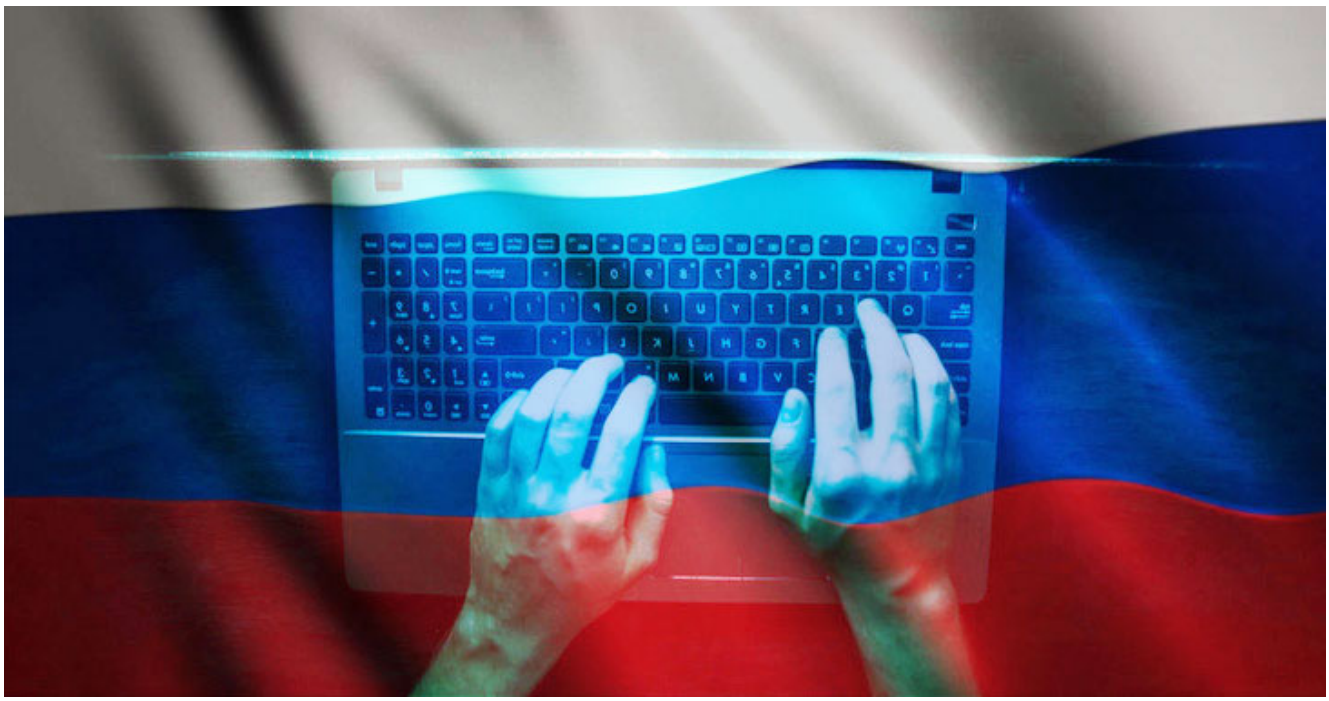
Microsoft Obtains Court Order to Take Down Domains Used to Target Ukraine

thehackernews.com/2022/04/microsoft-obtains-court-order-to-take.html

April 8, 2022



Microsoft on Thursday disclosed that it obtained a court order to take control of seven domains used by APT28, a state-sponsored group operated by Russia's military intelligence service, with the goal of neutralizing its attacks on Ukraine.

"We have since re-directed these domains to a sinkhole controlled by Microsoft, enabling us to mitigate Strontium's current use of these domains and enable victim notifications," Tom Burt, Microsoft's corporate vice president of customer security and trust, said.

APT28, also known by the names Sofacy, Sednit, Pawn Storm, Fancy Bear, Iron Twilight, and Strontium, is a cyber espionage group and an advanced persistent threat that's known to be active since 2009, striking media, governments, military, and international non-governmental organizations (NGOs) that often have a security focus.

The tech giant noted that the sinkholed infrastructure was used by the threat actor to target Ukrainian institutions as well as governments and think tanks in the U.S. and the European Union so as to maintain long term persistent access and exfiltrate sensitive information.

The seizure is part of a long-term investment to systematically dismantle infrastructure used by the threat actor, Microsoft said, adding it has used the expedited legal framework put in place 15 times to take down more than 100 Strontium-controlled domains.

Meta takes action against Ghostwriter and Phosphorus

The disclosure from Microsoft comes as Meta, the company formerly known as Facebook, revealed that it took action against covert adversarial networks originating from Azerbaijan and Iran on its platform, by taking down the accounts and blocking their domains from being shared.

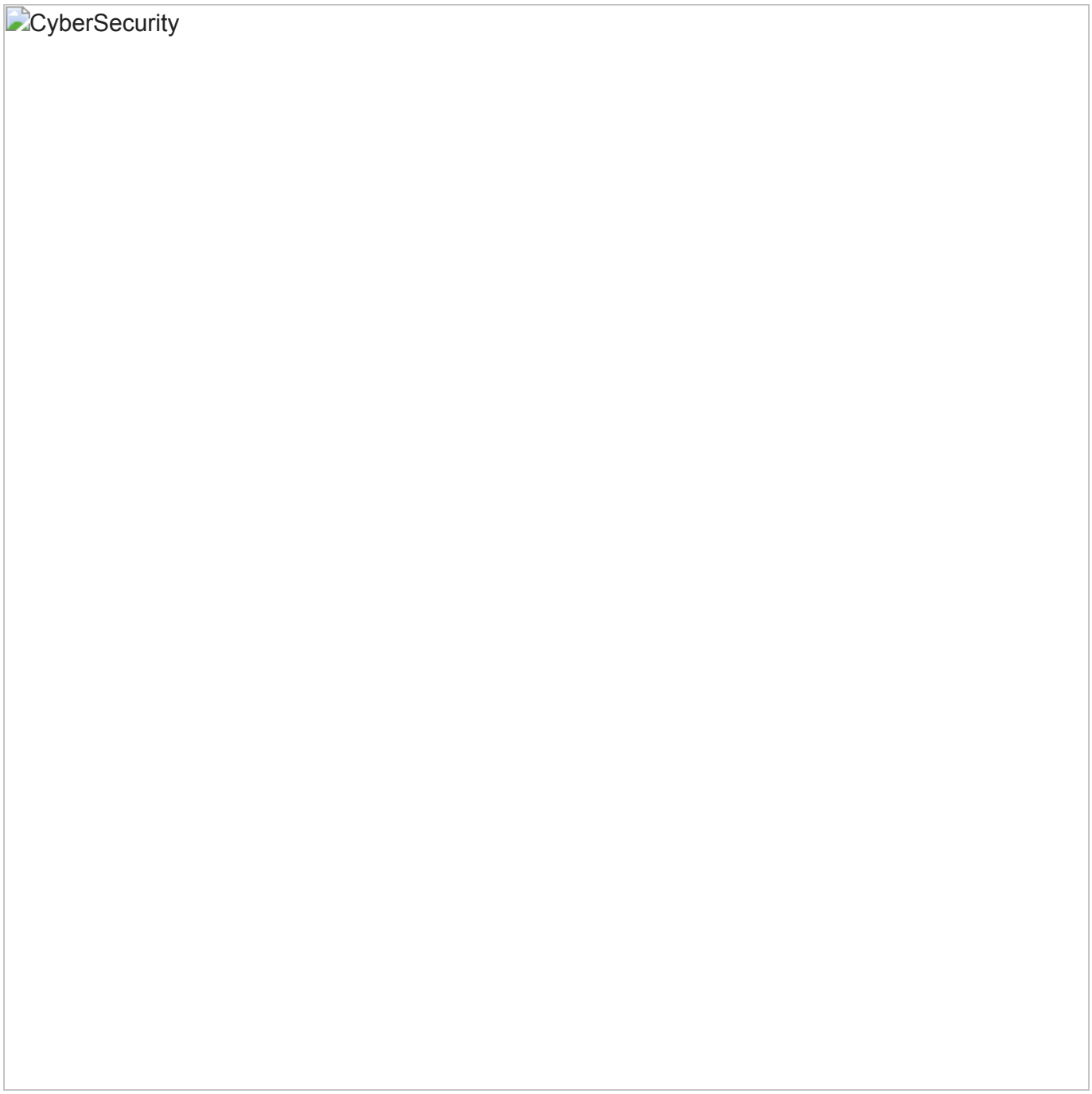
The Azerbaijanian operation is believed to have singled out democracy activists, opposition groups, and journalists from the country and government critics abroad for carrying out credential phishing and espionage activities.

Another involved UNC788 (aka Charming Kitten, TA453, or Phosphorus), a government-linked hacking crew that has a history of conducting surveillance operations in support of Iranian strategic priorities.

"This group used a combination of low-sophistication fake accounts and more elaborate fictitious personas, which they likely used to build trust with potential targets and trick them into clicking on phishing links or downloading malicious applications," Meta outlined in its first quarterly Adversarial Threat Report.

The malicious Android applications, dubbed HilalRAT, impersonated seemingly harmless Quran apps to extract sensitive information, such as contacts list, text messages, files, location information, as well as activate camera and microphone.

Meta also said it blocked the malicious activities associated with an unreported Iranian hacking group that leveraged tactics similar to that of Tortoiseshell to target or spoof companies in the energy, IT, maritime logistics, semiconductor, and telecom industries.



This campaign featured an elaborate set of bogus profiles on Instagram, LinkedIn, Facebook, and Twitter, with the actors posing as recruiters of real and front companies to trick users into clicking on phishing links to deliver information stealing malware that were disguised as VPN, calculator, audiobook, and messaging apps.

"They developed malware on the VMWare ThinApp virtualization platform, which allowed them to run it on many different systems and hold malicious payload back until the last minute, making malware detection more challenging," Meta explained.

Lastly, also disrupted by Meta were takeover attempts made by the Belarus-aligned Ghostwriter group to break into the Facebook accounts of dozens of Ukrainian military personnel.

The attacks, which were successful in a "handful of cases," abused the access to victims' social media accounts and posted disinformation "calling on the Army to surrender as if these posts were coming from the legitimate account owners."

SHARE □ □ □ □ □
SHARE □