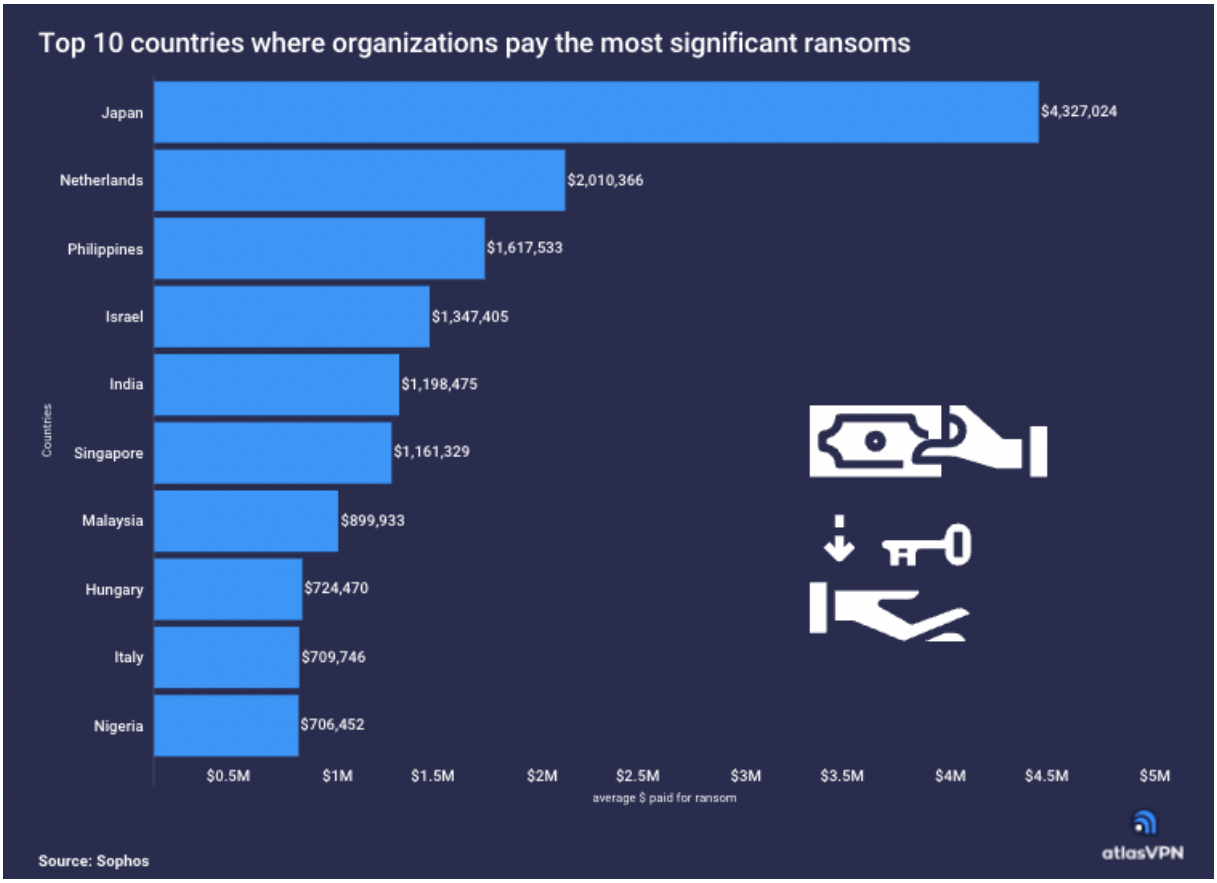
Japan and Netherlands-based businesses pay the largest price for ransomware attacks

William S. | May 18, 2022

Cybercriminals encrypt essential files and documents, leaving victims with the option of paying a ransom to regain access or restoring data from backups. That makes ransomware attacks one of the most severe cyber risks businesses face.

According to the Atlas VPN team's findings, organizations in Japan and Netherlands paid the most significant price for suffering ransomware attacks in 2021. In addition, cybercriminals targeted media, leisure, entertainment, and retail businesses the most.

The data is based on Sophos the State of Ransomware 2022 report. The research surveyed 5,600 IT professionals in mid-sized organizations (100-5,000 employees) across 31 countries. The average ransom payment is determined by how much the organizations paid in the most significant ransomware attacks.



Businesses in **Japan** paid an average price of nearly **$4.3 million** in the most significant ransomware attacks in 2021. Japan is home to many companies in the IT and manufacturing industry, which is why cybercriminals target Japanese organizations heavily. National Police Agency received 146 requests over ransomware attacks last year.

Companies in the **Netherlands** handed over an average of **$2 million** in ransom to cybercriminals. The Dutch government announced in 2021 that it might use intelligence agencies or military services to counter ransomware attacks.

Organizations in the **Philippines** paid an average price of **$1.6 million** in ransom. **Israeli** businesses handed over about **$1.3 million** to hackers after

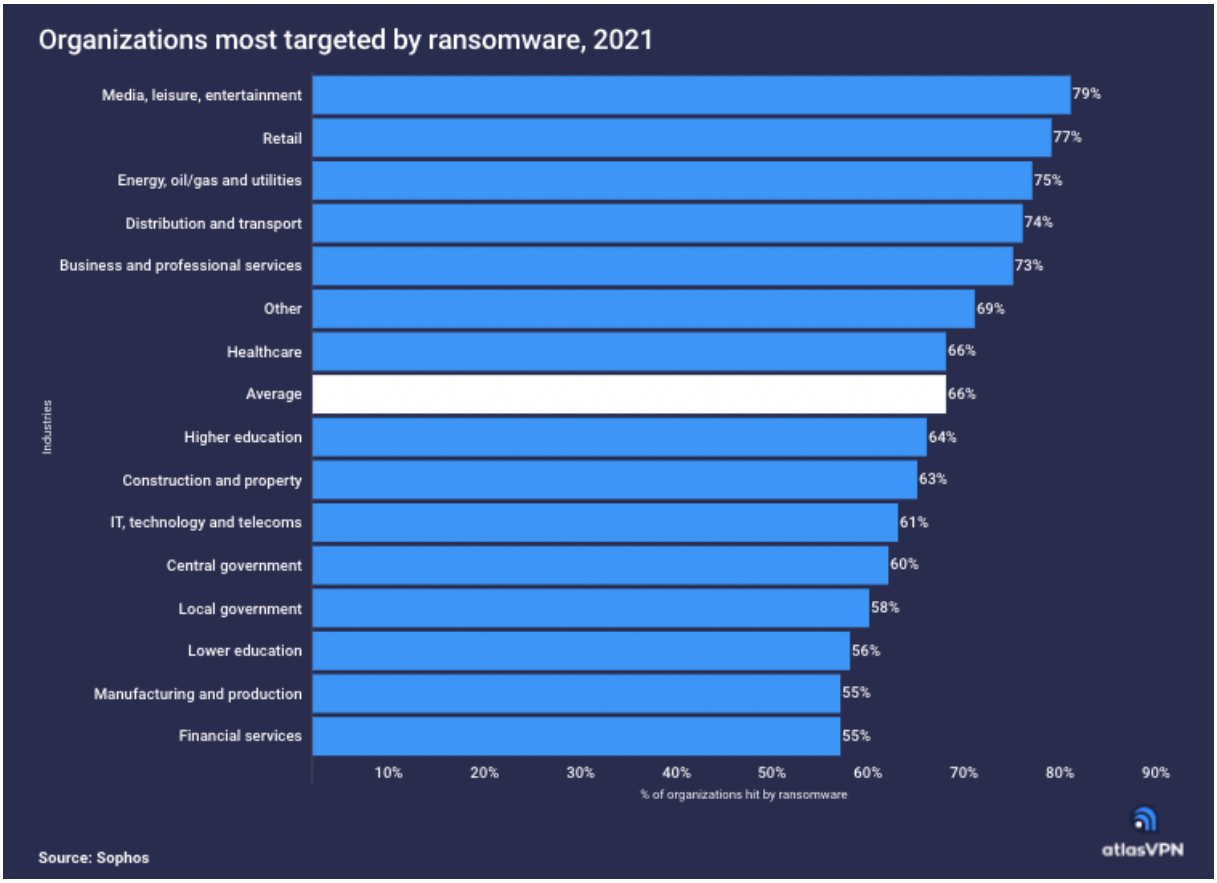
ransomware attacks in 2021. At the same time, **Indian** companies paid **$1.2 million** in ransom to decrypt their information.

Paying millions of dollars to hackers for mid-sized organizations can be devastating. Such businesses are highly vulnerable as they have limited resources for cybersecurity budgets, meaning easier access for cybercriminals.

Industries most targeted by ransomware

While looking at the statistics, a horrific pattern can be seen. About **two-thirds** of all surveyed organizations claim to have experienced ransomware attacks in 2021. All analyzed industries have a higher than 50% chance of being targeted with ransomware.

Out of all surveyed **media, leisure, and entertainment** businesses, **79%** suffered ransomware attacks in 2021. As social media and entertainment consumption increase, threat actors focus more on such channels. Phishing attack campaigns through social media open doors for malware to access the network.



The **retail** industry is the second most targeted by ransomware, as **77%** of organizations claimed to have suffered an attack. Online shopping and e-commerce continued to grow in 2021, which fueled ransomware attacks on retail businesses. As many companies moved to the digital space, cybersecurity became a new challenge to manage.

Three out of four (**75%**) businesses in the **energy and gas** sector suffered ransomware attacks. Cyberattacks on such companies can have a significant effect not only on the business itself but also on countries' supply of gas and petrol. Gas shortages were recorded in countries where ransomware disrupted energy infrastructure.

Out of surveyed respondents in the **distribution and transport** industry, **74%** experienced ransomware attacks in 2021. The **business and**

professional services sector is next up, as **73%** of companies were attacked with ransomware. Furthermore, **69%** of **other** companies dealt with ransomware, while **66%** of **healthcare** institutions were targets of such attacks.

Based on the evidence, ransomware assaults are not going away anytime soon. Hackers will continue to target various countries and businesses as long as they uncover flaws to exploit. Whether you are a smaller business or a giant corporation, spending on cybersecurity is necessary to keep your and your client's data secure.