RANSOMWARE ATTACKS ARE ON THE RISE

Ransomware breaches grew by 13% from 2020 to 2021, marking an increase as big as the last five years combined. The average ransom payment in 2021 was $541,000.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious attack carried out by a criminal computer hacker to extort money from individuals and/or organizations. Once successfully installed onto a victim's computer, oftentimes by tricking the user to click on a fraudulent hyperlink, the ransomware encrypts hard drives and locks key system functions, preventing victims from accessing important files or using their computer altogether. The hacker then demands payment (usually in an untraceable, digital currency), threatening to destroy or leak the victim's files if the ransom does not arrive on time. Whereas other cyber-attacks seek to steal data or commandeer a computer in secret, the defining feature of ransomware is extortion.

MAY 2022

Costa Rica became the first country to declare a national emergency in response to a cyber-attack following two major ransomware attacks that had vast consequences paralyzing imports/exports and generating chaos across the healthcare system.

JULY 2021

A software supply chain attack was carried out against Kaseya, an IT solutions developer for managed service providers, impacting over 1,000 companies. The hackers claimed to have encrypted over 1 million systems during the incident.

MAY 2021

The world's largest meat supplier, JBS, paid $11 million in ransom to resolve an attack that forced it to close all of its beef plants throughout the U.S.

MAY 2021

An emergency declaration was issued after the Colonial Pipeline suffered a ransomware attack. Fear of a resulting gas shortage caused the public to "panic-buy" gasoline, triggering an actual shortage in some areas and a spike in prices.

MAY 2017

Cyber criminals exploited a weakness in the Microsoft Windows operating system, targeting around 230,000 computers in 150 countries in an attack known as WannaCry. Recovery is estimated to have cost $4 billion globally.

MARCH 2016

A ransomware known as Petya was released via an email scam, impacting critical infrastructure all over the world. Variations of Petya have caused more than $10 billion in estimated losses.

RANSOMWARE DISRUPTS AN ORGANIZATION'S OPERATIONS AND POSES A SERIOUS DILEMMA.

Does the organization pay the ransom and hope that the attackers are truthful in their promise to restore access?

Does it refuse to pay the ransom and take on the task of attempting to restore operations itself?

***82%** of of cyber breaches involve the human element*

HOW CAN YOU DEFEND AGAINST RANSOMWARE?

- Update software
- Block suspicious email accounts
- Restrict the download of programs that are not pre-approved
- **Provide cybersecurity training to employees**
- Continually back up data (on separate networks or in the cloud)
- Account for ransomware in your incident response strategy

If you fall victim to a ransomware attack, immediately isolate your impacted systems and contact your local FBI field office to report the event and request assistance.

nga.org/ransomware