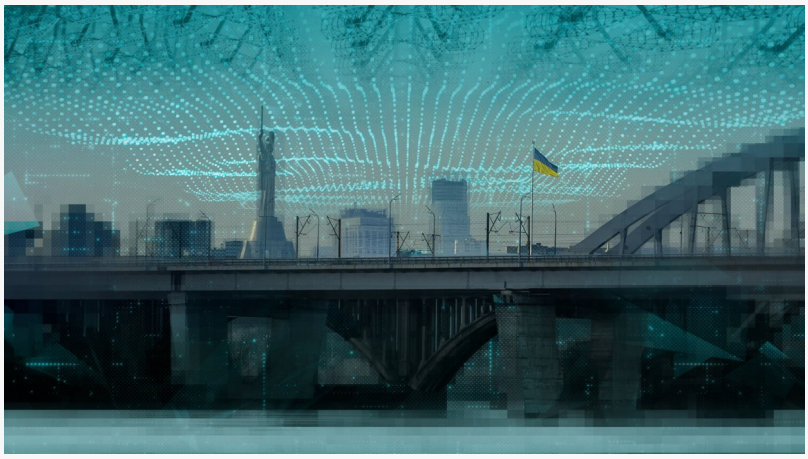
ESET Research investigates Gamaredon APT group: Cyberespionage aimed at high-profile targets in Ukraine & NATO countries



DUBAI, DUBAI, UNITED ARAB EMIRATES, September 30, 2024 /EINPresswire.com/ -- ESET Research examined the operations of Gamaredon, a Russia-aligned APT group that has been active since at least 2013 and is currently the most engaged APT group in Ukraine. Gamaredon has been attributed by the Security Service of Ukraine (SSU) to the Russian 18th Center of Information Security of the FSB, operating out of occupied Crimea. ESET believes this group to be collaborating with another threat actor that ESET Research discovered and named InvisiMole. The majority of Gamaredon's cyberespionage attacks are directed against Ukrainian governmental institutions. However, in April 2022 and February 2023, ESET also saw a few attempts to compromise targets in several NATO countries, namely Bulgaria, Latvia, Lithuania, and Poland, but no successful breaches were observed.

Gamaredon is using ever-changing obfuscation tricks and numerous techniques used for bypassing domain-based blocking. These tactics pose a significant challenge to tracking efforts, as they make it harder for systems to automatically detect and block the group's tools. Nevertheless, during ESET's investigation, ESET researchers managed to identify and understand these tactics and kept track of Gamaredon's activities. The group has been methodically deploying its malicious tools against its targets since well before the 2022 invasion began. To compromise new victims, Gamaredon conducts spearphishing campaigns and then uses its custom malware to weaponize Word documents and USB drives accessible to the initial victim, expecting them to be shared with further potential victims.

During 2023, Gamaredon notably improved its cyberespionage capabilities, and developed several new tools in PowerShell, with a focus on stealing valuable data – from email clients, instant messaging applications such as Signal and Telegram, and web applications running inside internet browsers. However, PteroBleed, an infostealer ESET discovered in August 2023, also

focuses on stealing data related to a Ukrainian military system – and from the webmail service used by a Ukrainian governmental institution.

“Gamaredon, unlike most APT groups, does not try to be stealthy and remain hidden as long as possible by using novel techniques while conducting cyberespionage operations, but rather, the operators are reckless and do not mind being discovered by defenders during their activities. Even though they do not care so much about being noisy, they still put in a lot of effort to avoid being blocked by security products and try very hard to maintain access to compromised systems,” explains ESET researcher Zoltán Rusnák, who investigated Gamaredon.

“Typically, Gamaredon attempts to preserve its access by deploying multiple simple downloaders or backdoors simultaneously. The lack of sophistication of Gamaredon tools is compensated by frequent updates and the use of regularly changing obfuscation,” adds Rusnák. “Despite the relative simplicity of its tools, Gamaredon’s aggressive approach and persistence make it a significant threat. Given the ongoing war in the region, we expect Gamaredon to continue in its focus on Ukraine,” he concludes.

For a more detailed analysis and technical breakdown of Gamaredon’s tools and activities, check out the latest ESET Research white paper “Cyberespionage the Gamaredon way: Analysis of toolset used to spy on Ukraine in 2022 and 2023” 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