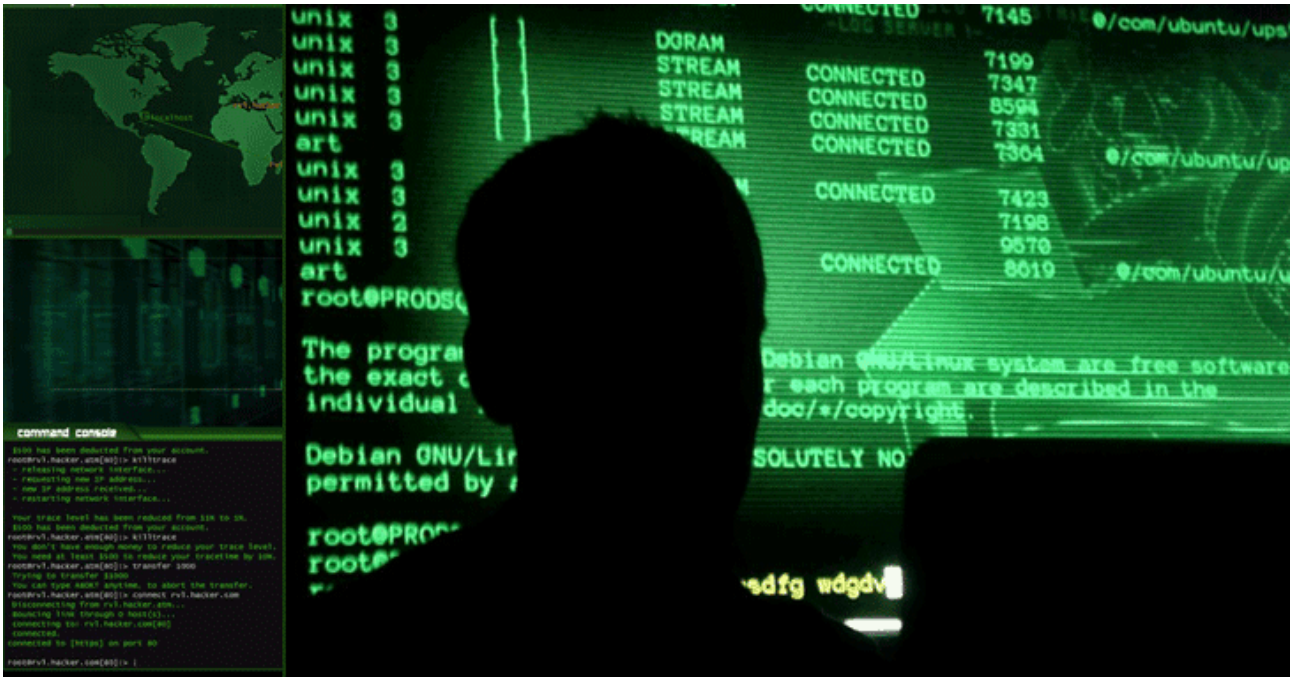
Hackers Exploited MSHTML Flaw to Spy on Government and Defense Targets

By The Hacker News

Published: 2022-01-25 · Archived: 2026-04-05 16:32:32 UTC



Cybersecurity researchers on Tuesday took the wraps off a multi-stage espionage campaign targeting high-ranking government officials overseeing national security policy and individuals in the defense industry in Western Asia.

The attack is unique as it leverages Microsoft OneDrive as a command-and-control (C2) server and is split into as many as six stages to stay as hidden as possible, Trellix — a new company created following the merger of security firms McAfee Enterprise and FireEye — said in a report shared with The Hacker News.

"This type of communication allows the malware to go unnoticed in the victims' systems since it will only connect to legitimate Microsoft domains and won't show any suspicious network traffic," Trellix explained.

First signs of activity associated with the covert operation are said to have commenced as early as June 18, 2021, with two victims reported on September 21 and 29, followed by 17 more in a short span of three days between October 6 and 8.

"The attack is particularly unique due to the prominence of its victims, the use of a recent [security flaw], and the use of an attack technique that the team had not seen before," Christiaan Beek, lead scientist at Trellix, said. "The objective was clearly espionage."

Trellix attributed the sophisticated attacks with moderate confidence to the Russia-based APT28 group, also tracked under the monikers Sofacy, Strontium, Fancy Bear, and Sednit, based on similarities in the source code as well as in the attack indicators and geopolitical objectives.

"We are supremely confident that we are dealing with a very skilled actor based on how infrastructure, malware coding and operation were set up," Trellix security researcher Marc Elias said.

The infection chain begins with the execution of a Microsoft Excel file containing an exploit for the MSHTML remote code execution vulnerability (CVE-2021-40444), which is used to run a malicious binary that acts as the downloader for a third-stage malware dubbed Graphite.

The DLL executable uses OneDrive as the C2 server via the Microsoft Graph API to retrieve additional stager malware that ultimately downloads and executes Empire, an open-source PowerShell-based post-exploitation framework widely abused by threat actors for follow-on activities.

"Using the Microsoft OneDrive as a command-and-control Server mechanism was a surprise, a novel way of quickly interacting with the infected machines by dragging the encrypted commands into the victim's folders," Beek explained. "Next OneDrive would sync with the victim's machines and encrypted commands being executed, whereafter the requested info was encrypted and sent back to the OneDrive of the attacker."

If anything, the development marks the continued exploitation of the MSTHML rendering engine flaw, with Microsoft and SafeBreach Labs disclosing multiple campaigns that have weaponized the vulnerability to plant malware and distribute custom Cobalt Strike Beacon loaders.

"The main takeaway is to highlight the level of access threat campaigns, and in particular how capable threat actors are able to permeate the most senior levels of government," Raj Samani, chief scientist and fellow at Trellix told The Hacker News. "It is of paramount importance that security practitioners tasked with protecting such high value systems consider additional security measures to prevent, detect and remediate against such hostile actions."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
