leaked source code to build new ransomware variants. During the first half of 2023, sextortion email scams made a comeback, and ESET observed an alarming growth in the number of deceptive Android loan apps.

According to the report, in a new attempt to bypass Microsoft security measures, attackers substituted Office macros with weaponized OneNote files in H1 2023, leveraging the capability to embed scripts and files directly into OneNote. In response, Microsoft adjusted the default setup, prompting cybercriminals to continue exploring alternative intrusion vectors, with intensifying brute-force attacks against Microsoft SQL servers potentially representing one of the tested replacement approaches.

“Regarding the leaked source code of ransomware families such as Babyk, LockBit, and Conti, these allow amateurs to engage in ransomware activities, but at the same time enable us as defenders to cover a broader range of variants with a more generic or well-known set of detections and rules,” says ESET Chief Research Officer Roman Kováč.

While cryptocurrency threats have been steadily declining in ESET telemetry – not even being resurrected by the recent increase in bitcoin's value – cryptocurrency-related cybercriminal activities continue to persist, with cryptomining and cryptostealing capabilities being increasingly incorporated into more versatile malware strains. This evolution follows a pattern observed in the past, such as when keylogger malware was initially identified as a separate threat, but eventually became a common capability of many malware families.

Looking at other threats focused on financial gain, ESET researchers observed the comeback of so-called sextortion scam emails, exploiting people’s fears related to their online activities, and an alarming growth in deceptive Android loan apps masquerading as legitimate personal loan services and taking advantage of vulnerable individuals with urgent financial needs.

For more information, check out the ESET Threat Report H1 2023 on WeLiveSecurity. Make sure to follow ESET Research on Twitter 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.

Sanjeev Kant
Vistar Communications
+971559724623 ext.
email us here