Ransomware payments nearly double in one year

Publication Date: 2023-05-10

Author: Dan Milmo

Section: Technology

Tags: Cybercrime, Internet, news

Article URL: https://www.theguardian.com/technology/2023/may/10/ransomware-payments-nearly-double-in-one-year

Ransomware payments have nearly doubled to $1.5m (£1.2m) over the past year, with the highest-earning organisations the most likely to pay attackers, according to a survey. Sophos, a British cybersecurity firm, found that the average ransomware payment rose from $812,000 the previous year. The average payment by UK organisations in 2023 was even higher than the global average, at $2.1m. More than a quarter of the companies that made payments in the global survey handed over between $1m and $5m, with high-earning firms the most likely to fork out. The average payout by companies with revenues of more than $5bn a year was just under $2.5m. “Perhaps unsurprisingly, the largest revenue organisations were most likely to pay the highest ransoms, reflecting that adversaries will adjust the amount they will accept based on ability to pay,” said Sophos. Ransomware attacks involve rogue actors gaining access to an entity’s computer system and deploying a piece of malware – malicious software – that encrypts computers, making it impossible to access their content. The attacker, who could also steal data as part of the attack, then demands money in exchange for decrypting or unlocking the computers. High-profile victims of ransomware attacks over the past year include Royal Mail and the Guardian. The Sophos report was drawn from a survey of 3,000 senior IT and cybersecurity professionals at a range of organisations, such as schools, retailers and healthcare providers, across 14 countries including the US, the UK and Australia. However, the 2023 survey is smaller than the previous year’s, when 5,600 professionals were interviewed across 31 countries. The 2023 report interviewed 200 UK organisations. The rate of ransomware attacks in the 2023 report was unchanged from 2022, with two-thirds of respondents saying they had been hit by an attack. Singapore had the highest rate of attack at 84%, with the UK the lowest at 44%. South Africa had the biggest increase in the survey from 51% of firms in the 2022 survey to 78%. The education sector was the most likely to have experienced an attack last year at 80% – evenly split between lower and higher education organisations – which Sophos said reflected a lower level of resources and technology. The construction and property sectors were the second most affected, while IT, tech and telecoms companies reported the lowest level of attack, indicating a higher level of cyber readiness. Companies with the highest incomes were most likely to be targeted. If an organisation had annual revenue of more than $5bn it was more likely to be attacked. In three out of 10 attacks email was the root cause, such as through phishing emails, where people are fooled into clicking on a link that downloads malicious software. More than three-quarters of attacks resulted in the victims’ data being encrypted and rendered inaccessible. Of those attacks, three out of 10 involved data being stolen. Nearly all organisations that had their data frozen got it back, largely through backup systems, although 46% paid the ransom – with the highest-earning companies the most likely to pay the attackers. In the UK and France, around one in 10 organisations that paid the ransom did not get data back. “Organisations with lower annual revenue have less money to fund ransom payments, forcing them to focus on backups for data recovery,” said the report. “At the same time, larger revenue organisations typically have complex IT

infrastructures, which may make it harder for them to use backups to recover data in a timely fashion. They are also the businesses most able to buy their way out of such situations."