Ransomware in 2023

Why ransomware attacks have been increasing

Almost all the threat vectors for cyber [breaches] are exploited by ransomware. According to the survey, the main reason leaders think an organization falls victim to a ransomware attack is a lack of a unified cybersecurity strategy (37%).

The software supply chain and leaky APIs are the biggest targets for ransomware attacks, followed by employee vulnerabilities to blackmail / extortion (78%).

Leaders point to employees as the main vulnerability points exploited by ransomware (78%). As for why ransomware has been making the news more often recently, leaders believe it’s mainly due to the fact that remote work has revealed holes in the security stack that teams have been unable to patch sufficiently.

Ransomware attacks are getting more generic (22%) and more often secondarily targeted (36%), which makes it harder to identify and prevent them. Incidents of ransomware, when attackers use malware to seal off data until a ransom demand is made illegal to use for ransom payments), the market has become more regulated (or one that can be copied), and ransomware payments are likely to increase in the future.

Almost three-quarters (71%) of leaders have worked in an organization that has experienced a ransomware incident. Of these, 70% of leaders consider ransomware attacks an operating cost for businesses. To what extent do you agree with the following:

- Businesses are more vulnerable to ransomware attacks in the past than in the future?
  - Yes: 49%
  - No: 44%
  - Neutral: 7%

- Was the ransomed data recovered?
  - Likely: 37%
  - Unlikely: 6%
  - Don’t know: 57%

- Was the ransomware paid?
  - Yes: 34%
  - No: 58%
  - Don’t know: 8%

- From an organizational viewpoint, is ransomware attacks more or less likely to occur in the future?
  - More likely: 66%
  - Less likely: 23%
  - The same likelihood: 11%

- To what extent do you agree with the following?
  - The proliferation of cryptocurrencies makes it harder to trace ransomware payments?
    - Strongly agree: 23%
    - Agree: 49%
    - Neutral: 16%
    - Disagree: 11%
    - Strongly disagree: 3%

- Do you agree with any of the following?
  - The public availability of organizational power / who can be exploited (79%) and healthcare (72%).
  - Insufficient partner audits (not mainly due to the fact that remote work has revealed holes in the security stack that teams have been unable to patch sufficiently.

- Does the software supply chain and leaky APIs are the biggest targets for ransomware attacks, followed by employee vulnerabilities to blackmail / extortion (78%).

- The survey was conducted from June 26 - August 28, 2021, with a total of 331 tech decision-makers participating. The respondent breakdown includes:
  - C-Suite, 54%
  - VP, 27%
  - Director, 18%
  - Other, 1%
  - Breakdown by company size:
    - <1,001: 23%
    - 1,001-5,000: 23%
    - 5,001-10,000: 19%
    - 10,001+: 39%

- Breakdown by region:
  - EMEA: 54%
  - APAC: 27%
  - Americas: 13%
  - Other: 6%

- Breakdown by industry:
  - Energy: 27%
  - Healthcare: 11%
  - Sport franchises/events: 11%
  - Other: 11%