# CERT-UA attributed phishing efforts targeting Ukrainian and European government agencies to Russian espionage unit Gamaredon

5th April 2022

Orpheus severity score: 60

---

Ukraine's Computer Emergency Response Team (CERT-UA) has detected phishing efforts it has attributed to Russian espionage unit Gamaredon (also known as Armageddon, Primitive Bear, Shuckworm and ACTINIUM). The malicious activity targets government agencies in Ukraine and across the European Union.

Gamaredon has been active since at least 2013 and has consistently focused its espionage efforts against government officials and organisations in Ukraine. It is believed to operate under Russia's Federal Security Service (FSB).

The phishing emails sent to Ukrainian government agencies purport to share information on Russian war criminals. The messages distribute an HTML attachment that, if opened, creates and drops a RAR archive containing a LNK file with the details of Russian individuals responsible for committing war crimes in Ukraine. If clicked on, however, the LNK file downloads an additional HTA file laden with VBScript code that, in turn, executes PowerShell code that fetches a malware payload.

The phishing efforts directed against European government institutions feature the same malware infection chain but a different lure. Malicious messages carry RAR archives labelled "Assistance" and "Necessary_military_assistance", which contain LNK files listing items needed to provide military and humanitarian assistance to Ukraine. They originate from the address info@military-ukraine[.]site and the signature displayed reads Deputy Command for Armaments and Major General in Ukraine: two elements that contribute to the perceived legitimacy of the emails.

Russia routinely engages in cyber espionage against Ukraine and member states of the European Union and NATO to collect political and military intelligence and anticipate political, military and economic developments within the region. The country has become increasingly assertive in using cyber espionage and attack capabilities since it invaded Ukraine in February 2022.

This latest activity also aligns with other reported phishing efforts conducted following the invasion. On 11 March, CERT-UA warned about an ongoing phishing campaign impersonating Ukrainian government agencies. On March 30, it was reported that a Russian-based threat group tracked as COLDRIVER had launched phishing operations against the military apparatuses of multiple Eastern European countries and a NATO Centre of Excellence, amongst other targets in the US.

As the war progresses and further diplomatic actions are taken against Russia, we anticipate the country will continue to engage in similar phishing efforts, broadening its focus and victimology.

| | |
|---|---|
| **Threat Subcategory** | Russia |
| **Threat Actor** | Gamaredon |
| **Sectors** | Government |
| **Objective** | Political intelligence collection \| Military intelligence collection |
| **Countries & Target** | Latvia \| Russia \| Ukraine |
| **Infection Vectors** | Spear-phishing |
| **Source** | https://www.bleepingcomputer.com/news/security/ukraine-spots-russian-linked-armageddon-phishing-attacks/ |