Russian govt hackers hit Ukraine with Cobalt Strike, CredoMap malware

By Bill Toulas

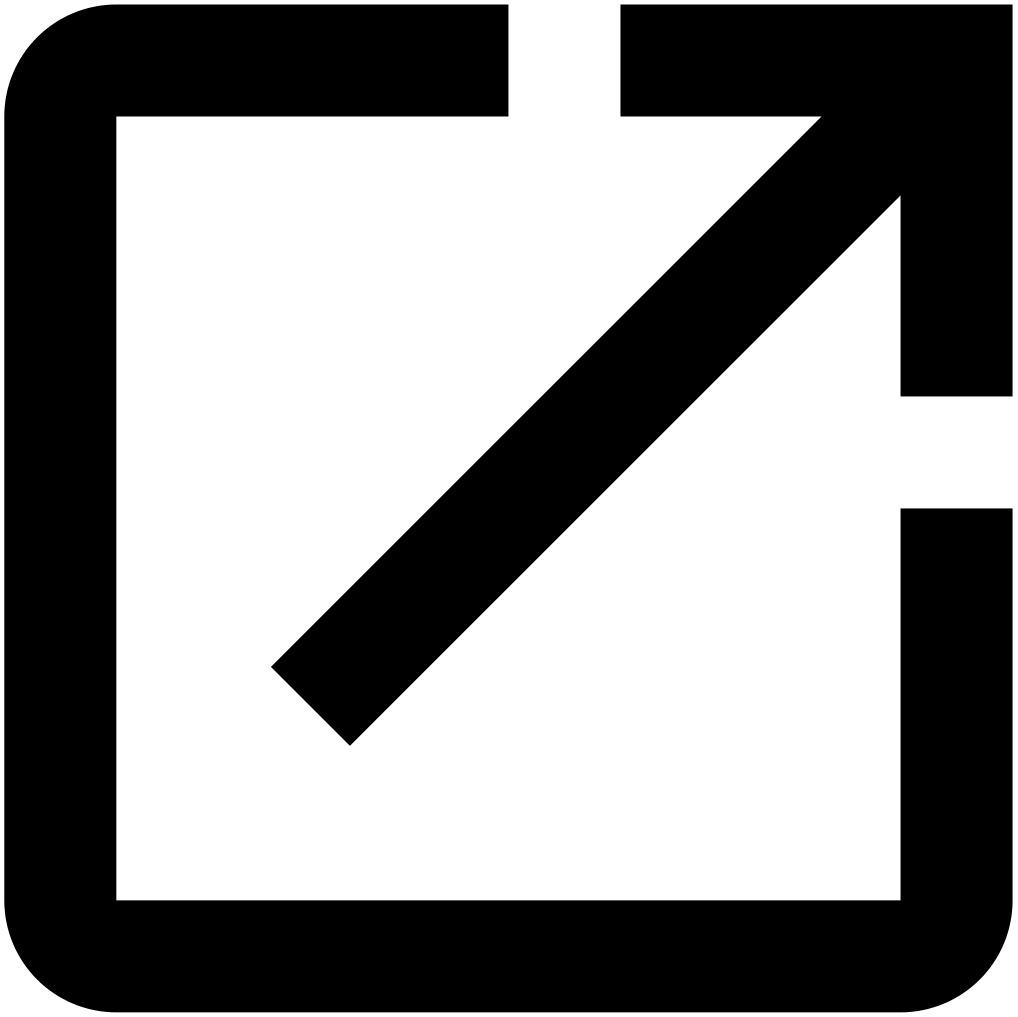
Published: 2022-06-21 · Archived: 2026-04-05 15:23:59 UTC

The Ukrainian Computer Emergency Response Team (CERT) is warning that Russian hacking groups are exploiting the Follina code execution vulnerability in new phishing campaigns to install the CredoMap malware and Cobalt Strike beacons.

The APT28 hacking group is believed to be sending emails containing a malicious document name "Nuclear Terrorism A Very Real Threat.rtf.". The threat actors selected the topic of this email to entice recipients to open it, exploiting the fear that's spread among Ukrainians about a potential nuclear attack.

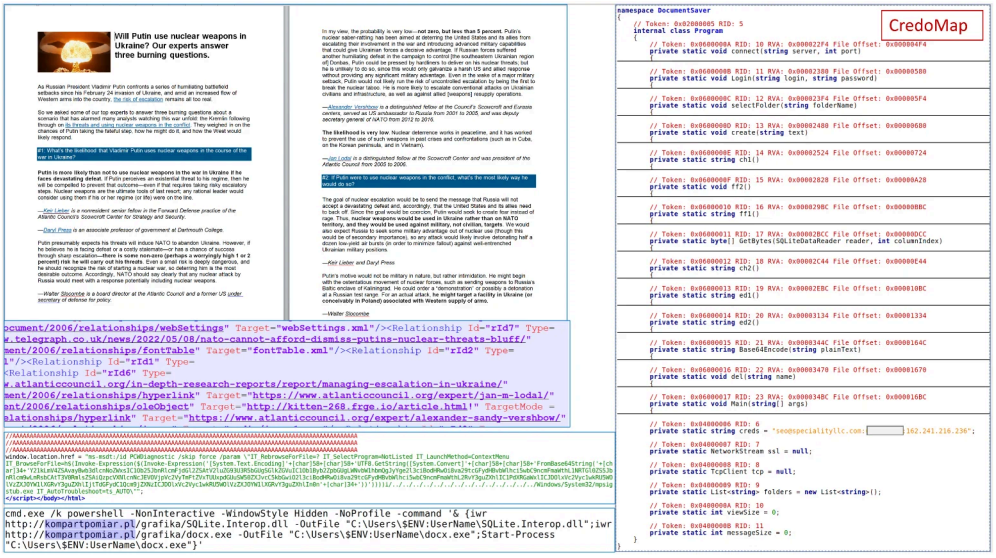
Threat actors also used a similar tactic in May 2022, when CERT-UA identified the dissemination of malicious documents warning about a chemical attack.


DIE LINKE.
0:00



Visit Advertiser website[GO TO PAGE]

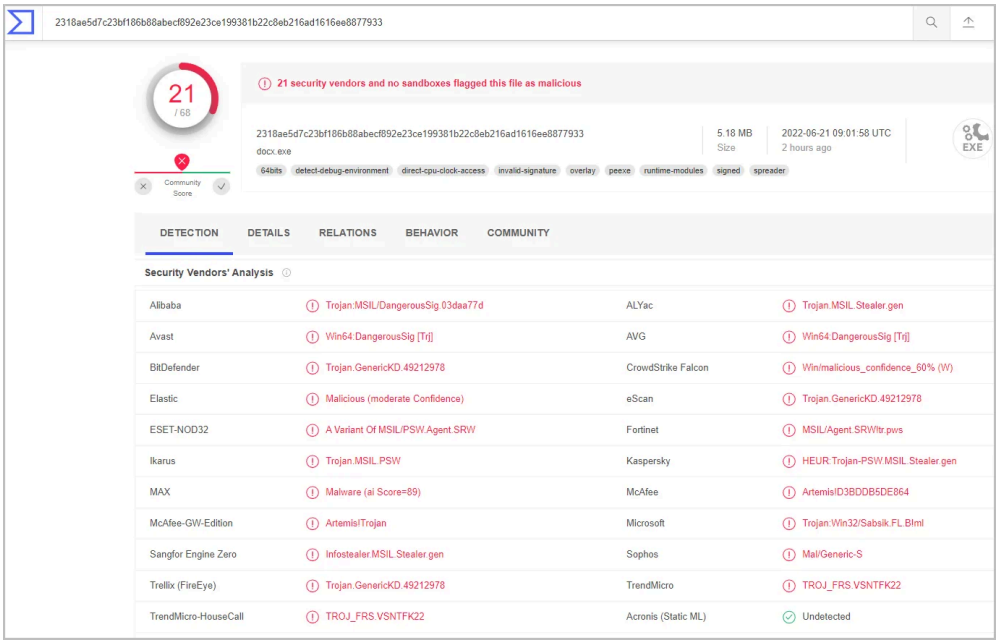
The RTF document used in the APT28 campaign attempts to exploit CVE-2022-30190, aka "Follina," to download and launch the CredoMap malware (docx.exe) on a target's device.



CredoMap infection process *(CERT-UA)*

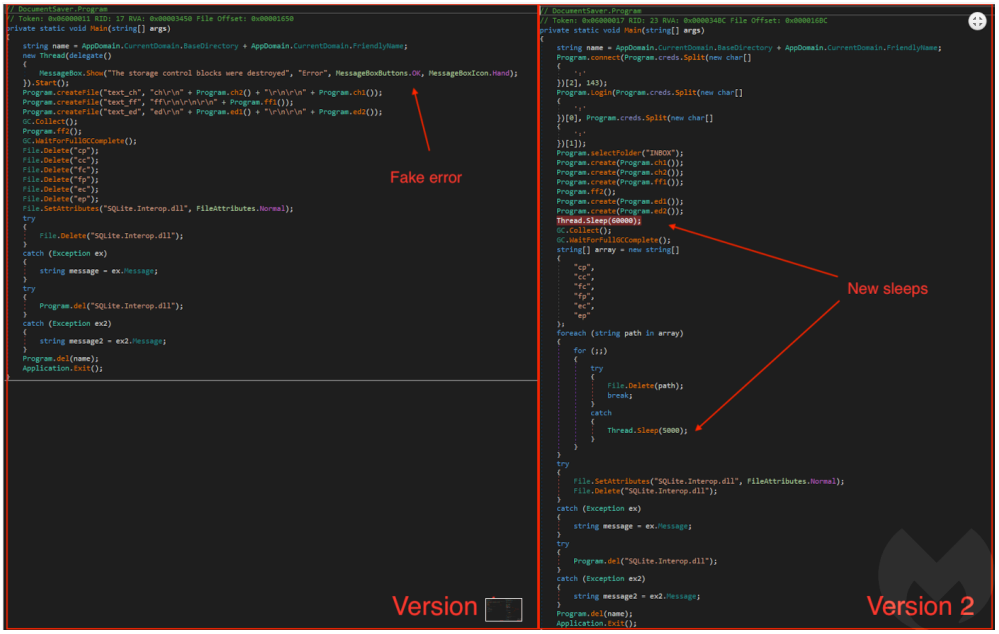
This vulnerability is a flaw in the Microsoft Diagnostic Tool, exploited in the wild since at least April 2022, triggering malicious downloads by simply opening a document file, or in the case of RTFs, merely [viewing it in the Windows preview pane].

CredoMap is an unknown malware strain detected by several AV engines on [Virus Total], with numerous vendors classifying it as a password-stealing Trojan.



Virus Total scan results for CredoMap

In an associated report published by [Malwarebytes] today, the security analysts clarify that the payload is an info-stealer that APT28 used against Ukrainian targets in May.



Malware featuring minor changes compared to the variant sampled in May *(Malwarebytes)*

The malware aims to steal information stored in Chrome, Edge, and Firefox web browsers, like account credentials and cookies.

Finally, the malware exfiltrates the stolen data using the IMAP email protocol, sending everything to the C2 address, which is hosted on an abandoned Dubai-based site.

According to cybersecurity researcher MalwareHunterteam, who discovered this campaign yesterday, the malware uses hard-coded IMAP credentials, potentially allowing any researcher to access the stolen data.

CERT-UA warned about CVE-2022-30190 exploitation by Russian hackers of the Sandworm group last week, but this time, the threat actors responsible for the attacks are identified as the APT28 group.

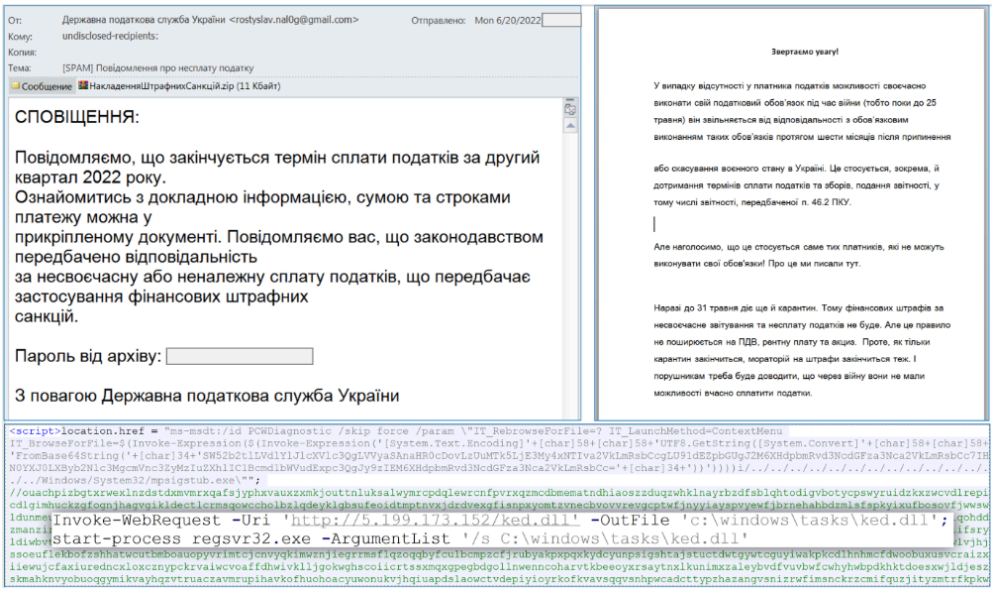
APT28 (aka STRONTIUM, Fancy Bear, and Sofacy) is a Russian hacking group focusing on cyber espionage and is believed to have ties to the Russian government.

The group has been active since 2007, targeting governments, military, and security organizations.

Cobalt Strike campaign also underway

In parallel to the above activity, the CERT-UA has also identified a different campaign by a threat actor tracked as UAC-0098, also using CVE-2022-30190 to infect the target with minimal interaction.

In this case, CERT-UA says the threat actor uses a DOCX file named "Imposition of penalties.docx", and the payload fetched from a remote resource is a Cobalt Strike beacon (ked.dll) with a recent compilation date.



Cobalt Strike campaign details *(CERT-UA)*

The sent emails supposedly come from the State Tax Service of Ukraine, with the subject: "Notice of non-payment of tax."

Since Ukraine is at war with Russia and many citizens have naturally neglected their regular tax-paying obligations towards the state, the lure might be effective against many people in this case.

CERT-UA advises employees in critical organizations to remain vigilant against email-delivered threats, as the number of spear-phishing attacks remains high.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
