Ukraine CERT-UA warns of new attacks launched by Russia-linked Armageddon APT - Security Affairs

By Pierluigi Paganini

Published: 2022-05-15 · Archived: 2026-04-05 13:30:07 UTC

Ukraine Computer Emergency Response Team (CERT-UA) reported a phishing campaign conducted by Armageddon APT using GammaLoad.PS1_v2 malware.

Ukraine Computer Emergency Response Team (CERT-UA) reported a phishing campaign using messages with subject “On revenge in Kherson!” and containing the “Plan Kherson.htm” attachment.

The HTM-file will decode and create an archive named “Herson.rar”, which contains a file-shortcut named “Plan of approach and planting explosives on the objects of critical infrastructure of Kherson.lnk”.

Upon clicking on the link file, the HTA-file “precarious.xml” is loaded and executed leading to the creation and execution of files “desktop.txt” and “user.txt”.

In the last stage of the attack chain, the GammaLoad.PS1_v2 malware is downloaded and executed on the victim’s computer.

The government experts attributes the attack to the Russia-linked Armageddon APT (UAC-0010) (aka Gamaredon, Primitive Bear, Armageddon, Winterflounder, or Iron Tilden) which was involved in a long string of attacks against the local state organizations.

“As a result, the malicious program GammaLoad.PS1_v2 will be downloaded to the computer (the mechanism of taking a screenshot and sending it to the management server has been implemented).” reads the advisory published by CERT-UA. “The activity is carried out by the group UAC-0010 (Armageddon).”

The Ukrainian CERT shared the indicators of compromise (IoCs) for this campaign.

> **Please vote for Security Affairs as the best European Cybersecurity Blogger Awards 2022 – VOTE FOR YOUR WINNERS**
> **Vote for me in the sections “The Underdogs – Best Personal (non-commercial) Security Blog” and “The Tech Whizz – Best Technical Blog” and others of your choice.**
> **To nominate, please visit:** https://docs.google.com/forms/d/e/1FAIpQLSfxxrxICiMZ9QM9iiPuMQIC-IoM-NpQMOsFZnJXrBQRYJGCOw/viewform

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner=”9″]	[adrotate banner=”12″]

Pierluigi Paganini

(SecurityAffairs – hacking, CERT-UA)

[adrotate banner=”5″]

[adrotate banner=”13″]
