New cyberattacks targeting sporting and anti-doping organizations - Microsoft On the Issues

By Tom Burt

Published: 2019-10-28 · Archived: 2026-04-02 12:47:18 UTC

Today we're sharing that the Microsoft Threat Intelligence Center has recently tracked significant cyberattacks originating from a group we call Strontium, also known as Fancy Bear/APT28, targeting anti-doping authorities and sporting organizations around the world. As the world looks forward with anticipation to the Tokyo Summer Games in 2020, we thought it important to share information about this new round of activity.

At least 16 national and international sporting and anti-doping organizations across three continents were targeted in these attacks which began September 16th, just before news reports about new potential action being taken by the World Anti-Doping Agency. Some of these attacks were successful, but the majority were not. Microsoft has notified all customers targeted in these attacks and has worked with those who have sought our help to secure compromised accounts or systems.

This is not the first time Strontium has targeted such organizations. The group reportedly released medical records and emails taken from sporting organizations and anti-doping officials in 2016 and 2018, resulting in a 2018 indictment in federal court in the United States.

The methods used in the most recent attacks are similar to those routinely used by Strontium to target governments, militaries, think tanks, law firms, human rights organizations, financial firms and universities around the world. Strontium's methods include spear-phishing, password spray, exploiting internet-connected devices and the use of both open-source and custom malware.

We've previously announced separate Strontium activity we've seen targeting organizations involved in the democratic process and have described the legal steps we routinely take to prevent Strontium from using fake Microsoft internet domains to execute its attacks. Additionally, the data and information we learn from our disruption work is used to improve the security and security features of our products and services.

As we've said in the past, we believe it's important to share significant threat activity like that we're announcing today. We think it's critical that governments and the private sector are increasingly transparent about nation-state activity so we can all continue the global dialogue about protecting the internet. We also hope publishing this information helps raise awareness among organizations and individuals about steps they can take to protect themselves.

You can protect yourself from these types of attacks in at least three ways. We recommend, first, that you enable two-factor authentication on all business and personal email accounts. Second, learn how to spot phishing schemes and protect yourself from them. Third, enable security alerts about links and files from suspicious websites.

Tags: anti-doping, cyberattacks, cybercrime, cybersecurity, Microsoft Threat Intelligence Center, phishing, The Digital Crimes Unit

---