Cyber-hacking victims ‘paid out record $1.1bn in ransoms last year‘

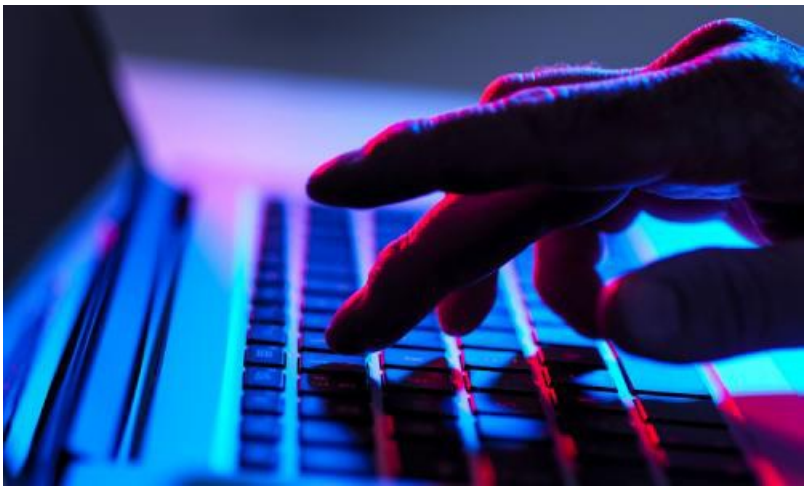
Publication Date: 2024-02-07

Author: Dan Milmo

Section: Technology

Tags: Cybercrime, Internet, Cryptocurrencies, Technology sector, news

Article URL: https://www.theguardian.com/technology/2024/feb/07/ransomware-gangs-staged-comeback-last-year-says-crypto-research-firm



Ransomware gangs staged a “major comeback” last year, according to research, with victims of hacking attacks paying out a record $1.1bn to assailants. Cyber criminals stepped up their global operations in 2023 after a lull in 2022, with victims including hospitals, schools and major corporations. Payments to criminal gangs in the wake of attacks doubled compared with 2022 when $567m was paid out, a report by the cryptocurrency research firm Chainalysis found. It added that “big game hunting” had become a feature of attacks last year, with a greater share of ransom payments costing $1m or more as wealthier entities were targeted. Chainalysis said: “2023 marks a major comeback for ransomware, with record-breaking payments and a substantial increase in the scope and complexity of attacks – a significant reversal from the decline observed in 2022.” Ransomware attacks typically involve hackers entering a target’s computer system and paralysing it with malware, which encrypts files and makes them inaccessible. A new trend in attacks involves assailants extracting data from the IT system, such as staff or customer details. The gang then asks for payment in cryptocurrency, usually bitcoin, to unlock the files or to delete their copy of the stolen data. Chainalysis said a number of factors contributed to the payments dip in 2022, including Russia’s invasion of Ukraine. Most ransomware groups are linked to eastern Europe, former Soviet republics and Russia in particular, with Chainalysis reporting that some rogue actors were either disrupted or shifted their focus from ransomware to politically motivated cyber-espionage. One major hacker group, Conti, disbanded amid internal upheaval after an anonymous leaker who expressed sympathy for Ukraine released 60,000 internal messages. The FBI also disrupted the Hive ransomware group by capturing its decryption keys and saving victims from making $130m in ransom payments. Chainalysis also cited research showing that attacks last year showed a growth in the number of attackers and ransomware variants. “A major thing we’re seeing is the astronomical growth in the number of threat actors carrying out ransomware attacks,” said Allan Liska, analyst at cybersecurity firm Recorded Future. According to Recorded Future, there were 538 new ransomware variants in 2023, which indicates the emergence of new, independent groups. The Clop group emerged as a significant player last year, claiming responsibility for the hack of the payroll provider Zellis, which targeted a vulnerability in MOVEit software, which is used to transfer files around internal networks. Affected customers included British Airways, Boots and the BBC. The British Library is still recovering from a ransomware attack by a rebranded group, Rhysida, that targeted the institution in October. The library has declined to pay a ransom. The growth of “ransomware as a service”, where malware is hired out to criminals in exchange for a cut of the proceeds has also stoked activity, along with “initial access brokers” who sell vulnerabilities in the networks of potential targets to ransomware attackers. Ellie Ludlam, a partner specialising in

cybersecurity at UK law firm Pinsent Masons, said she expected the increase in attacks to continue. “This increase is expected to continue in 2024 and with an ongoing focus on mass data exfiltration by threat actor groups, which holds the potential for higher ransom payments by impacted companies,” she said.