# Ukraine: Russian Armageddon phishing targets EU govt agencies

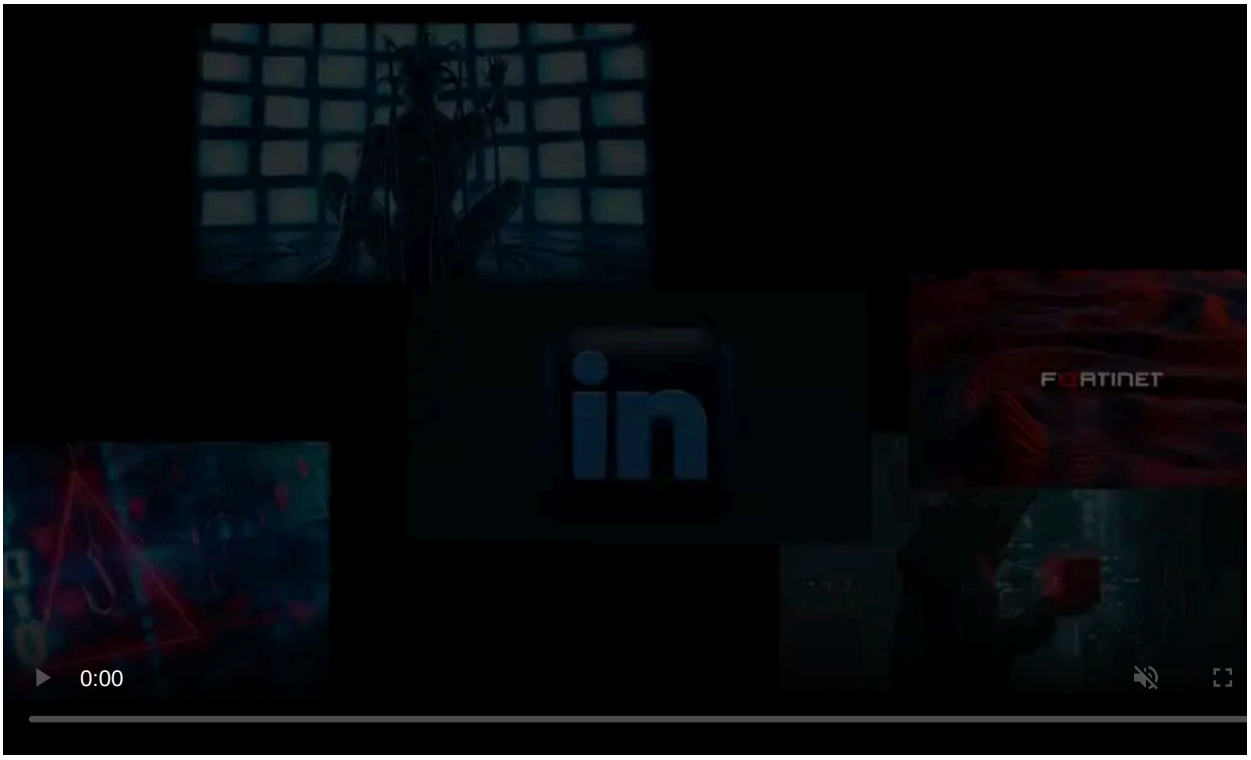
By Bill Toulas

Published: 2022-04-05 · Archived: 2026-04-05 20:02:05 UTC

The Computer Emergency Response Team of Ukraine (CERT-UA) has spotted new phishing attempts attributed to the Russian threat group tracked as Armageddon (Gamaredon).

The malicious emails attempt to trick the recipients with lures themed after the war in Ukraine and infect the target systems with espionage-focused malware.

CERT-UA has identified two separate cases, one targeting Ukrainian organizations and the other focusing on government agencies in the European Union.


0:00

## Who is Armageddon

Armageddon is a Russian state-sponsored threat actor who has been targeting Ukraine since at least 2014 and is considered part of the FSB (Russian Federal Security Service).

According to a detailed technical report published by the Ukrainian secret service in November 2021, Armageddon has launched at least 5,000 cyber-attacks against 1,500 critical entities in the country.

The Ukrainian forces have previously identified members of the Armageddon cyber-force, exposed their toolset, and traced custom malware development efforts to Russian hacking forums.

As such, even in chaotic wartime situations where cyber-response teams have limited resources and time, some attributions can be made with greater confidence due to the extensive identification efforts that took place in the past.

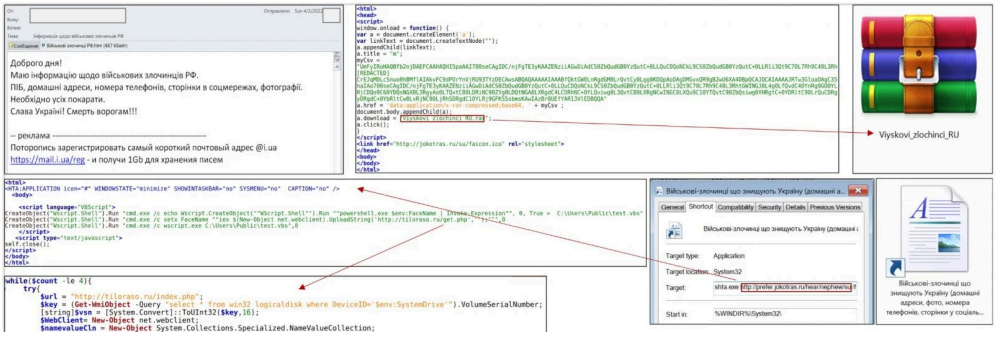
## Ukraine-focused campaign

Armageddon's Ukraine-targeting campaign distributes emails on "Information on war criminals of the Russian Federation," to various government agencies in the country.

The emails, sent from "vadim_melnik88@i[.]ua", contain an HTML attachment that CERT-UA says has low detections by security software at this time.

If opened, a RAR file is automatically created and dropped on the computer, supposedly containing the identification details of those responsible for war crimes in Ukraine in a shortcut file (.lnk).

However, clicking on this LNK file will download another HTA file laced with VBScript code that runs a PowerShell script to fetch the final payload.



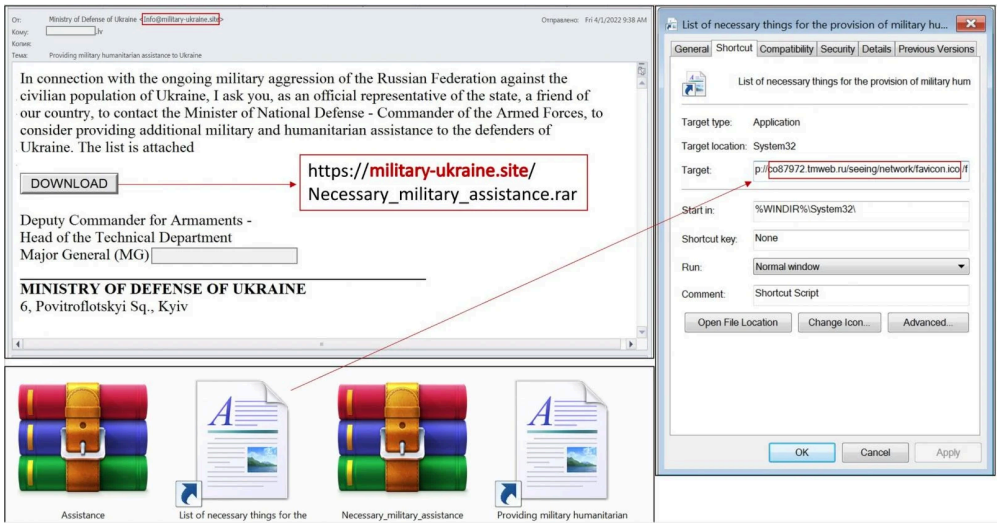

**Details of the Ukraine-targeting campaign** *(CERT-UA)*

## EU campaign

In the campaign targeting various EU government officials, Armageddon uses RAR archive attachments named "Assistance" and "Necessary_military_assistance".

Those archives contain shortcut files (.lnk) that supposedly include lists of things needed for military and humanitarian assistance to Ukraine. Opening that file triggers the same malware infection chain described in the previous section.

The sender's address is "info@military-ukraine[.]site", which may pass as legitimate, while the signee is supposedly the Deputy Commander for Armaments and Major General in Ukraine.




**Details of the EU phishing campaign** *(CERT-UA)*

The CERT-UA has confirmed at least one case of these emails reaching the inbox of the Latvian government. As such, the same campaign is likely targeting more European governments.

This report is in line with other recent findings of Russia-originating attacks targeting EU entities, like last week's Google TAG phishing campaign report, the deployment of wiper-malware against the KA-SAT satellite service, GPS system interference in the Baltic region, and phishing attacks against those aiding with the refugee crisis.

---