INSIDER INTELLIGENCE | eMarketer

FEB 23
Jacob Bourne

Alarm bells ring over Russia DDoS attack on Ukraine

Article

The news: A spate of distributed denial of service (DDoS) attacks against Ukraine's government, at least two banks, and a web-hosting firm last week were carried out by Russian government-backed hackers, according to US and UK officials. In response, nations around the world rushed to shore up their own cybersecurity.

More on this: Days before Russian troops began entering Ukraine's eastern Donbas region, triggering sanctions, **cyberattacks temporarily took down Ukraine's Ministry of Defense website and private sector websites**, per ComputerWeekly.

- The attack was deemed the worst of its kind in Ukraine's history and had likely been planned long in advance.
- Despite the large scope of the attack and resulting disruptions in online payments and bank apps, **no lasting damage was inflicted**.
- Although Russia denied responsibility, US officials moved more quickly than usual to place blame due to the unstable situation and Russia's history of mounting cyberattacks against Ukraine over the past decade.
- In response, **cybersecurity experts from six EU countries are heading to Ukraine to help counter threats**, and the EU issued a list of 14 recommendations for public and private organizations as defensive measures.
- New York state announced added cybersecurity preparations in wake of the attack, with plans for a **$62 million** cybersecurity investment.

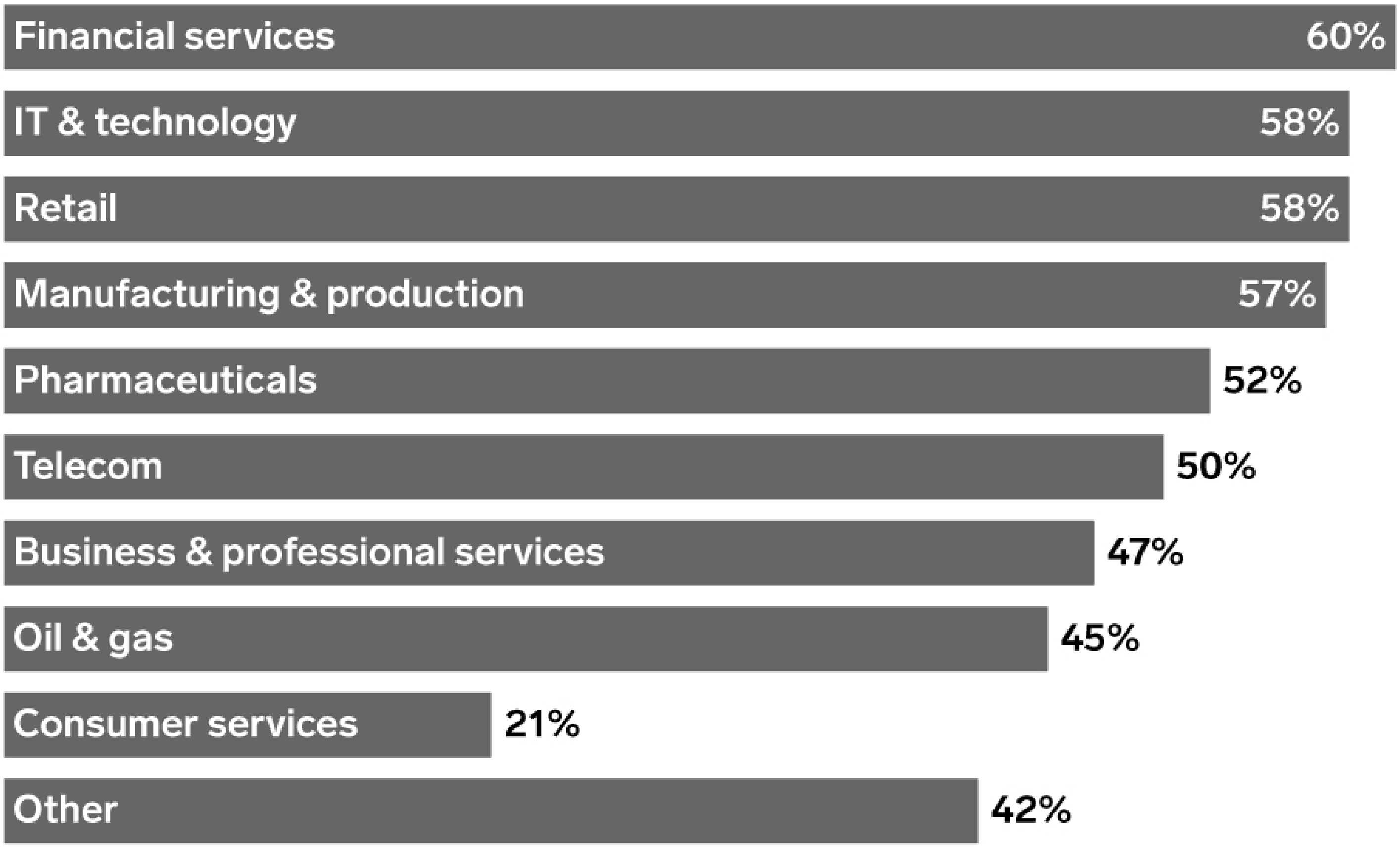
Why it's worth watching: The cyberattacks are a stark reminder that warfare is no longer limited to physical force but entails **network assaults to cripple governments, critical infrastructure, financial services, healthcare, and the energy sector**—escalating global volatility.

The **FBI issued a report warning the US private sector to beef up cybersecurity** in preparation for potential war in Eastern Europe, per Newsweek. The agency views defense contractors as primary targets, signaling that the threat extends far beyond Ukraine.

- With the world already dealing with supply chain disruptions, cyberattacks against logistics companies and infrastructure would result in further delays.
- As prices of oil, natural gas, agricultural products, aluminum, and nickel surge due to the specter of war, cyberattacks against these industries are likely to send prices even higher.
- Although Russia might target specific sectors, copycat hackers could take advantage of vulnerabilities to launch broader assaults.

UK and US IT and Business Decision-Makers with Fully Implemented Cybersecurity Strategies, by Sector, Sep 2021

% of respondents



Source: S-RM, "Investing in Cyber Resilience: Spend, Strategy, and Search for Value," conducted by Vanson Bourne, Nov 12, 2021

271395 InsiderIntelligence.com