Recent Cyber Attacks: Major Incidents & Key Trends | Fortinet

Archived: 2026-04-29 02:10:24 UTC

Recent cyberattacks reflect that threat actors are no longer relying on isolated exploits. They are combining several tactics, like automation and social engineering, to achieve maximum impact. Here are a few cybersecurity trends that define how cyber risk has evolved in 2025.

Third-party and supply-chain compromise is a primary attack vector

Many of 2025's most damaging incidents began with compromised vendors or shared platforms. For instance, attacks on UNFI, the U.S. Treasury, Snowflake customers, and the UK Ministry of Defence all highlight how third-party vulnerabilities can lead to disruptions.

Credential-based attacks are replacing complex malware

Threat groups increasingly conduct phishing and credential stuffing over complex malware. Campaigns targeting M&S, Ukrainian government users, retailers, and SaaS platforms show how stolen credentials enable rapid access without triggering alarms. This trend highlights the critical role of MFA, identity monitoring, and user awareness.

Zero-day and unpatched software exploitation is accelerating

Today, attackers are actively scanning for vulnerable enterprise software and weaponizing flaws within days. The SAP NetWeaver zero-day and Microsoft SharePoint exploits reveal how a single unpatched flaw can expose hundreds of organizations at once. Patch management delays now directly translate into systemic risk.

Cyber incidents are causing real-world operational disruption

Incidents in 2025 increasingly disrupted food supply chains, healthcare services, airports, and government operations. Ransomware attacks forced hospital diversions, grounded flights, and manual airport operations. Cybersecurity has become a public safety and economic stability concern.

State-linked cyber operations are blending espionage and cybercrime

Attacks related to China, Russia, Iran, and North Korea reflect a growing overlap between espionage and political influence. From election interference to crypto theft funding weapons programs, cyber operations are now strategic tools of national power. Attribution may remain unclear, but the geopolitical consequences are not.

These evolving threats and cyber attacks require faster detection and automated response. Fortinet's SIEM and SOAR solutions, including FortiSIEM and FortiSOAR, can help organizations detect advanced attacks. These solutions can help correlate signals across IT and OT environments and enable teams to respond proactively. Backed by FortiGuard threat intelligence, Fortinet enables security teams to stay ahead of high-impact cyber risks.

When major data breaches and fast-moving cyber threats outpace defenses, every delayed detection increases risk — the right intelligence can make the difference. Discover FortiGuard Services.

Source: https://www.fortinet.com/uk/resources/cyberglossary/recent-cyber-attacks