Gamaredon APT Improves Toolset to Target Ukraine Government, Military

By Tara Seals

Published: 2020-02-05 · Archived: 2026-04-05 23:37:35 UTC

Research have been tracking an uptick in Gamaredon cyberattacks on Ukrainian military and security institutions that started in December.

The Gamaredon advanced persistent threat (APT) group has been supercharging its operations lately, improving its toolset and ramping up attacks on Ukrainian national security targets.

Vitali Kremez, head of SentinelLabs, said in research released on Wednesday that he has been tracking an uptick in Gamaredon cyberattacks on Ukrainian military and security institutions that started in December. He said that these include digital attacks on physical infrastructure and field hardware, including artillery – along with more expected cyber-espionage activity. One of the latter campaigns was a series of reconnaissance actions against the Hetman Petro Sahaidachnyi National Ground Forces Academy, in the Ukraine; and, spyware implants were spotted in a range of Ukrainian governmental targets.

“Based on SentinelLabs visibility into some of the affected victims, APT Gamaredon affected a large disposition of victim across Ukrainian separatist line with more than five thousand unique Ukrainian entities affected for the past months,” Kremez wrote.

In examining the campaign, SentinelLabs found that Gamaredon has improved its toolset. The latest malware implant appears to be a modified version of the group’s proprietary Pterodo malware, discovered on computers of state authorities of Ukraine performing system reconnaissance.

“This virus collects system data, regularly sends it to command-control servers and expects further commands,” Kremez wrote. “Packaged as self-extracting zip-archive (.SFX), the Gamaredon malware implant components contain a batch script, a binary processor .NET component and macro payloads.”

Notably, the implant boasts the addition of a .NET framework interop integrator known as Microsoft.Vbe.Interop.

“The newer tool [carries out] updated execution via an obfuscated .NET application of Excel and Word macros,” wrote Kremez. He added that the macro payload execution approach uses a specific processor that leverages scripting persistence. “The macro execution security registry [allows] macro execution and disabling Visual Basic for Applications (VBA) warnings,” he said. “[This] malware Interop component [also] uses fake Microsoft digital certificates belonging to Microsoft Time-Stamp Service.”

In addition, the group is also now using a system of Nginx forwarders to process traffic from compromised victim machines, oftentimes relying on dynamic DNS providers, according to the analysis.

Gamaredon, which Kremez said is linked to the Russian military, has ramped up its malware capabilities while exclusively targeting the Ukrainian national security institutions.

“Gamaredon has introduced new tools into its arsenal that significantly up its offensive capabilities,” he noted. “Their operations have impacted more than five thousand unique Ukrainian entities in the past few months.” He added, “This ability to efficiently integrate cyber-offense measures into the actual battlefield of a traditional or asymmetric warfare model has been for years tested in the long-term military conflict unfolding in Eastern Ukraine since 2014.”
