Microsoft disrupts Bohrium hackers' spear-phishing operation

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** June 3, 2022 11:24 AM **0**

The Microsoft Digital Crimes Unit (DCU) has disrupted a spear-phishing operation linked to an Iranian threat actor tracked as Bohrium that targeted customers in the U.S., Middle East, and India.

Bohrium has targeted organizations from a wide range of industry sectors, including tech, transportation, government, and education, according to Amy Hogan-Burney, the General Manager of Microsoft DCU.

Microsoft has taken down 41 domains used in this campaign to establish a command and control infrastructure that enabled the attackers to deploy malicious tools designed to help them gain access to targets' devices and exfiltrate stolen information from compromised systems.

According to evidence provided by Microsoft in court filings [PDF (https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/06/Doc.-No.-16-Ex-parte-TRO-SEALED.pdf)], the Iranian hackers have been "intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computers networks of Microsoft and the customers of Microsoft, without authorization [..]."

While Microsoft did not reveal the timeline of this spear-phishing operation, some of the dozens of domains taken down have been used to host and push malware payloads as far back as 2017 (https://twitter.com/securitydoggo/status/888366917521735680).

"Bohrium actors create fake social media profiles, often posing as recruiters. Once personal information was obtained from the victims, Bohrium sent malicious emails with links that ultimately infected their target's computers with malware," Hogan-Burney said (https://twitter.com/CyberAmyHB/status/1532398959888457729).

"This activity was uncovered by Microsoft's Threat Intelligence Center (MSTIC), which tracks the world's nation-state and cybercrime actors so we can better protect our customers."

(https://twitter.com/CyberAmyHB/status/1532398956918890500)

This action is part of a long series of lawsuits targeting malicious infrastructure used in attacks against Microsoft customers worldwide.

"To date, in 24 lawsuits – five against nation-state actors – we've taken down more than 10,000 malicious websites used by cybercriminals and nearly 600 sites used by nation-state actors," Microsoft's Corporate Vice

when Redmond seized sites used by APT15 Chinese state hackers (https://www.bleepingcomputer.com/news/microsoft/microsoft-seizes-sites-used-by-apt15-chinese-state-hackers/).

Earlier this year, Microsoft also took down APT28 domains (https://www.bleepingcomputer.com/news/microsoft/microsoft-takes-down-apt28-domains-used-in-attacks-against-ukraine/) used in attacks against Ukraine and sinkhole 65 hardcoded domains to disrupt a botnet controlled by the ZLoader cybercrime gang (https://www.bleepingcomputer.com/news/security/microsoft-disrupts-zloader-malware-in-global-operation/).

Redmond also sued the North Korean-linked Thallium cyber-espionage group (https://www.bleepingcomputer.com/news/security/microsoft-takes-north-korean-hacking-group-thallium-to-court/) in December 2019 and seized 50 domains part of their malicious domain infrastructure.

The same month, Microsoft's Digital Crimes Unit successfully took over servers used in attacks by the Iran-backed APT35 (aka Charming Kitten, Phosphorus, or Ajax Security Team) threat actor (https://www.bleepingcomputer.com/news/security/microsoft-retaliates-against-apt35-hacker-group-by-seizing-99-domains/).

Previously, Microsoft filed 15 other similar cases (https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/) against the APT28 Russian-backed group in August 2018, which led to the seizure of another set of 91 malicious domains.