Cyberattack shuts down hundreds of Russian pharmacies, disrupts healthcare services

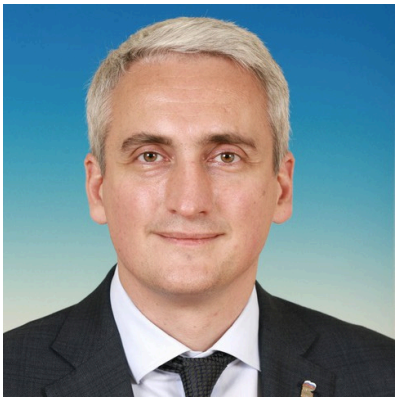
Infosources™

August 10, 2025

In recent weeks, Russia has faced a coordinated wave of cyber intrusions that disrupted everyday services—from pharmacies and clinics to airlines and alcohol retailers. Each incident laid bare vulnerabilities in systems once deemed resilient, but none matched the gravity of the final assault: a crippling DDoS strike on one of St. Petersburg's largest internet providers. This series of attacks not only underscored the evolving tactics of anonymous threat actors but also highlighted how dependent citizens and businesses are on uninterrupted digital connectivity.

Pharmacy Chains Paralyzed by Ransomware or Hack

Two of Russia's biggest pharmacy players, Stolichki (1,000 stores nationwide) and Neofarm (110 outlets in Moscow and St. Petersburg), saw all payment systems and online drug-reservation portals go dark after a malicious breach. Stolichki confirmed that a "technical failure" on Tuesday was, in fact, a cyberattack, and by Wednesday only half of its outlets had reopened. Neofarm likewise posted storefront notices blaming unspecified "technical issues" and sent its staff home until normal operations could resume. Both chains trace back to ex-lawmaker Yevgeny Nifantiev's holding company, though he ostensibly divested under Western sanctions in 2022.



Yevgeny Nifantiev

Healthcare Network's Patient Portal Knocked Offline

Moscow's Family Doctor clinic group reported a separate cyber incident that forced its patient portal and appointment scheduler offline. With no clear link to the pharmacy hacks, the network defaulted to walk-in appointments to maintain care continuity. Roskomnadzor, the state internet regulator, stated these outages were not the result of DDoS campaigns but declined to explain the attackers' methods or point to any perpetrators.

Aeroflot Struggles under Critical Infrastructure Breach

Earlier in the month, Aeroflot—the nation's flagship carrier—suffered a significant cyberattack that snarled flight schedules across Russia. Pro-Ukrainian hacking collective Silent Crow, along with the Belarusian Cyber Partisans, claimed responsibility, highlighting a growing trend of cyber assaults on transportation hubs. The incident forced widespread delays and cancellations, demonstrating that even well-protected aviation systems can be brought to their knees.

Silent Crow

Belarussian Cyber Partisans

WineLab Stores Shut by Ransomware Pressure

Novabev Group, operator of over 2,000 WineLab liquor shops, was hit by a ransomware infection that shuttered every outlet for three days. The company steadfastly refused to pay the demanded ransom, opting instead to rebuild its IT infrastructure from backup systems. This episode illustrated how profit-driven attacks on non-essential retail can still inflict broad economic pain and alarm business operators.

Critical Communications Disrupted: The St. Petersburg ISP DDoS

On Wednesday, one of St. Petersburg's largest internet service providers experienced a "malicious activity" outage caused by a sophisticated distributed denial-of-service assault. Unlike prior incidents that targeted specific businesses, this attack struck at the heart of regional connectivity, severing access for thousands of residential and commercial customers. No hacking group has yet claimed credit, but its scale and timing suggest a calculated effort to sow maximum disruption. By incapacitating the underlying network fabric, this operation represents the most consequential blow in the recent hacking spree—threatening not only commerce and communications but also emergency services and critical infrastructure reliant on the internet.

Taken together, these breaches paint a clear picture: adversaries are increasingly willing to target civilian-facing systems to achieve geopolitical or financial ends. With no single actor claiming all the strikes, attribution remains murky, and Russian authorities must now confront the reality that assuring digital resilience is as critical as safeguarding borders.