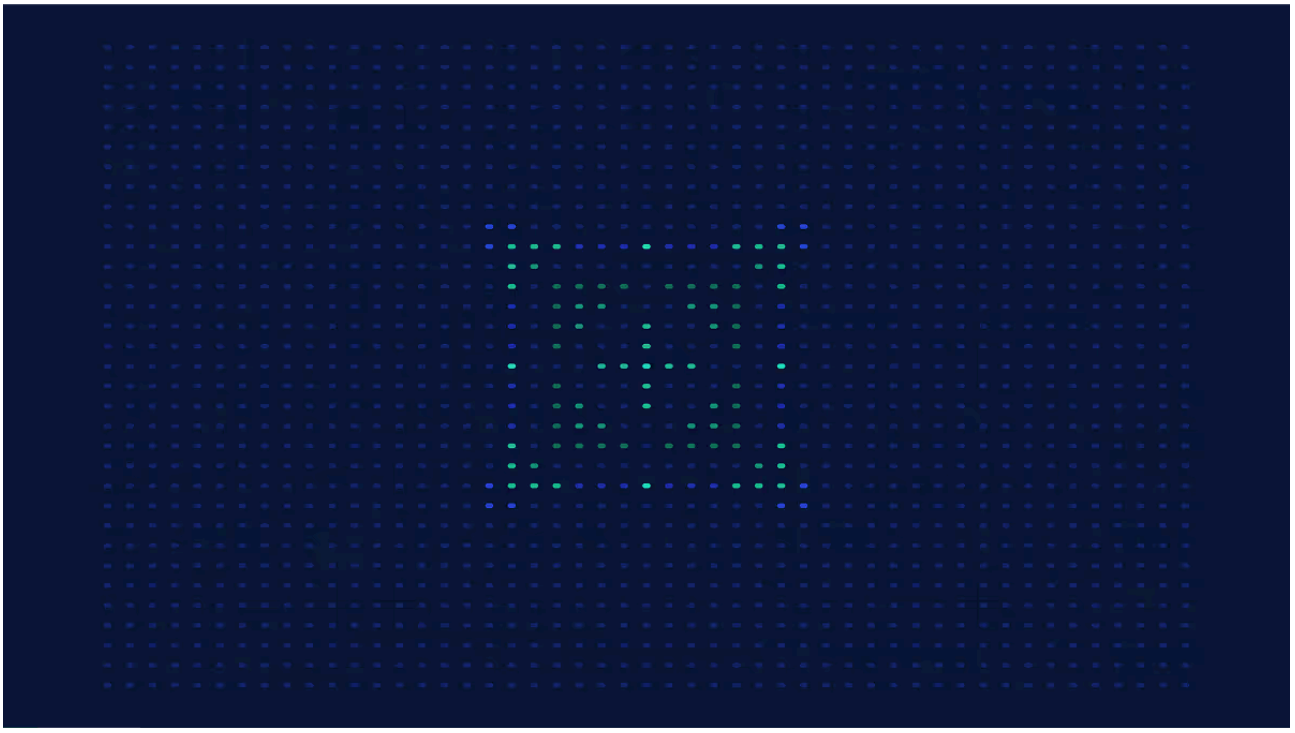
Malicious Activity Aligning with Gamaredon TTPs Targets Ukraine

By Anomali Threat Research

Published: 2025-12-31 · Archived: 2026-04-05 20:04:02 UTC

The Anomali Threat Research (ATR) team has identified malicious activity that we believe is being conducted by the Russia-sponsored Advanced Persistent Threat (APT) group Gamaredon (Primitive Bear).



Overview

The Anomali Threat Research (ATR) team has identified malicious activity that we believe is being conducted by the Russia-sponsored Advanced Persistent Threat (APT) group Gamaredon (Primitive Bear). Some of the documents have been discussed by other researchers.[1] This Gamaredon campaign appears to have begun in mid-October 2019 and is ongoing as of November 25, 2019. Based on lure documents observed by ATR, we believe that at least the following Ukrainian entities and individuals may be targeted:

- Diplomats
- Government officials and employees

- Journalists
- Law enforcement
- Military officials and personnel
- Non-Governmental Organization (NGO)
- The Ministry of Foreign Affairs of Ukraine

ATR analysts have found Tactics, Techniques, and Procedures (TTPs) that align with known Gamaredon tactics, in addition to a new template-injection technique that has not previously been observed to be utilized by the group.

The object of this report is to highlight a new Gamaredon TTP and share IOCs to the security community for awareness and further analysis. Several lure documents will also be examined, as well as a technical analysis section that showcases the functionalities of the template injection.

Get the full report on Gamaredon (Primitive Bear) and read through our key findings here.

Endnotes

[1] Evgeny Ananin and Artern Semenchenko “The Gamaredon Group: A TTP Profile Analysis,” Fortinet Blog, accessed November 25, 2019, published August 21 2019, https://www.fortinet.com/blog/threat-research/gamaredon-group-ttp-profile-analysis.html; ZLAB-YOROI, “The Russian Shadow in Eastern Europe: Ukrainian MOD Campaign,” YOROI Blog, accessed November 25, 2019, published April, 24, 2019 https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-ukrainian-mod-campaign/; ZLAB-YOROI, “The Russian Shadow in Eastern Europe: A Month Later,” YORIO Blog, accessed November 25, 2019, published June 4, 2019, https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-a-month-later/.

Iran’s IRGC Names Western Tech Giants as “Legitimate Targets”: What CISOs Must Do Now

When 766 Systems Fall in 24 Hours: The Threats Bearing Down on State Government Networks

The Iran Cyber Threat Machine Isn’t Slowing Down — Here’s What CISOs Need to Know Now

---

Source: https://www.anomali.com/blog/malicious-activity-aligning-with-gamaredon-ttps-targets-ukraine#When:15:00:00Z