ESET Research analyzes Spacecolon toolset, which spreads ransomware across the world and steals sensitive data

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 24, 2023 /EINPresswire.com/ -- ESET Research has released its analysis of Spacecolon, a small toolset used to deploy variants of Scarab ransomware to victims all over the world. It likely penetrates victim organizations through operators compromising vulnerable web servers or via brute forcing RDP credentials. Several Spacecolon builds contain many Turkish strings; therefore, ESET believes it is written by a Turkish-speaking developer. ESET was able to track the origins of Spacecolon back to at least May 2020, and its campaigns are ongoing. ESET named Spacecolon's operators CosmicBeetle to represent the link to "space" and "scarab."

Spacecolon incidents identified by ESET telemetry encompass the globe, with high prevalence in European Union countries, such as Spain, France, Belgium, Poland, and Hungary; elsewhere, ESET has detected high prevalence in Turkey and Mexico. CosmicBeetle appears to be preparing the distribution of new ransomware — ScRansom. Post-compromise, along with installing ransomware, Spacecolon offers a large variety of third-party tools that allow the attackers to disable security products, extract sensitive information, and gain further access.

"We have not observed any pattern to Spacecolon's victims besides them being vulnerable to the initial access methods employed by CosmicBeetle. Neither have we found any pattern among the targets' areas of focus or size. However, to name a few (by type and geography), we have observed Spacecolon at a hospital and tourist resort in Thailand, an insurance company in Israel, a local governmental institution in Poland, an entertainment provider in Brazil, an environmental company in Turkey, and a school in Mexico," says ESET researcher Jakub Souček, author of the analysis.

CosmicBeetle probably compromises web servers vulnerable to the ZeroLogon vulnerability or

those with RDP credentials that it is able to brute force. Additionally, Spacecolon can provide backdoor access for its operators. CosmicBeetle doesn't make any considerable effort to hide its malware and leaves plenty of artifacts on compromised systems.

After CosmicBeetle compromises a vulnerable web server, it deploys ScHackTool, the main Spacecolon component that CosmicBeetle uses. It relies heavily on its GUI and active participation of its operators; it allows them to orchestrate the attack, downloading and executing additional tools to the compromised machine on demand as they see fit. If the target is deemed valuable, CosmicBeetle can deploy ScInstaller and use it, e.g., to install ScService, which provides further remote access.

The final payload CosmicBeetle deploys is a variant of the Scarab ransomware. This variant internally deploys a ClipBanker, a type of malware that monitors the content of the clipboard and changes content that it deems likely to be a cryptocurrency wallet address to an attacker-controlled address.

Furthermore, a new ransomware family is being developed, with samples being uploaded to VirusTotal from Turkey. ESET Research believes with high confidence that it is written by the same developers as Spacecolon, and ESET has named it ScRansom. ScRansom attempts to encrypt all hard, removable, and remote drives. ESET has not observed this ransomware being deployed in the wild, and it appears to still be in a development stage.

For more technical information about Spacecolon and CosmicBeetle, check out the blogpost "Scarabs colon-izing vulnerable servers" 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
email us here

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.