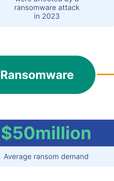
Spin.ai

How Phishing Facilitates Cloud Ransomware Attacks

The State of Ransomware

Ransomware incidents have intensified in recent years, as bad actors and their methods become increasingly sophisticated.



A ransomware attack occurs

EVERY **11** SECONDS

72%

of organizations were affected by a ransomware attack in 2023

The Cost of Ransomware

36%

of organizations that pay the ransom fall victim to ransomware attack for a **second** time

$50million

Average ransom demand

$1.85million

Average cost of recovery in 2023 - not including the ransom itself

Bad Actors are Getting Bolder

62%

increase year-over-year in ransomware incidents in 2022 based on **FBI's Internet Crime Complaint report**.

In 2022, bad actors launched ransomware attacks against

14 of the 16

U.S. critical infrastructure sectors

How Bad Actors Use Phishing to Launch Cloud Ransomware Attacks

Phishers utilize sophisticated emails that spoof internal business communications, right down to visual design and tone of voice, to confuse and deceive their target into opening emails and installing the ransomware.

Step 1

Attackers masquerade as a reputable organization or individual and send emails containing the ransomware using **a spoofed or compromised email account**. They usually gain login credentials through extensive social engineering.

Step 2

The recipient opens the email, **deceived into believing it is legitimate business** communication from a reputable sender. The majority of employees are not trained to recognize possible fraudulent emails containing ransomware and other forms of malware.

Step 3

The victim **unknowingly installs the ransomware** by clicking on a link or downloading a file attached to the email. This one click is all that it takes for ransomware to infect files and systems.

Step 4

Ransomware encrypts the organization's files and systems, rendering them unusable. The average time for a median ransomware variant to encrypt 100,000 files is **42 minutes and 54 seconds.**

Step 5

Bad actors demand a ransom in exchange for decryption along with threats of leaking sensitive, valuable information to the public or selling it to competitors and other interested parties.

Bolster Your Ransomware Protection Now

Secure email channels.

91% of all cyberattacks start with phishing emails. Invest in an enterprise cybersecurity solution that provides advanced email security but also enterprise-level protection for all mission-critical communication and business apps.

Train employees against email-based attacks.

Employee error and negligence are involved in **82%** of all successful breaches. Ensure that your employees receive extensive training to detect potential email attacks and respond appropriately.

Leverage advanced cybersecurity technologies to improve ransomware defense.

Partner with a reliable enterprise cybersecurity provider that delivers comprehensive proactive SaaS ransomware monitoring and fast incident response.