EINPRESSWIRE

ESET Research: CosmicBeetle group joins forces with other ransomware gangs, targets businesses in Europe and Asia

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 25, 2024 /EINPresswire.com/ -- ESET researchers have mapped the recent activities of the CosmicBeetle threat group, documenting its new ScRansom ransomware being deployed and discovering connections to other well-established ransomware gangs. CosmicBeetle has been spreading ransomware to small and medium businesses (SMBs), mainly in Europe and Asia. ESET Research has observed the threat actor using the leaked LockBit builder and trying to leverage LockBit's ransomware reputation. Besides LockBit, ESET believes that CosmicBeetle is probably a new affiliate of ransomware-as-a-service actor RansomHub, a new ransomware gang active since March 2024 with rapidly increasing activity.

“Probably due to the obstacles that writing custom ransomware from scratch brings, CosmicBeetle attempted to leech off LockBit's reputation, possibly to mask the issues in the underlying ransomware and in turn to increase the chance that victims would pay,” says ESET researcher Jakub Souček, who analyzed the latest activity of CosmicBeetle. “Additionally, recently, we observed the deployment of ScRansom and RansomHub payloads on the same machine only a week apart. This execution of RansomHub was very unusual compared to the typical cases we have seen in ESET telemetry, but quite similar to CosmicBeetle's modus operandi. Since there are no public leaks of RansomHub, this leads us to believe with medium confidence that CosmicBeetle may be a recent affiliate of theirs,” adds Souček.

CosmicBeetle often uses brute-force methods to breach its targets. Besides that, it misuses various known vulnerabilities. Small and medium-sized businesses from all sorts of verticals all over the world are the most common victims of this threat actor because that is the segment most likely to use the affected software, or lack robust patch management processes in place. ESET Research has observed attacks on SMBs in the following verticals: manufacturing, pharmaceuticals, legal, education, healthcare, technology, hospitality leisure, financial services, and regional government.

Besides encrypting, ScRansom can also kill various processes and services on the affected machine. ScRansom is not a very sophisticated piece of ransomware, though CosmicBeetle has been able to compromise interesting targets and cause great harm to them. This is mostly because CosmicBeetle is an immature actor in the ransomware world, and problems plague the deployment of ScRansom. Victims affected by ScRansom, who decide to pay, should be cautious.

ESET Research was able to obtain a decryptor implemented by CosmicBeetle for its recent encryption scheme. ScRansom is undergoing constant development, which is never a good sign for ransomware. The overcomplexity of the encryption (and decryption) process is prone to errors, making restoration of all files doubtful. Successful decryption relies on the decryptor working properly and on CosmicBeetle providing all the necessary keys, and even in that case, some files may be destroyed permanently by the threat actor. Even in the best-case scenario, decryption is long and complicated.

CosmicBeetle, active since at least 2020, is the name ESET researchers assigned to a threat actor discovered in 2023. This threat actor is most known for the usage of its custom collection of Delphi tools, commonly called Spacecolon, consisting of ScHackTool, ScInstaller, ScService, and ScPatcher.

For more technical information about the latest activity of CosmicBeetle, check out the blogpost "CosmicBeetle steps up: Probation period at RansomHub" 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