TitanHQ

The Ransomware Review 2022

Looking to the future: preparing for the evolution of threats

Ransomware is a form of malware which encrypts a victim's data or blocks access until a ransom is paid. **Ransomware was named the top threat type of 2021**, and has shown no sign of slowing down in 2022.

Some interesting figures

Cyber criminals can now penetrate **93% of company networks**.

Today, businesses suffer ransomware attacks every **40 seconds**.

46% of organisations that had data encrypted in a ransomware attack paid the ransom.

Ransomware breaches have increased by **13% in 2022** – more than the last five years combined.

The average ransomware victim loses around **35%** of their data.

The average downtime a company experiences after a ransomware attack is **22 days**.

The effects of ransomware are significant...

The average ransom payment has increased by **82%** since 2020, reaching **$570,000** in the first half of 2021 alone.

In 2021, **11%** of organisations said they paid ransoms of **$1 million** or more, up from **4%** in 2020.

The average cost to recover from the most recent ransomware attack in 2021 was **$1.4 million**.

On average, it takes one month to recover from the damage and disruption of a ransomware attack.

90% of organisations said suffering a ransomware attack impacted their ability to operate.

80% of businesses that chose to pay a ransom demand suffered a second ransomware attack.

Following a ransomware attack, **61%** of consumers switched some or all their business to a competing brand.

Top 5 industry targets

01.	02.	03.	04.	05.
Education	Retail	Business, professional and legal services	Government	I.T.

Education is the sector least capable of preventing data encryption in a ransomware attack. Higher education reported the highest data encryption rate of all sectors at **74%**, with lower education reporting **72%**.

45% of lower education and **50%** of higher education organisations paid the ransom to retrieve encrypted data.

Why has ransomware increased?

Paying the ransom

As more victims are now paying the ransom to retrieve their encrypted data, cyber criminals have more monetary incentive.

Human error

82% of cyber breaches involved a human element, including social attacks, errors and misuse.

Geopolitical tensions

Growing global conflicts have contributed to the significant increase in ransomware attacks.

Upcoming ransomware trends

Ransomware is a many-headed beast, with new mutations developing all the time. These threats are set to dominate the cyber sphere in the coming years.

Ransomware as a Service

Ransomware as a Service describes the act of cyber criminals selling subscriptions to their malware, allowing anyone to buy and launch a ransomware attack.

Double extortion ransomware

Double extortion ransomware is an attack in which threat actors exfiltrate a victim's sensitive data in addition to encrypting it. If the ransom is not paid, sensitive data will be published.

Intermittent encryption

Intermittent encryption only encrypts certain parts of files, so they appear as corrupted data. This approach allows the attack to bypass many forms of threat detection and prevention.

What to expect in 2023

In 2023, ransomware is expected to continue to dominate the threat landscape. As a result of the developing risk, it is predicted that governments and businesses will begin to develop a more mature response.

- Attackers are expected to execute more personalised double-extortion attacks in **2023**
- The number of global governments with legislation around ransomware payments is forecast to grow from **1%** to **30%** by **2025**
- By **2025**, **40%** of boards will have a dedicated cybersecurity committee overseen by a qualified board member

How to best protect your organisation

Implementing a multi-layered security posture is key to defending your organisation from the growing threat of ransomware.

- Advanced anti-malware protection
- Regular Backups
- Anti-spam and anti-phishing solutions
- Regular patching
- Content filtering
- Breach detection systems

TitanHQ

Fortify your defences today

Your organisation's level of preparation decides your level of success at preventing and protecting against ransomware. To avoid the negative consequences, ensure that you are implementing the optimal tools and solutions.

To find out more, get in touch with TitanHQ today.

GET IN TOUCH