EINPRESSWIRE

Iran-aligned Agrius group deploys new wiper through supply-chain attack in diamond industry, ESET Research discovers

DUBAI, UNITED ARAB EMIRATES, December 15, 2022 / EINPresswire.com/ -- ESET researchers discovered a new wiper and its execution tool, both attributed to the Iran-aligned Agrius APT group. The malware operators conducted a supply-chain attack abusing an Israeli software developer to deploy their new wiper, Fantasy, and a new lateral movement and Fantasy execution tool, Sandals. The abused Israeli software suite is used in the diamond industry, and in February 2022, Agrius began targeting an Israeli HR firm, a diamond wholesaler, and an IT consulting firm. The group is known for its destructive activities. Victims were observed in South Africa and Hong Kong as well.

“The campaign lasted less than three hours, and within that timeframe, ESET customers were already protected with detections identifying Fantasy as a wiper and blocking its execution. We observed the software developer pushing out clean updates within a matter of hours of the attack,” says Adam Burgher, ESET Senior Threat Intelligence Analyst. ESET contacted the software developer to notify them about a potential compromise, but the inquiries went unanswered.

“On February 20, 2022, at an organization in the diamond industry in South Africa, Agrius deployed credential harvesting tools, probably in preparation for this campaign. Then, on March 12, 2022, Agrius launched the wiping attack by deploying Fantasy and Sandals, first to the victim in South Africa, then to victims in Israel, and lastly to a victim in Hong Kong,” elaborates Burgher.

Fantasy wiper either wipes all files on disk or wipes all files with extensions on a list of 682 extensions, including filename extensions for Microsoft 365 applications such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel, and for common video, audio, and image file formats. Even though the malware takes steps to make recovery and forensic analysis more difficult, it is likely that recovery of the Windows operating system drive is possible. Victims were observed to be back up and running within a matter of hours.

Agrius is a newer Iran-aligned group targeting victims in Israel and the United Arab Emirates since 2020. The group initially deployed a wiper, Apostle, disguised as ransomware, but later modified Apostle into fully fledged ransomware. Agrius exploits known vulnerabilities in internet-facing applications to install webshells, then conducts internal reconnaissance before moving laterally and then deploying its malicious payloads.

Since its discovery in 2021, Agrius has focused solely on destructive operations. Fantasy is similar in many respects to the previous Agrius wiper, Apostle. However, Fantasy makes no effort to disguise itself as ransomware. There are only a few small tweaks between many of the original functions in Apostle and the Fantasy implementation.

For more technical information about Agrius's Fantasy wiper, check out the blogpost "Fantasy – a new Agrius wiper deployed through a supply-chain attack" 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
+971 55 972 4623
email us here