LOGPOINT

Warning about Russian threat actor Gamaredon

Feb 23, 2023 13:00 CET

Warning about Russian threat actor Gamaredon: How to stay protected ahead of invasion anniversary cyber threat

- **Ukrainian authorities have issued a warning that Russia could conduct large-scale cyberattacks on the anniversary of the invasion**
- **Logpoint has conducted research into the hacktivist group Gamaredon, which according to Ukrainian CERT, is actively renewing attack efforts shifting focus from destruction to espionage and information stealing**

COPENHAGEN, Denmark & BOSTON, February 23, 2023 – Russian

cyberattacks against Ukraine have nearly tripled during the last year, and now the Ukrainian Defense Minister, Oleksii Reznikov, expresses concern that Russia will renew its offensive to coincide with the anniversary of the all-out war. Ukraine's National Security and Defense Council has issued a warning that Russia could conduct a large-scale cyberattack as part of its renewed aggression.

Ukranian CERT has released reports stating that the Russian threat actor Gamaredon, also known as UAC-0010, Primitive Bear, BlueAlpha, ACTINIUM, and Trident Ursa, is actively renewing its attack efforts. Reportedly, the group operates from Sevastopol in Crimea and follows instructions from the FSB Center for Information Security in Moscow.

“Gamaredon has carried out several cyberattacks against Ukraine since it originated in June 2013, a few months before Russia forcibly annexed the Crimean Peninsula. We’ve recently seen significant spikes in their activities and the group remains the most active, intrusive, and pervasive APT,” says Doron Davidson, Logpoint VP Global Services. “We’re monitoring the situation closely to keep up with threat intelligence and defense techniques that can mitigate the risk of Gamaredon.”

Ukraine’s State Service of Special Communication and Information Protection states that Gamaredon focuses more on information stealing and espionage than destruction and increasingly uses GammaLoad and GammaSteal spyware. These malware variants are custom-made information-stealing implants that can exfiltrate files of specific extensions, steal user credentials, and take screenshots of the victim’s computer.

Logpoint’s investigation into GammaLoad and GammaSteal shows that the malware variants get delivered via spear-phishing emails from compromised government employees, including malicious HTML files, Office documents, and phishing websites to target devices. The malware is designed to attack all Windows, Linux, and Android operating systems.

“It’s always crucial to detect an attack before it takes root in the systems,” says Doron Davidson. “With Gamaredon and other APTs, it’s not enough to follow best practices. You need to have capabilities to efficiently detect threats based on known indicators of compromise, using active monitoring and incident response plans.”

Read Logpoint's report about Gamaredon hereand get an in-depth analysis of the threat actor's techniques, indicators of compromise, and insights about incident investigation and response.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and BCS technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98