BANK-OF-AMERICA (RANSOM DATA BREACH)

- RANSOMWARE ATTACK.

- BANK OF AMERICA CORPORATION and Infosys.

IBM

Lock-Bit
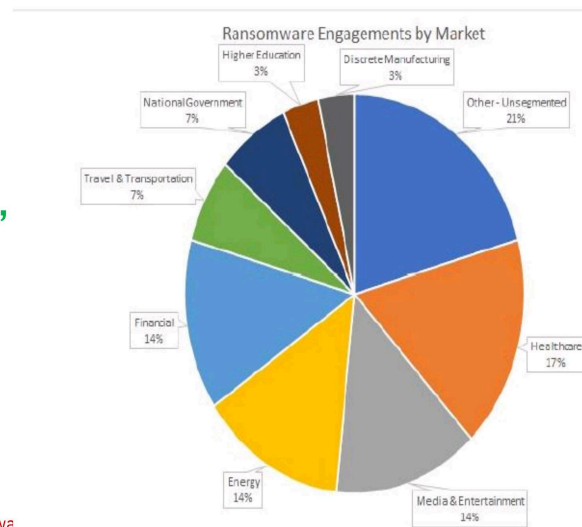# RANSOMWARE

RANSOMWARE :

→

Ransomware is a type of malware that locks and encrypts a victim's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment.
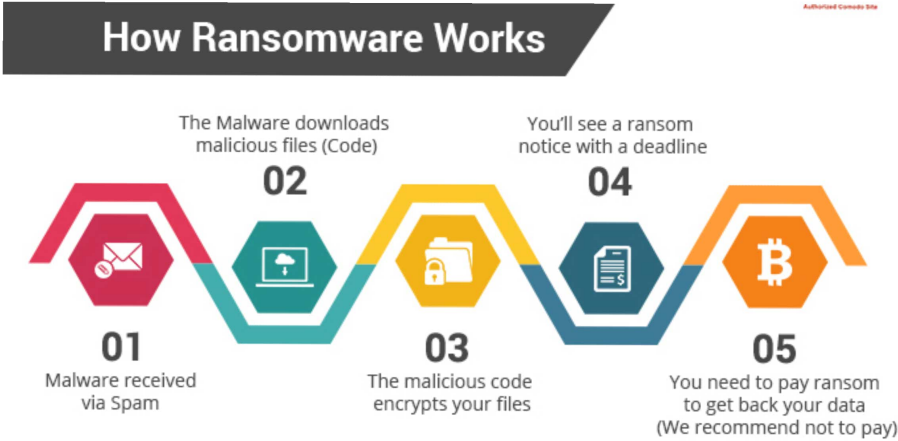
STATISTIC :

→

Ransomware gangs stole more than $1-billion in 2023, The largest amount ever recorded.

Ransomware Engagements by Market

- Higher Education 3%
- Discrete Manufacturing 3%
- National Government 7%
- Other - Unsegmented 21%
- Travel & Transportation 7%
- Financial 14%
- Energy 14%
- Media & Entertainment 14%
- Healthcare 17%

https://news.bloomberglaw.com/crypto/ransomwa
2023#:~:text=Ransomware%20gangs%20stole%20more%20than,blockchain%20analysis%20firm%20Chainalysis%20Inc.

RANSOM ATTACK STEPS

How Ransomware Works

Authorized Comodo Site

01 Malware received via Spam

The Malware downloads malicious files (Code)
02

03 The malicious code encrypts your files

You'll see a ransom notice with a deadline
04

05 You need to pay ransom to get back your data (We recommend not to pay)

•This Data Breach occurred on NOV 3rd 2023.

• BOA is one of the trusted bank and Backed by 164 years in the industry and over $5 billion in assets.

• Infosys BPM is a software based corporation who provided software to run BOA

CASE STUDY:

•BANK OF AMERICA is a clint of INFOSYS INC, McCanish is a software used by BOA provided by Infosys which has software Loop-hole in it.

•A data breach at Infosys McCamish, a financial software provider, compromised Personal information and other account information of 57,028 deferred compensation customers whose accounts were serviced by Bank of America.

•An unauthorized party — apparently a ransomware group known as LockBit accessed the customer's information through Infosys McCamish's system, not Bank of America says reports, The breach occurred Nov 3rd, according to the letter, Infosys McCamish notified Bank of America about the breach on Nov 4th 2024.

•Due to this data breach information like NAME, ADDRESS, E-MAIL, SOCIAL SECURITY NUMBER AND PERSONAL INFO. Has been compromised.

•After this data breach by lockbit group there is no evidence that information has been manipulated or misused.

Timeline actions of BOA and Infosys before and after incident.

1. BOA The put contract at the $42.00 strike price has a current bid of $5.45.

2. Bank of America got hit with massive data breach of customer personal information.

3. BOA has offered free two – years membership to affected customers.

4. In December, Infosys suffered termination of a $1.5 billion deal with an undisclosed global company, focused on artificial intelligence (AI) solutions.

TOOLS & METHODOLOGY

1. N-MAP

network scanner to discover open ports and communication ports.

2. SSH X-COMMAND Scripting

commanding through port to gain administrative access.

Third party risk is the vulnerability in BOA data breach.
Infosys McCanish software is the third party.

VULNERABILITY :

#1
SECURE SHELL (SSH)
(Protection towards ssh is weak.)

#2
DISCOVERABLE OPEN PORTS CONNECTS
SSH.

and lack of authentication in
common.

Bank of America and Infosys financial loss.	Costs	Prevention
	• 1) BOA Loss of Rs 250 crore - ($30 million). • 2) Infosys Loss of `$1.5 billion deal` • 3) Customers trust	• 1) Should update to secure software. • 2) Updating and Upgrading the software and developing secure software without vulnerables. • 3) Compliment to effected customers.

Thank you

By.
-- ERLA SAI THORAN --

IBM