Microsoft seized Russian domains targeting Ukrainian media organizations

Microsoft seized seven domains belonging to Strontium, also known as Fancy Bear or APT28, a Russian hacking group with ties to the country's military intelligence agency, the company announced in a blog post (via *TechCrunch*). According to Microsoft, Russian spies used these sites to target Ukrainian media outlets, as well as foreign policy think tanks and government institutions located in the US and the European Union.

Microsoft obtained a court order to take control of each domain on April 6th. It then redirected them to a sinkhole, or a server used by cybersecurity experts to capture and analyze malicious connections. The company says it has seized over 100 domains controlled by Fancy Bear before this most recent takedown.

"We believe Strontium was attempting to establish long-term access to the systems of its targets"
"We believe Strontium was attempting to establish long-term access to the systems of its targets, provide tactical support for the physical invasion and exfiltrate sensitive information," Tom Burt, Microsoft's corporate vice president of customer security and trust said in the post. "We have notified Ukraine's government about the activity we detected and the action we've taken."

This particular hacking group has a long history of attempting to interfere with both Ukraine and the US. Fancy Bear was linked to cyberattacks on the Democratic National Committee in

2016 and targeted the US election in 2020.

Russia’s invasion of Ukraine has only exacerbated cyberattacks by Fancy Bear and other bad actors. Last month, Google said Fancy Bear and Belarusian hacking group Ghostwriter carried out a phishing attack targeting Ukrainian officials and members of the Polish military. Russian state-sponsored hackers have also been accused of hacking into a European satellite service at the start of Russia’s invasion of Ukraine, as well as targeting US defense contractors in February. It’s unclear whether Fancy Bear was behind either attack.

https://www.theverge.com/2022/4/9/23018258/microsoft-control-russian-domains-ukraine-war-cyberattack-fancy-bear-apt28-strontium