Skillmine
Technology • Consulting • Services

infosec
Miners

RANSOMWARE – A MAJOR THREAT

WHAT IS RANSOMWARE?

Ransomware is a class of malware that is used to digitally extort victims into payment of a specific fee and often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by download occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge. The payload is executed on the target machine, one of the first actions taken is the encryption of the files on the hard drive. The virus then delivers a ransom note demanding payment in exchange for the decryption key of the victim's files.

HOW RANSOMWARE WORKS?

01 Victim receives a malicious link through different modes and user visits the link.

02 The web server of the visited link establishes a connection with victim's machine.

03 Ransomware arrives at the victim's machine and executes itself.

04 The ransomware tries to take over the system and tries to find alternate ways to travel through the network.

05 The ransomware then starts to encrypt the data on the victim's machine.

06 As soon as the data is encrypted it takes over the system completely and denies the user access to it.

07 It then displays the warning and the ransom message on screen.

08 Alongside this, the ransomware tries to spread in network in order to affect more systems.

IMPACT OF RANSOMWARE

01 Ransomware cost the world $20 billion in 2021. That number is expected to rise to $265 billion by 2031.

02 In 2021, 37% of all businesses and organizations were hit by ransomware.

03 Recovering from a ransomware attack cost businesses $1.85 million on average in 2021.

04 Out of all ransomware victims, 32% pay the ransom, but they only get 65% of their data back.

05 Only 57% of businesses are successful in recovering their data using a backup.

Source - https://www.cloudwards.net/

TOP RANSOMWARE ATTACKS OF RECENT TIMES

01

Colonial Pipeline Company:

- In May 2021, Colonial Pipeline Company, an American oil pipeline company, was hit by a significant ransomware assault. The virus impacted the company's computerized equipment that manages the pipeline that originates in Houston, Texas, causing a days-long disruption in fuel supplies to much of the US East Coast.

- Even though the attack only affected its IT systems, Colonial Pipeline Company shut down all its pipeline operations to avoid additional damage. The corporation paid the hackers $4.4 million in bitcoin with the help of the FBI.

02

Acer:

- In March 2021, the Taiwanese computer company Acer was attacked by the REvil ransomware attack. The hackers requested a stunning $50 million in exchange for their information. They released screenshots of stolen files as proof of the security breach & subsequent data leak at Acer. Images of financial spreadsheets, bank correspondence, & bank balances were among them.

03

CNA Financial:

- In March 2021, Chicago-based CNA Financial Corp., one of the country's major insurance businesses, discovered a breach. The ransomware assault is claimed to have exposed the personal information of about 75,000 people. Names, health benefits information, and social security numbers of current and past employees, contract workers, and their dependents might have been included in this data.

- According to media sources, CNA Financial agreed to pay $40 million to regain access to its network later in May. According to reports, the hackers employed Phoenic Locker, a variation of Hades created by the Russian cybercrime gang Evil Corp.

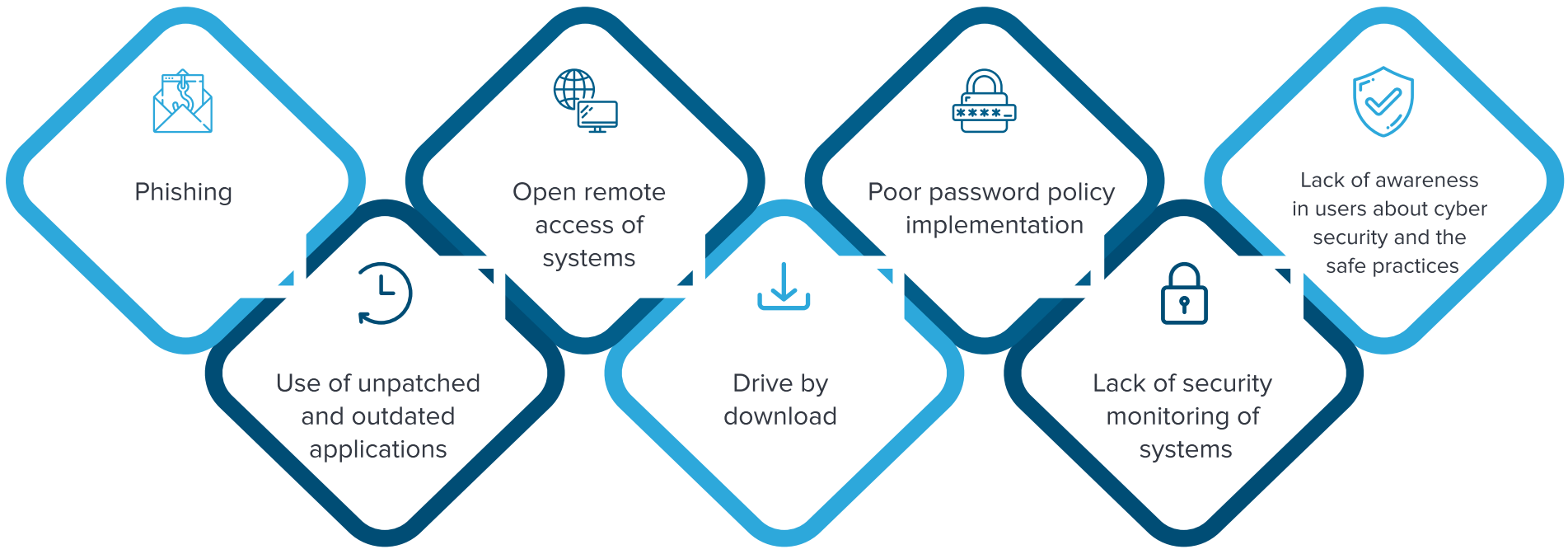
04

Brenntag:

- DarkSide, a hacking organisation based in Germany, targeted Brenntag in May 2021, a chemical delivery firm, around the same time as the Colonial Pipeline Company breach. DarkSide is said to have requested $7.5 million, or 133.65 bitcoin, in exchange for access to 150 GB of data. DarkSide also posted a data breach page with a summary of the data obtained and images of a few files to back up its allegations.

- The ransom was discussed, and Brenntag finally paid $4.4 million.

MAJOR ROOT CAUSES OF RANSOMWARE



HOW YOU CAN SAFEGUARD YOUR ORGANIZATION FROM A RANSOMWARE ATTACK?

Spread awareness and provide training to all the users and stakeholders in your company about basics of cyber security.

Strong security policy against phishing needs to be implemented to eliminate the threat of ransomware attack.

Create strong access policy for systems and data to protect unauthorized access from inside and outside of organization.

Strong infrastructure management policy should be implemented to make sure periodic review of systems, timely patching and updating systems and other applications to the latest release.

Strong web access policy and awareness of users to let them know which things should be accessed over internet and which should not.

Implement strong password policy for all users in an organization.

Implement strong security monitoring system which will monitor every user as well as all the devices present in the organization.

Implement solid data backup solutions to make sure in any circumstances an organization will never lose the data and it can recover the important information as and when required.

- Organizations should consider implementing security policies considering all factors that leads to ransomware attack. Security infrastructure management and monitoring teams should design the security policies keeping protection against ransomware in mind.

- Ransomware is the most dangerous cyber-attack as it focuses on the most important asset of current era that is Data. Data is the new fuel to the economy and if it is lost, it can cause a huge commercial impact on the organization.

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services

India | KSA | UK | USA

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

Stay connected