Gamaredon remains major player in Ukrainian conflict

What Cisco Talos knows about this group, and how to defend against them

BACKGROUND

Gamaredon (aka Armageddon) is a Russian state-sponsored advanced persistent threat (APT), based on Cisco Talos’ intelligence, that primarily targets Ukrainian officials, organizations and other targets aligned with the Russian government’s strategic interests. Active since at least 2013, Gamaredon has predominantly focused on cyberespionage against Ukrainian entities responsible for the nation’s defense, diplomacy, and internal security, as well as non-governmental organizations. These activities have only escalated since Russia’s invasion of Ukrainian territory.

CAPABILITIES

• Gamaredon uses a massive number of domains that are continuously recycled across IP infrastructure, leveraging specific dynamic DNS providers, leading to an overall decreased level of operational security (opsec).

• Gamaredon has predominantly used aggressive spear-phishing campaigns to gain initial access to target environments, often trying to trick users into opening malicious attachments.

• Gamaredon actors have used the COVID-19 pandemic to entice victims into opening attachments as well as themes related to the Russia-Ukraine war.

• The group deploys a variety of customized and off-the-shelf tools and malware ranging from script-based malware to information-stealers and backdoors. Notable malware families include GammaLoad, GammaSteel, Giddome, PowerPunch, Pterodo, and QuietSieve.

• Gamaredon exfiltrates sensitive data to its C2 and attempts to spread to other endpoints and systems in the environment.

MOST RECENT ATTACK

• In September 2022, Cisco Talos identified a new, ongoing campaign attributed to Gamaredon infecting Ukrainian users with information-stealing malware.

• We discovered the use of a custom-made information stealer implant that can exfiltrate victim files of interest and deploy additional payloads as directed by the attackers.

• Gamaredon tried to infect victims by sending them malicious documents as email attachments purporting to contain information about Russia’s invasion of Ukraine.

OUTLOOK

• Gamaredon likely will continue to conduct cyberespionage operations in support of Moscow’s political and national security objectives, primarily against Ukraine.

• These motivations and targets may change over time as Russian interests evolve.

COVERAGE

• Cisco Secure Endpoint and Snort deploy coverage into users’ environments, blocking Gamaredon’s ability to exploit certain vulnerabilities or download their notable tools.

• Cisco Talos Incident Response (CTIR) can assist customers in preparing for an attack and discovering any potential points of entry.

• Cisco Secure Firewall and Secure Network Analytics detect any changes in our customers’ network and monitor both outbound and inbound traffic patterns that may point to a malware infection.