

[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)

> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)

> Microsoft blocks Polonium hackers from using OneDrive in attacks

Microsoft blocks Polonium hackers from using OneDrive in attacks

By
Sergiu Gatlan
(<https://www.bleepingcomputer.com/author/sergiu-gatlan/>)

June 2, 2022

01:36 PM

0



Microsoft said it blocked a Lebanon-based hacking group it tracks as Polonium from using the OneDrive cloud storage platform for data exfiltration and command and control while targeting and compromising Israeli organizations.



The company also suspended more than 20 malicious OneDrive applications used in Polonium's attacks, notifying the targeted organizations and quarantining the threat actors' tools via security intelligence updates.

Throughout the attacks that mainly targeted Israel's critical manufacturing, IT, and defense industry sectors since February 2022, Polonium operators have also likely coordinated their hacking attempts with multiple Iran-linked threat actors, according to Redmond's analysis.



"We also assess with moderate confidence that the observed activity was coordinated with other actors affiliated with Iran's Ministry of Intelligence and Security (MOIS), based primarily on victim overlap and commonality of tools and techniques," Microsoft said.





"Such collaboration or direction from Tehran would align with a string of revelations since late 2020 that the Government of Iran is using third parties to carry out cyber operations on their behalf, likely to enhance Iran's plausible deniability."

In some of the attacks, Microsoft has observed evidence pointing at MOIS operators possibly providing Polonium hackers with access to previously breached networks.

Polonium operators have also targeted multiple victims compromised by the MuddyWater APT group, tracked by Microsoft as Mercury, and linked to the Iranian Ministry of Intelligence and Security (<https://www.bleepingcomputer.com/news/security/us-links-muddywater-hacking-group-to-iranian-intelligence-agency/>) by US Cyber Command.

The threat actors have used several malware strains in their attacks, such as CreepyDrive and PowerShell-based CreepySnail implants for command and control and data theft.

Possible initial access via vulnerable Fortinet devices

Microsoft added that, for the vast majority of victims, the initial access vector seems to be unpatched Fortinet FortiOS SSL VPN devices vulnerable to CVE-2018-13379 exploits targeting a critical path traversal



flaw allowing login credentials theft.

This comes after a hacker leaked the credentials for almost 50,000 vulnerable Fortinet VPNs

(<https://www.bleepingcomputer.com/news/security/passwords-exposed-for-almost-50-000-vulnerable-fortinet-vpns/>) in November 2020, just a few days after a list of CVE-2018-13379 one-line exploits was shared online

(<https://www.bleepingcomputer.com/news/security/hacker-posts-exploits-for-over-49-000-vulnerable-fortinet-vpns/>).

Almost one year later, a list of nearly 500,000 Fortinet VPN credentials allegedly scraped from exploitable devices was again leaked online (<https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/>).

US, UK, and Australian cybersecurity agencies warned in November 2021 of several Fortinet vulnerabilities (including the CVE-2018-13379 path traversal) being actively exploited by an Iranian-backed hacking group.

"While we continue to pursue confirmation of how POLONIUM gained initial access to many of their victims, MSTIC notes that approximately 80% of the observed victims beaconing to graph.microsoft.com were running Fortinet appliances," Microsoft added

(<https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/>).

"This suggests, but does not definitively prove, that POLONIUM compromised these Fortinet devices by exploiting the CVE-2018-13379 vulnerability to gain access to the compromised organizations."

Microsoft urged customers to ensure that Microsoft Defender Antivirus uses the latest security intelligence updates (1.365.40.0 or later) and that multi-factor authentication (MFA) is enforced for all remote connectivity to block the abuse of potentially compromised credentials.

