

## Threat Landscape

As we enter July, the cybersecurity landscape faces an extraordinary test with the upcoming Paris 2024 Olympics and Paralympics. Scheduled from July 26 to August 11 and August 28 to September 8, these events will likely be targets for organized crime, activists, and state actors. (1)

Paris 2024 has teamed up with the French national agency for information security (ANSSI) and other organizations, and they have hired ethical hackers to stress test their systems. “We can't prevent all the attacks, there will not be Games without attacks, but we have to limit their impacts on the Olympics”, said Vincent Strubel, the director general of ANSSI. (1)

The perspective that it's impossible to prevent all attacks, but crucial to reduce their impact, is a sound approach. Therefore, staying on top of patch management is essential. In late June, Atlassian released updates to address six security defects, all disclosed this year. The most severe of these is a broken access control issue in the Spring Framework, enabling unauthenticated attackers to access assets they should not have access to. (2) In mid-June, Microsoft disclosed a critical Wi-Fi vulnerability related to their Patch Tuesday updates. This vulnerability allows remote code execution without user interaction, affecting Wi-Fi drivers across all supported Windows versions. (3)

On 26 June 2024, TeamViewer detected an irregularity within its internal corporate IT environment. They immediately activated their response team and implemented necessary remediation measures. Two days after, they confirmed that the Russian hacking group APT29, also known as Cozy Bear, BlueBravo and Midnight Blizzard, had breached the corporate IT environment using employee credentials. It is advised to enhance monitoring or remove TeamViewer software to mitigate potential risks. (4,5) APT29 was also responsible for the SolarWinds attack in 2020, and the Microsoft attack earlier this year where they breached Microsoft's corporate infrastructure and stole customers emails. (6)

The Vultur banking trojan has been detected in Norway, allowing remote control of infected devices. The attack begins with an SMS notification regarding an unpaid invoice, leading recipients to call a specified number and then install malware disguised as a McAfee Security app. Once installed, the trojan grants full control over the device, blocks interaction with certain apps, and bypasses lock screen security. The threat mainly targets Android users. (7)

Lastly, researchers have identified several vulnerabilities in the Netgear WNR614 N300 router, once popular among home users and small businesses due to its affordability. These vulnerabilities include authentication bypass, weak password policies, plaintext password storage, and WPS PIN exposure, presenting significant security risks to networks and user data. As the router has reached its end-of-life and is no longer supported by Netgear, users are advised to replace it with a supported model for improved security. (8)

### Most recent online cybersecurity risks (9)

- RCE Vulnerability Discovered in Mailcow
- Fake Virtual Meeting Software Spreads Infostealers
- Critical Vulnerability in VMware vCenter Patched
- LockBit Attacks Soar Following Law Enforcement Takedown
- New Infostealer Uses Several Infection Methods

- (1) <https://www.reuters.com/technology/cybersecurity/paris-2024-gearing-up-face-unprecedented-cybersecurity-threat-2024-05-06/>
- (2) <https://www.securityweek.com/atlassian-patches-high-severity-vulnerabilities-in-confluence-crucible-jira/>
- (3) <https://www.forbes.com/sites/daveywinder/2024/06/14/new-wi-fi-takeover-attack-all-windows-users-warned-to-update-now/>
- (4) <https://www.teamviewer.com/en/resources/trust-center/statement/>
- (5) <https://therecord.media/teamviewer-cozy-bear-hack-confirmed>
- (6) <https://www.securityweek.com/microsoft-alerts-more-customers-to-email-theft-in-expanding-midnight-blizzard-hack/>
- (7) <https://www.telenor.no/bedrift/blogg/sikkerhet/banktrojaner/>
- (8) <https://www.bleepingcomputer.com/news/security/netgear-wnr614-flaws-allow-device-takeover-no-fix-available/>
- (9) <https://innovatecybersecurity.com/security-threat-advisory/>