Microsoft: 17 European Nations Targeted by Russia in 2023 as Espionage Ramping Up

Russia has been ramping up its cyberespionage operations in 2023, according to a new intelligence report from Microsoft that analyzes Russia's hybrid warfare in Ukraine.

Russia has launched many disruptive cyberattacks against Ukraine, including DDoS attacks and wiper attacks, and it has stepped up its misinformation campaigns. Since the start of the conflict, Moscow-backed hackers have deployed at least two ransomware and nine wiper families against over 100 organizations.

However, Ukraine is not the only country targeted by Russian state-sponsored cyber actors since the start of the war, particularly when it comes to cyberespionage operations.

A report published on Wednesday by Microsoft's threat intelligence unit shows that at least 17 European countries have been targeted in espionage campaigns in the first couple of months of 2023, and 74 countries have been targeted since the start of the war.

Of these 74 countries – the list does not include Ukraine – Microsoft saw the highest percentage of attacks against the United States (21%), followed by Poland (10%) and the UK (9%).

"EU and NATO member states, especially on the eastern flank, dominate the top 10 most targeted countries by number of threat events recorded. However, Russian threat actors

conducted activities that ranged from reconnaissance to data exfiltration in organizations across the globe, in Africa, Asia, Latin America, and the Middle East," Microsoft explained.

Unsurprisingly, the government sector was the most targeted, followed by IT/communications, and think tank/NGO.

[Read: A Year of Conflict: Cybersecurity Industry Assesses Impact of Russia-Ukraine War **]**

While a majority of the attacks were part of espionage operations, Microsoft cautioned that state-sponsored threat actors have "already shown a willingness to use destructive tools outside

Ukraine if instructed".

Microsoft's report highlights three trends related to Russia's tactics: disguising destructive attacks as ransomware; the use of various methods for initial access, including pirated software, vulnerability exploitation, and supply chain attacks; and the use of real and fake hacktivists for power projection.

Microsoft's report was published on the same day the tech giant revealed that a Russian threat group has been exploiting an Outlook zero-day vulnerability in attacks aimed at the government, transportation, energy, and military sectors in Europe.

Related: Russia-Linked APT 'Winter Vivern' Targeting Governments in Europe, Asia

Related: Russian Cyberspies Abuse EU Information Exchange Systems in Government Attacks

Related: Exploitation of Bitrix CMS Vulnerability Drives ICS Attack Surge in Russia

Microsoft: 17 European Nations Targeted by Russia in 2023 as Espionage Ramping Up