• What is Ransomware?

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

**Definition**

Types of Ransomwares

- **Crypto**
  - Encrypts valuable files and renders them unusable. Victims pay for the ransom to recover their files.

- **Locker**
  - Locks victim out of their device while encrypting the files. Ransom must be paid to unlock the device.
Ransomware Strains

Top 10 most well-known ransomware strains:

• Petya: Petya encrypts entire computer systems. Petya overwrites the master boot record, rendering the operating system unbootable. It was first observed in 2016.

• NotPetya: Known to be a Petya variant it was first seen in 2016, now classified as a malware known as Viper. It destroys the data instead of obtaining a ransom.

• Ryuk: It is a 2018, strain of malware wreaking havoc on hospitals, governments and municipalities in 2020. Ryuk encrypts business-critical files and demands a high ransom - typically in the multi-millions. It was known to disable windows restore option.

• WannaCry: WannaCry is a ransomware attack that spread across 150 countries in 2017. Designed to exploit a vulnerability in Windows, it was allegedly created by the United States National Security Agency and leaked by the Shadow Brokers group. WannaCry affected 230,000 computers globally.
Ransomware Strains

- **Bad Rabbit**: 2017 Ransomware strain also known as drive-by-attack. Hackers compromised a website where user does not have to take any action but visit the site. Most famous component was fake request to install Adobe flash malware dropper as the infected package.

- **Cryptolocker**: First seen in 2007, passed through a malicious email attachments. Thought to have affected 500,000 computers.

- **GoldenEye**: Encrypts victims entire hard-drive then the files rendering HD incapable. Theorized to be spread through HR departments via fake Job application email with infected Dropbox link. GoldenEye even forced workers at the Chernobyl nuclear plant to check radiation levels manually as they had been locked out of their Windows PCs.

- **Jigsaw**: 2016, Virus strain, Jigsaw gradually deleted more of the victim's files each hour that the ransom demand was left unpaid. Derived from the Saw movie franchise.

- **Locky**: 2016 type, with ability to encrypt over 160 file types, Locky spreads by tricking victims to install it via fake emails with infected attachments.

- **Maze**: 2019, strain: Maze ransomware has quickly made news for being responsible for the release of data belonging to victims, mainly in the healthcare sectors.

And many more.....
The AIDS Trojan, also known as the PC Cyborg virus, was the first ever ransomware virus documented. It was released via floppy disk before most of us ever had the opportunity to touch a computer in 1989.

The AIDS trojan was created by a biologist Joseph Popp who handed out 20,000 infected disks to attendees of the World Health Organization's AIDS conference. The disks were labeled “AIDS Information - Introductory Diskettes” and included leaflets that warned that the software would “Adversely affect other program applications” and also stated, “you will owe compensation and possible damages to PC Cyborg Corporation and your microcomputer will stop functioning normally.”
Some known Ransomware as Service (RaaS) organization names…

<table>
<thead>
<tr>
<th>Place</th>
<th>RaaS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Avaddon RaaS Operator(s)</td>
</tr>
<tr>
<td>2</td>
<td>Conti RaaS Operator(s)</td>
</tr>
<tr>
<td>3</td>
<td>REvil/Sodinokibi RaaS Operator(s)</td>
</tr>
<tr>
<td>4</td>
<td>Mespinoza/Pysa RaaS Operator(s)</td>
</tr>
<tr>
<td>5</td>
<td>Babyk RaaS Operator(s)</td>
</tr>
</tbody>
</table>
Ransomware Stats in Brief

Annual number of ransomware attacks worldwide from 2014 to 2020 (in millions)

Ransomware remains one of the major threats in business continuity and availability. There is a reduction in recent years on number of attacks, but the attacks are on critical assets.

Reference: Statista(1)
Ransomware Stats in Brief

Based on the Sophos research - The State of Ransomware 2021

Sophos commissioned an independent research house Vanson Bourne to survey 5400 IT decision makes across 30 countries from all sectors. The survey was carried over January and February 2021.

- 37% of respondents’ organizations were hit by ransomware in the last year
- 54% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack
- 96% of those whose data was encrypted got their data back in the most significant ransomware attack
- The average ransom paid by mid-sized organizations was US$170,404
- However, on average, only 65% of the encrypted data was restored after the ransom was paid
- The average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was US$1.85 million
- Having trained IT staff who can stop attacks is the most common reason some organizations are confident they will not be hit by ransomware in the future.

Reference: Sophos Research and Survey[2]
Ransomware Stats in Brief

Based on the Sophos research - The State of Ransomware 2021

Sophos commissioned an independent research house Vanson Bourne to survey 5400 IT decision makes across 30 countries from all sectors.

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th># RESPONDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>250</td>
</tr>
<tr>
<td>Austria</td>
<td>100</td>
</tr>
<tr>
<td>Belgium</td>
<td>100</td>
</tr>
<tr>
<td>Brazil</td>
<td>300</td>
</tr>
<tr>
<td>Canada</td>
<td>200</td>
</tr>
<tr>
<td>Chile</td>
<td>200</td>
</tr>
<tr>
<td>Colombia</td>
<td>200</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>100</td>
</tr>
<tr>
<td>France</td>
<td>200</td>
</tr>
<tr>
<td>Germany</td>
<td>300</td>
</tr>
<tr>
<td>India</td>
<td>300</td>
</tr>
<tr>
<td>Israel</td>
<td>100</td>
</tr>
<tr>
<td>Italy</td>
<td>200</td>
</tr>
<tr>
<td>Japan</td>
<td>300</td>
</tr>
<tr>
<td>Malaysia</td>
<td>150</td>
</tr>
<tr>
<td>Mexico</td>
<td>200</td>
</tr>
<tr>
<td>Netherlands</td>
<td>150</td>
</tr>
<tr>
<td>Nigeria</td>
<td>100</td>
</tr>
<tr>
<td>Philippines</td>
<td>150</td>
</tr>
<tr>
<td>Poland</td>
<td>100</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>100</td>
</tr>
<tr>
<td>Singapore</td>
<td>150</td>
</tr>
<tr>
<td>South Africa</td>
<td>200</td>
</tr>
<tr>
<td>Spain</td>
<td>150</td>
</tr>
<tr>
<td>Sweden</td>
<td>100</td>
</tr>
<tr>
<td>Switzerland</td>
<td>100</td>
</tr>
<tr>
<td>Turkey</td>
<td>100</td>
</tr>
<tr>
<td>UAE</td>
<td>100</td>
</tr>
<tr>
<td>U.K.</td>
<td>300</td>
</tr>
<tr>
<td>U.S.</td>
<td>500</td>
</tr>
</tbody>
</table>

How many employees does your organization have globally?

- 100 - 250 employees
- 251 - 500 employees
- 501 - 1,000 employees
- 1,001 - 3,000 employees
- 3,001 - 5,000 employees

Within which sector is your organization?

- IT, technology & telecoms
- Financial services
- Education
- Manufacturing & production
- Retail
- Business & professional services
- Healthcare
- Construction & property
- Distribution & transport
- Energy, oil/gas & utilities
- Media, leisure & entertainment
- Local government
- Central government & NDPB
- Other

- 996
- 550
- 499
- 438
- 435
- 361
- 328
- 232
- 203
- 197
- 145
- 131
- 117
- 768
Ransomware Stats in Brief

- 37% of respondents’ organizations were hit by ransomware in the last year
- 54% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack
- The average ransom paid by mid-sized organizations was US$170,404
- However, on average, only 65% of the encrypted data was restored after the ransom was paid
- The average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was US$1.85 million

<table>
<thead>
<tr>
<th></th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>73%</td>
<td>54%</td>
<td>Cybercriminals succeeded in encrypting data</td>
</tr>
<tr>
<td>24%</td>
<td>39%</td>
<td>Attack stopped before the data could be encrypted</td>
</tr>
<tr>
<td>3%</td>
<td>7%</td>
<td>Data not encrypted but victim still held to ransom</td>
</tr>
</tbody>
</table>

Did the cybercriminals succeed in encrypting your organization’s data in the most significant ransomware attack? [2021=2,006, 2020=2,538] organizations that had been hit by ransomware in the last year
Recent Ransomware Attacks

• State-Sponsored Attacks:
  • A reputed cybersecurity firm Flashpoint reported that “Iran’s Islamic Revolutionary Guard Corps (IRGC)” was operating a state-sponsored ransomware campaign through an Iranian contracting company called ‘Emen Net Pasargard (ENP)’.
  • The cybersecurity firm’s analysis was based on three documents leaked by an anonymous entity named Read My Lips, or Lab Dookhtegan, between March 19 and April 1, 2021.
  • Potentially financially motivated, but more likely using the appearance of financial motivation as a cover.
  • Operation overlapped with deployment of Iranian state-sponsored Pay2Key ransomware targeting Israeli companies.
Recent Ransomware Attacks

- Darkside-Colonial Pipeline Attack:
  - DarkSide operates a "ransomware-as-a-service" (RaaS) model
  - Attack resulted in payment of $4.4 million in ransom
  - Disruption to payment collection system led to shutdowns
  - Perceived gas shortage led to stockpiling and panic

Resource on how Darkside works technically (some forensics): https://www.nozominetworks.com/blog/colonial-pipeline-ransomware-attack-revealing-how-darkside-works
Recent Ransomware Attacks

- **Solarwinds:**
  - Ongoing research and investigation suggests involvement on Russian Hackers similar to NotPetya.
  - Attack resulted in breach of major government agencies including up to White House
  - Compromising a security and IT tool made it easy to propagate

Dec-8 and 13: FireEye revealed they were victim to nation-state attack. It was discovered to be a supply chain attack and backdoor Trojan was used to deploy the malware. FireEye named it “Sunburst”.

December 15-January 19: Microsoft says the Russian attackers breached some of its source code. Solarwinds issues advisory on Sunburst and Supernova

December 14-17: Solarwinds requests its customer to upgrade to Orion Platform version 2020.2.1 HF 1 to address a security vulnerability. WSJ reveals more names of the victims setting timeline back to March 2020

March 28-May 19: Reports states DHS cybersecurity leaders’ emails compromised. Microsoft reports new wave of attacks by the Russia-affiliated Nobelium gang now linked to the SolarWinds hack.

March 30-5: Reports states reports of a SolarWinds hack. SolarWinds issues advisory on Sunburst and Supernova

Today: Investigation is still going on...
Recent Ransomware Attacks

- Kaseya
  - Week of July 4th, 2021, cybercriminals deployed ransomware to 1,500 organizations, including many that provide IT security and technical support to other companies. Disruption to payment collection system led to shutdowns.
  - REvil RaaS accepts the responsibilities of the attack.
  - July 3rd, Revil starts deploying zero-day security hole (CVE-2021-30116) to deploy ransomware to hundreds of IT management companies running Kaseya’s remote management application Virtual System Administrator (VSA).
  - This is due to a known vulnerability from 2015 which Kaseya did not patch.
  - Still, Kaseya has yet to issue an official patch for the flaw Boonstra reported in April. Kaseya on July 7th that it was working “through the night” to push out an update.

- The REvil ransomware group said affected organizations could negotiate independently with them for a decryption key, or someone could pay $70 million worth of virtual currency to buy a key that works to decrypt all systems compromised in this attack.

In Recent News:
- Guess announces breach of employee SSNs and financial data after DarkSide ransomware attack
- REvil: Ransomware gang websites disappear from internet
Mitigation and Incident Response

- Require multi-factor authentication for remote access to OT and IT networks.
- Enable strong spam filters to prevent phishing emails from reaching end users. Filter emails containing executable files from reaching end users.
- Implement a user training program and simulated attacks for spear phishing to discourage users from visiting malicious websites or opening malicious attachments and re-enforce the appropriate user responses to spear phishing emails.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL block lists and/or allow lists.
- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.

3-2-1 Backup Rule

1. Copy stored offsite (in the modern digital age, this is recommended to be in the cloud)
2. Copies stored on different storage media/devices
3. Copies of data
Mitigation and Incident Response

- **Limit access to resources over networks, especially by restricting RDP.** After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multi-factor authentication.

- **Set anti-virus/anti-malware programs to conduct regular scans of IT network assets using up-to-date signatures.** Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.

- **Implement unauthorized execution prevention by:**
  - Disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
  - Implementing application allow-listing, which only allows systems to execute programs known and permitted by security policy.
  - Monitor and/or block inbound connections from Tor exit nodes and other anonymization services.
  - Deploy signatures to detect and/or block inbound connection from Cobalt Strike servers and other post exploitation tools.

If your organization is impacted by a ransomware incident:

- Isolate the infected system.
- Turn off other computers and devices. Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware.
- Take an image snapshot from the earliest available period before the attack and try to sandbox and generate signature hash.
- Validate the hash with known threat vectors and update SIEM and other perimeter security to detect and prevent the attack.
Questions
thank you!

This Photo

CC BY-NC
Appendix

• References:
  6. https://www.youtube.com/watch?v=EkL4jJQ6F7w&ab_channel=KevinGergely
  8. https://www.cisa.gov/stopransomware