MAR 22
Gadjo Sevilla

Study: Email, phone calls, and apps like Slack are vulnerable to ransomware

Article

The news: Companies are paying as much as $7 million to resolve ransomware attacks in 2023 as criminals are becoming more invasive and casting wider nets to infect systems with malware, per SiliconAngle.

By the numbers: Cybercriminals employ various techniques to pressure their victims into paying. Harassment and coercion via phone calls and emails have been involved in 20% of ransomware cases investigated by **Palo Alto Networks Unit 42**'s State of Email Security 2023 report.

- **59% of 1,700 chief information security officers** and other IT pros surveyed fear that cyberattacks are not stopping anytime soon and that the attack vectors are growing significantly sophisticated.
- **75% of companies have experienced an increase in email-based threats.** This method has become one of the most prevalent and lucrative cyber threats in recent years.
- **72% of companies expect to be victimized in 2023 by collaboration-tool-based attacks** involving apps like **Microsoft Teams**, **Discord**, **Slack**, or **Kaseya** to deliver malware.

Recent ransomware attacks:

- **The National Basketball Association** informed newsletter subscribers Monday that their data was stolen from an "unnamed third-party provider" that could result in phishing emails.
- **Ferrari** was targeted by a ransomware attack that exposed its customers' names, addresses, email, and phone numbers. The company has not paid the ransom demand, saying that doing so "does not ... change the data exposure."

The impact on companies: The median demand from hackers was **$650,000**, while the median payment was **$350,000**, revealing that effective negotiation can drive down ransom payments.

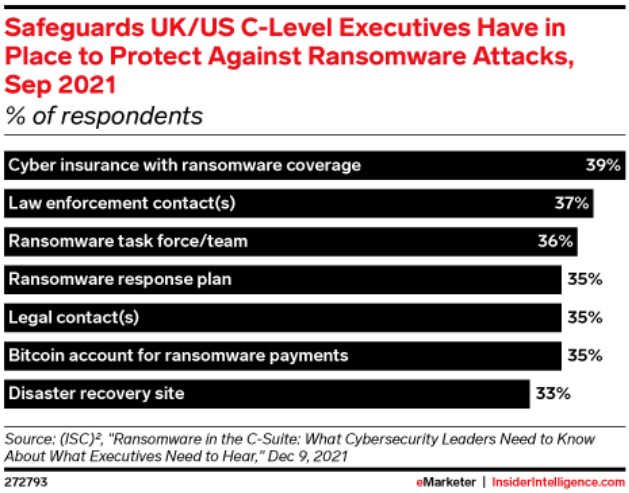
Companies in the US are the most affected, accounting for 42% of leaks in 2022, followed by Germany and the UK with 5% each.

The FBI fights back: The **Federal Bureau of Investigation** said it "hacked the hackers," shutting down Hive2, a major ransomware group responsible for attacking 1,500 companies in over 80 countries since mid-2021, per NPR.

The FBI was also able to provide decryption keys to some victims, saving over **$130 million** in ransom payments.

Key takeaway: The growing aggressiveness and sophistication of recent ransomware attacks reveals criminals are exploiting remote work tools. Agencies are combating the threat, but

more ransomware victims need to report attacks.



This article originally appeared in Insider Intelligence's Connectivity & Tech Briefing—a daily recap of top stories reshaping the technology industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.

- *Are you a client? Click here to subscribe.*
- *Want to learn more about how you can benefit from our expert analysis? Click here.*