Russian military hackers target Ukraine with new MASEPIE malware

By Bill Toulas

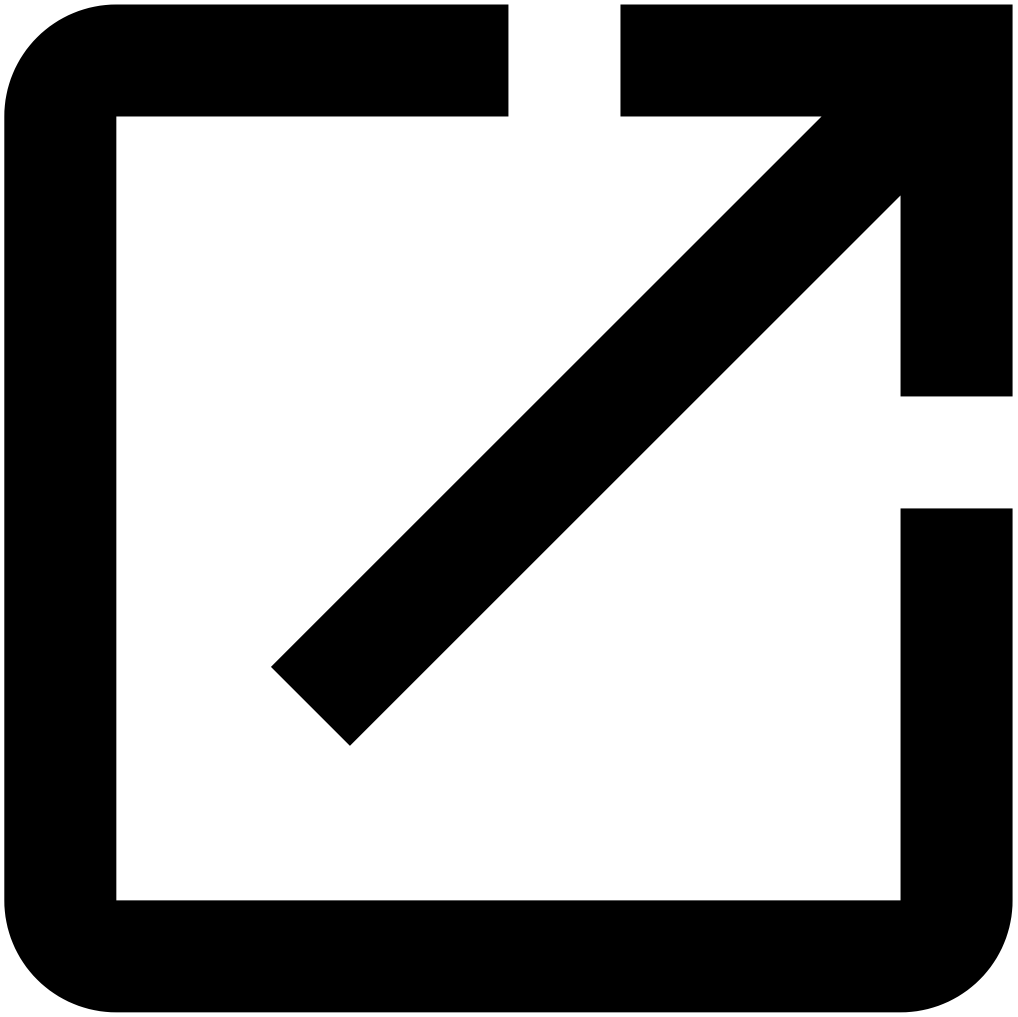
Published: 2023-12-28 · Archived: 2026-04-05 14:34:17 UTC

Ukraine's Computer Emergency Response Team (CERT) is warning of a new phishing campaign that allowed Russia-linked hackers to deploy previously unseen malware on a network in under one hour.

APT28, aka Fancy Bear or Strontium, is a Russian state-sponsored threat actor known for targeting government entities, businesses, universities, research institutes, and think tanks in Western countries and NATO orgs. The hacking group is known to employ phishing campaigns and exploit zero-day vulnerabilities in widely used software.

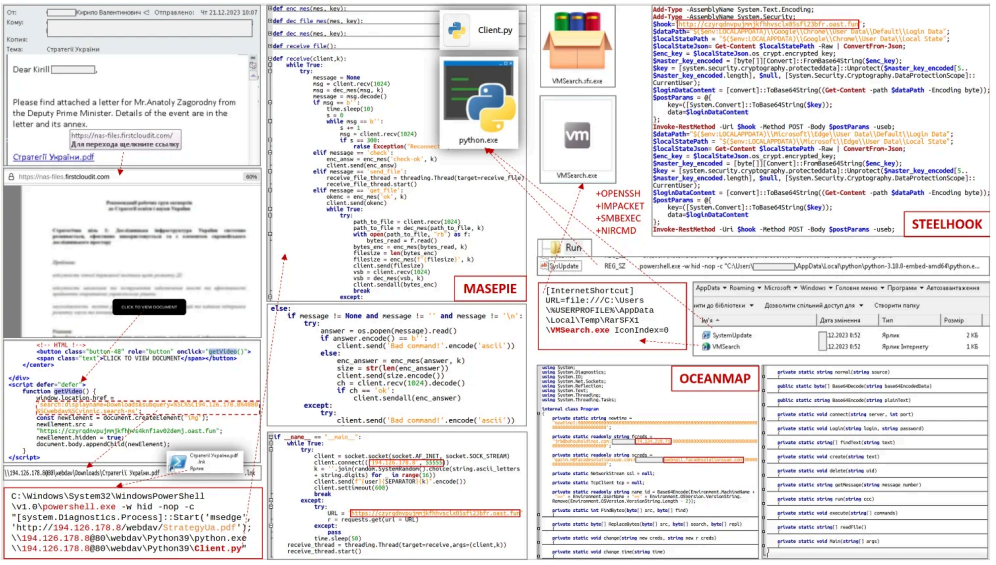
The latest campaign targeting Ukraine took place between December 15 and 25, 2023, utilizing phishing emails urging recipients to click on a link supposedly to view an important document.


DIE LINKE.
0:00



Visit Advertiser website[GO TO PAGE]

The links redirect victims to malicious web resources that employ JavaScript to drop a Windows shortcut file (LNK) that launches PowerShell commands to trigger an infection chain for a new Python malware downloader called 'MASEPIE.'



Attack diagram *(Ukraine CERT)*

MASEPIE establishes persistence on the infected device by modifying the Windows Registry and adding a deceptively named LNK file ('SystemUpdate.lnk') to the Windows Startup folder.

CERT-UA says the malware's primary role is to download additional malware on the infected device and steal data.

The Ukrainian CERT says APT28 also uses a set of PowerShell scripts named 'STEELHOOK' to steal data from Chrome-based web browsers, likely to extract sensitive information like passwords, authentication cookies, and browsing history.

Another tool used as part of the attack is the 'OCEANMAP,' a C# backdoor used primarily for executing base64-encoded commands via cmd.exe.

OCEANMAP establishes persistence on the system by creating a .URL file named 'VMSearch.url' in the Windows Startup folder.

OCEANMAP uses the Internet Message Access Protocol (IMAP) as a control channel to receive commands discreetly that are unlikely to raise alarms, storing them as email drafts containing the command, username, and OS version.

After executing the commands, OCEANMAP stores the results in the inbox directory, allowing APT28 to stealthily retrieve the outcomes and adjust their attack if needed.

Other tools deployed in the attacks for network reconnaissance and lateral movement include IMPACKET, a collection of Python classes for working with network protocols, and SMBEXEC, which enables remote command execution.

Ukraine's CERT says these tools are deployed in compromised systems within an hour from the initial compromise, indicating a rapid and well-coordinated attack.

Source: https://www.bleepingcomputer.com/news/security/russian-military-hackers-target-ukraine-with-new-masepie-malware/