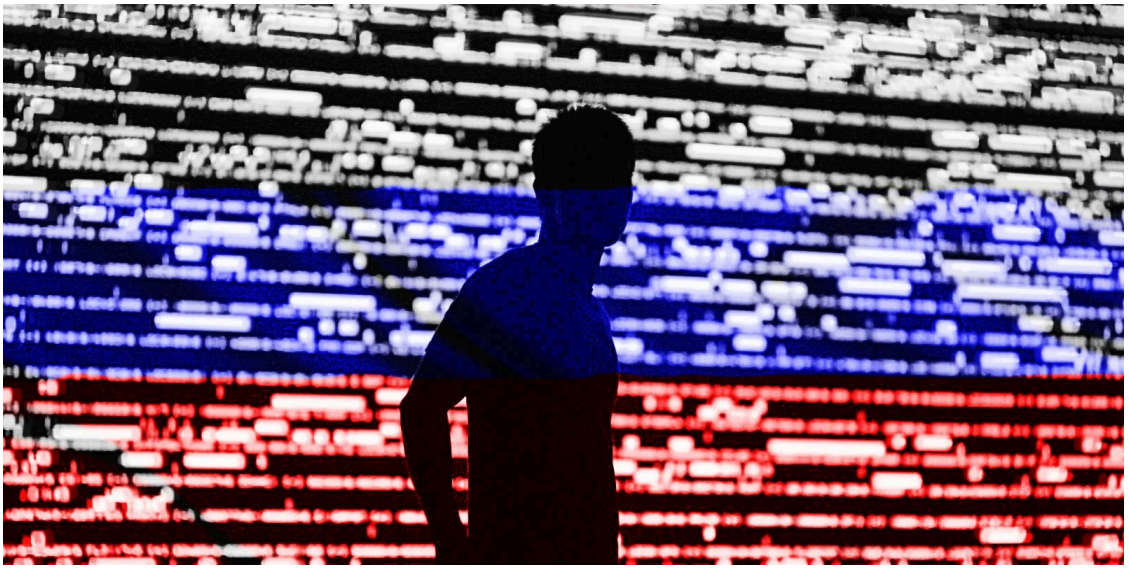
Russian hackers start targeting Ukraine with Follina exploits

By Bill Toulas

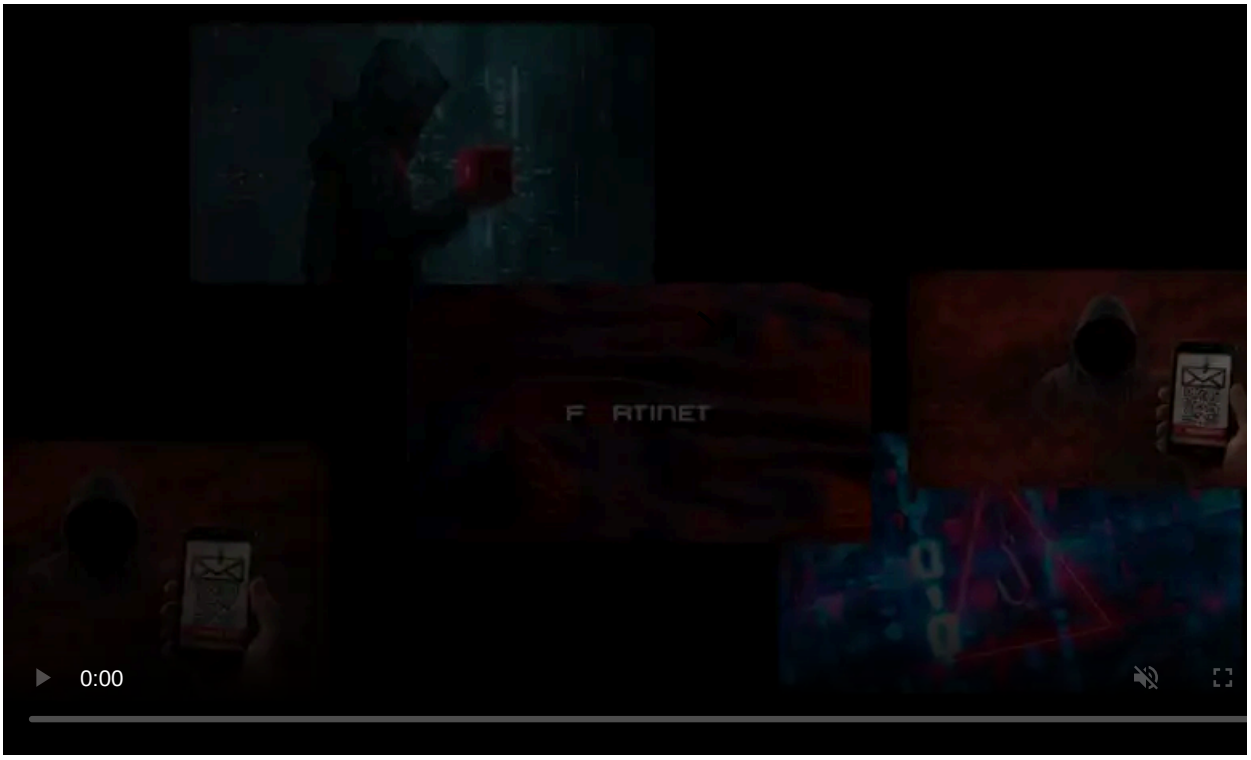
Published: 2022-06-13 · Archived: 2026-04-05 23:35:14 UTC

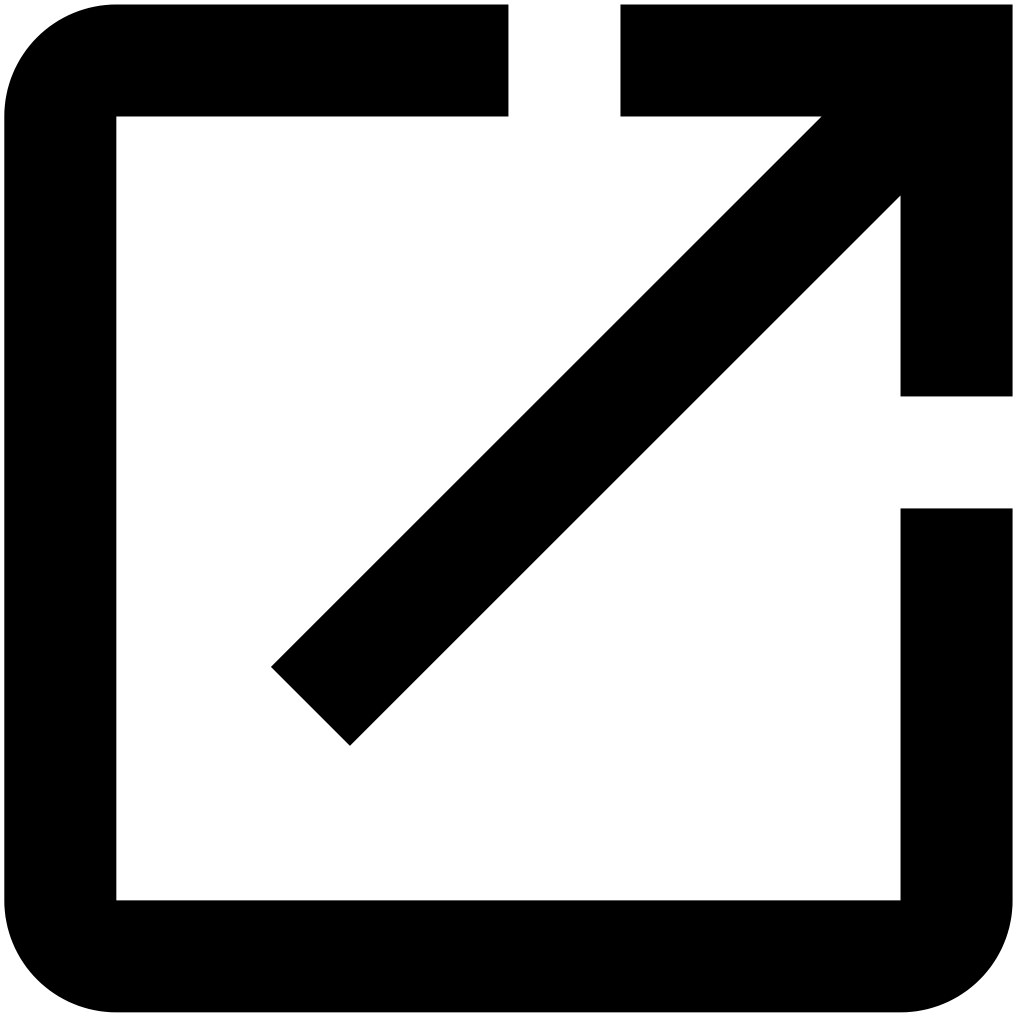


Ukraine's Computer Emergency Response Team (CERT) is warning that the Russian hacking group Sandworm may be exploiting Follina, a remote code execution vulnerability in Microsoft Windows Support Diagnostic Tool (MSDT) currently tracked as CVE-2022-30190.

The security issue can be triggered by either opening or selecting a specially crafted document and threat actors have been exploiting it in attacks since at least April 2022.

It is worth noting that Ukraine's agency assesses with medium confidence that behind the malicious activity is the Sandworm hacker group.

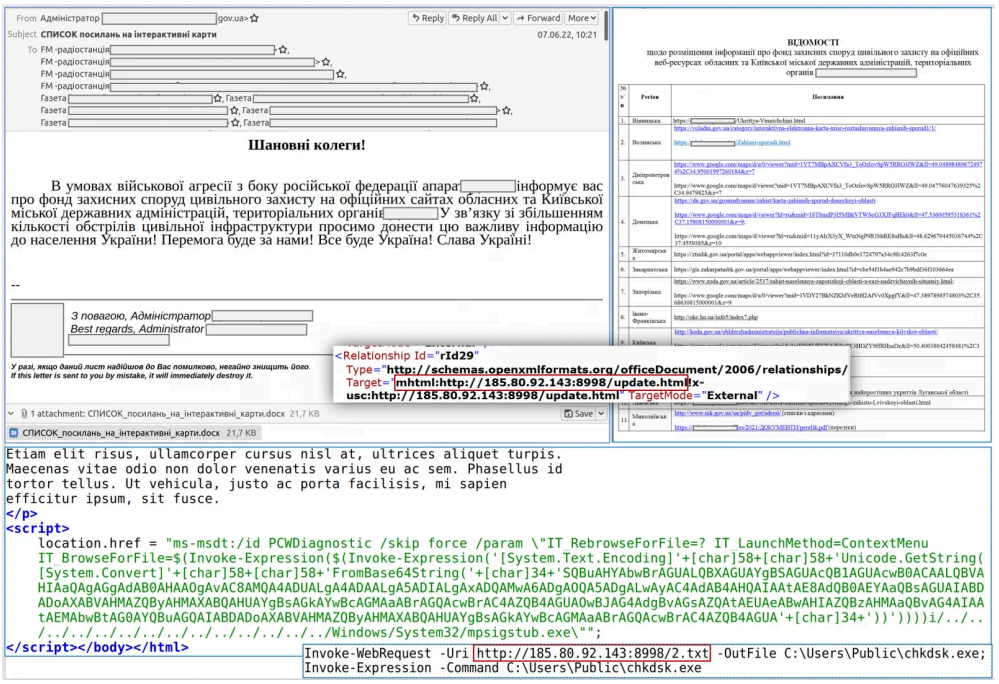

F RTINET
0:00



Targeting media orgs

CERT-UA says that Russian hackers launched a new malicious email campaign leveraging Follina and targeted more than 500 recipients at various media organizations in Ukraine, including radio stations and newspapers.

The emails have the subject “LIST of links to interactive maps”, and carry a .DOCX attachment with the same name. When opening the file, JavaScript code executes to fetch a payload named "2.txt," which CERT-UA classified as "malicious CrescentImp."



Infection chain dropping CrescentImp malware *(CERT-UA)*

CERT-UA has provided a short set of indicators of compromise to help defenders detect CrescentImp infections. However, it is unclear what type of malware family CrescentImp belongs to or its functionality.

The hashes from CERT-UA show no detection at the moment on the Virus Total scanning platform.

Sandworm activity in Ukraine

Sandworm has been targeting Ukraine constantly over the past few years, and the frequency of attacks increased after the Russian invasion into Ukraine.

In April, it was discovered that Sandworm attempted to take down a large Ukrainian energy provider by targeting its electrical substations with a new variant of the Industroyer malware.

In February, security researchers discovered that Sandworm was the group responsible for creating and operating the Cyclops Blink botnet, a highly persistent malware relying on firmware manipulation.

At the end of April, the U.S. set a reward of $10,000,000 for anyone who could help locate six individuals believed to be members of the notorious hacking group.

Source: https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/