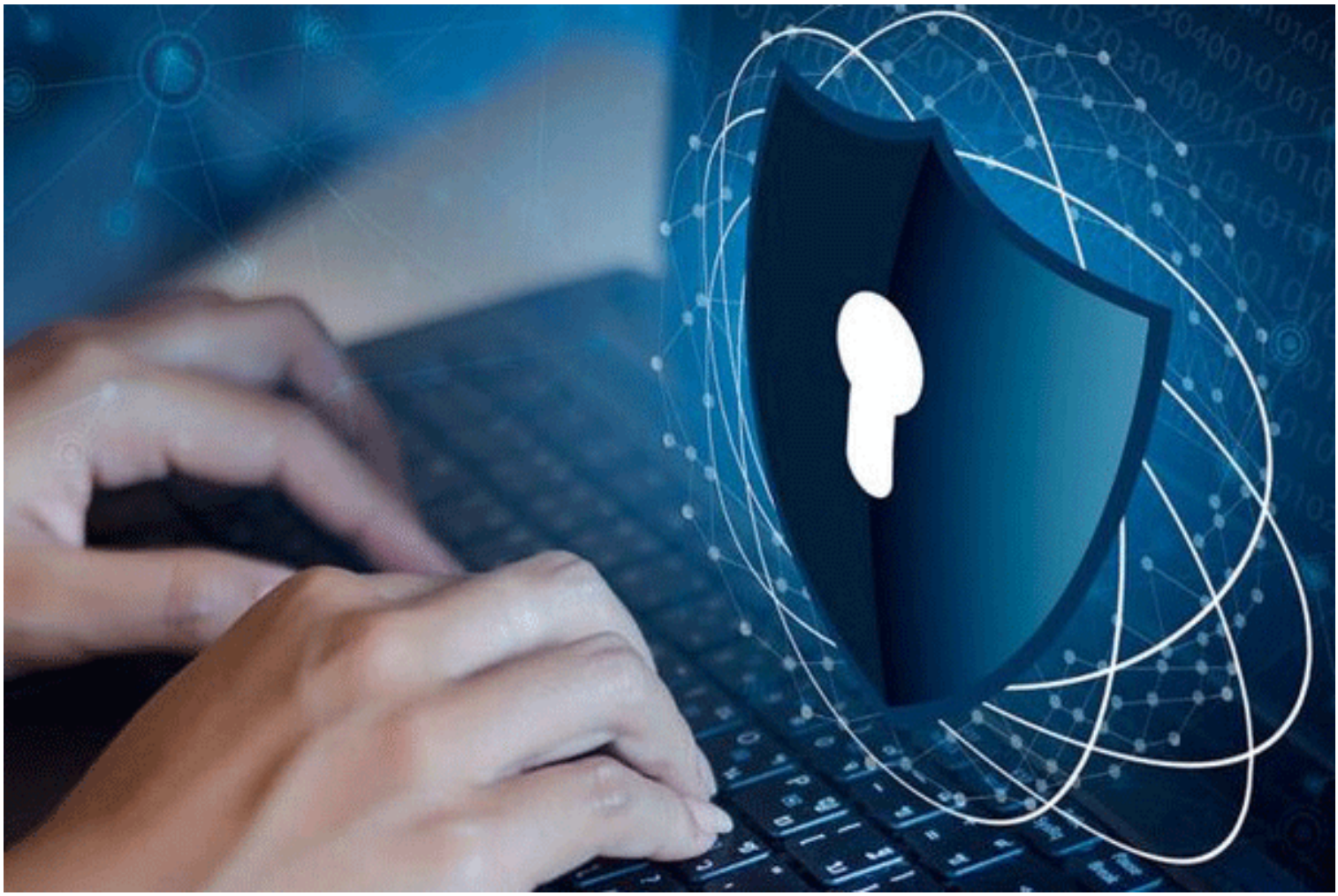
Tackling Strontium: a cyber-espionage group

By IASToppers | 2022-04-25 17:30:00



Tackling Strontium: a cyber-espionage group

Microsoft had recently disrupted cyberattacks from a Russian nation-state hacking group called ‘Strontium’.

[Ref: Sunday Guardian]

What is Strontium?

- Strontium is a **highly active cyber-espionage group**.
- It is known by different names such as Fancy Bear, Tsar Team, Pawn Storm, Sofacy, Sednit or Advanced Persistent Threat 28 (APT28) group.
- The group is **alleged to be connected to the GRU**, the Russian Armed Forces' main military intelligence wing.
- It has **access to highly sophisticated tools** to conduct spy operations, and has been attacking targets in the U.S., Europe, Central Asia and West Asia.
- It is said to have attacked The Democratic National Committee (DNC) (2016 U.S. presidential election), the global television network TV5Monde, the World Anti-Doping Agency (WADA) etc.

Modus Operandi

- The group deploys diverse malware and malicious tools to breach networks.
    - **VPNFilter malware** is used to target hundreds of thousands of routers and network-access storage devices worldwide
    - It uses **spear-phishing** (targeted campaigns to gain access to an individual's account) and **zero-day exploits** (taking advantage of unknown computer-software vulnerabilities) to target specific individuals and organisations.
- These tools can be used as hooks in system drivers to access local passwords, and can track keystroke, mouse movements, and control webcam and USB drives.
    - They employ **watering hole attack**, that compromises a site that a targeted victim visits to

gain access to the victim's computer and network.

- They can also search and replace local files and stay connected to the network.
    - A malware called **Drovorub**, provides file download and upload capabilities; execution of arbitrary commands; and implements hiding techniques to evade detection.