RANSOMWARE

IMPACT AND STATE IN 2021

PRESENTED BY: DHRUV PANDYA, MS

DATE: 07/14/2021

FOR: IEEE BUENAVENTURA SECTION

CONTENTS

DEFINITION

VARIANTS

TIMELINE

RANSOMWARE STATS IN BRIEF

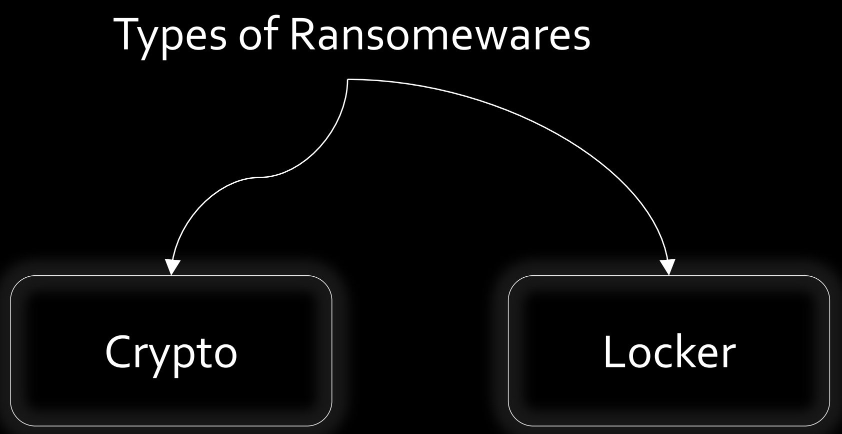
RECENT RANSOMWARES

MITIGATION AND INCIDENT RESPONSE

Definition

- 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



Types of Ransomewares

Crypto

Locker

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

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.

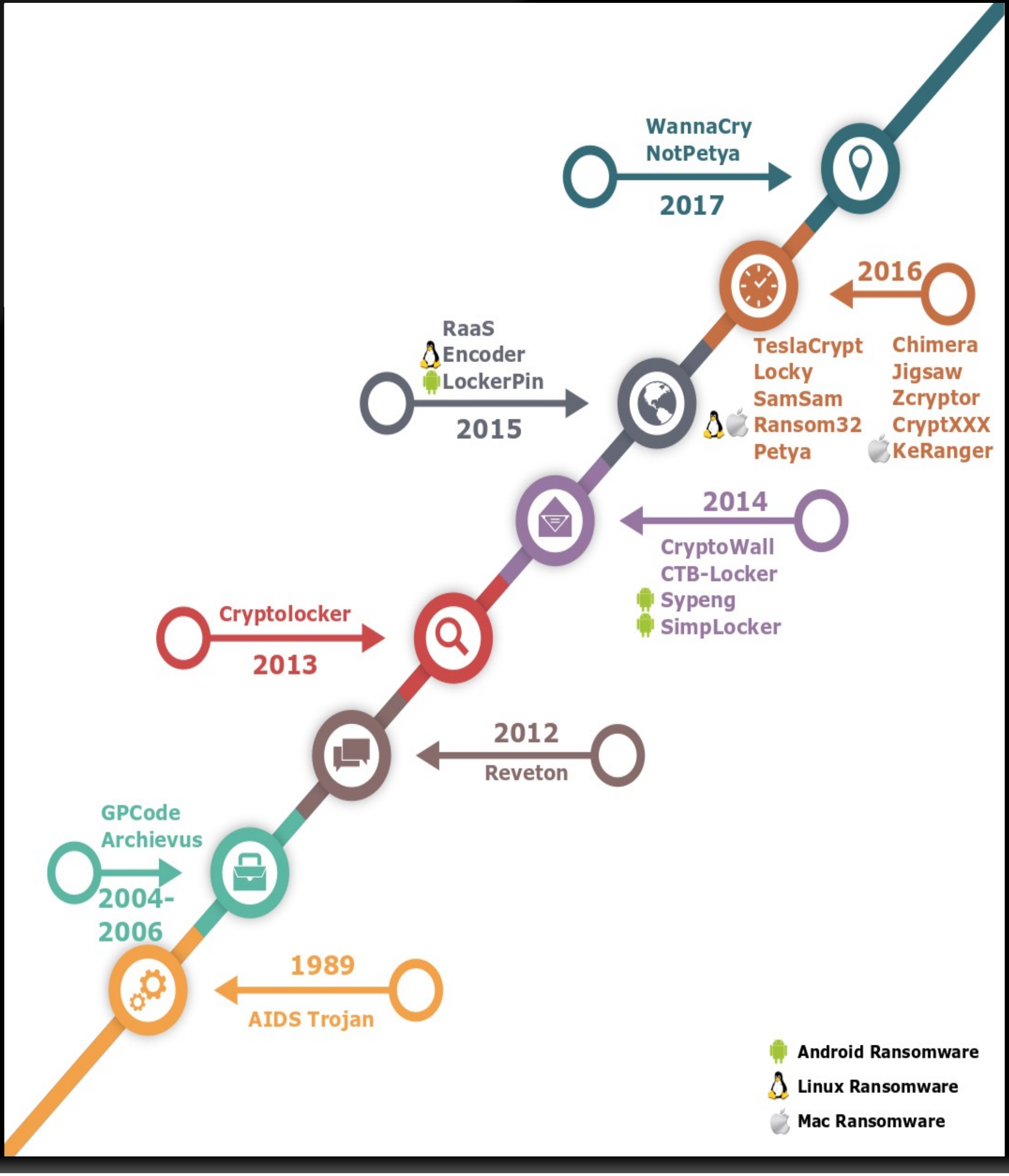
- Wannacry: WannaCry is a ransomware attack that spread across 150 countries in 2017. Designed to exploit a vulnerability in Windows, it was allegedly created by the United States National Security Agency and leaked by the Shadow Brokers group. WannaCry affected 230,000 computers globally.

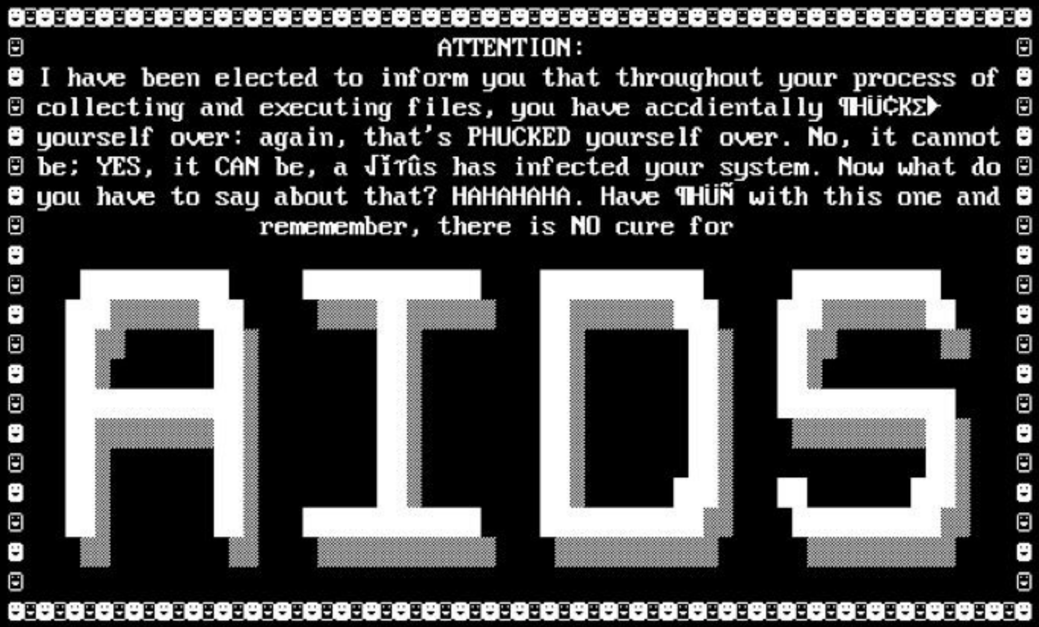
Ransomware Strains

- 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 500,00 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.....

Ransomware Crucial Timeline



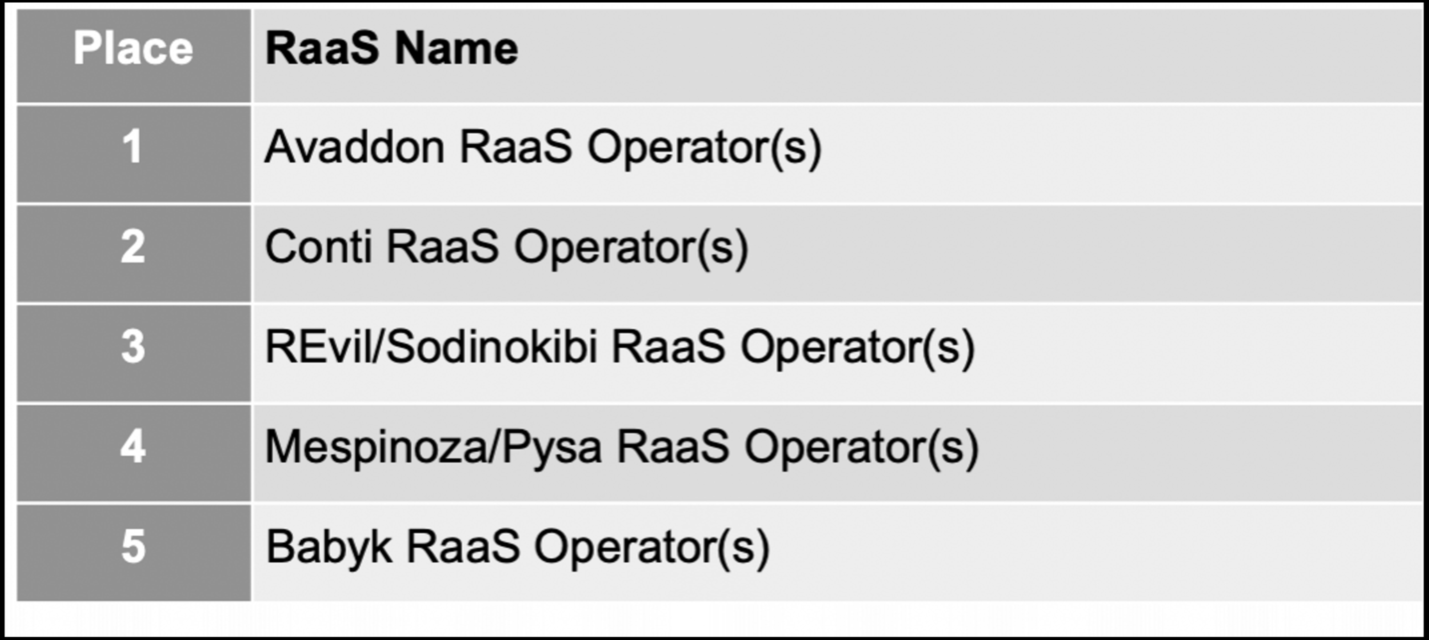


```
ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accdientally ¶HÜÇKΣ▶
yourself over: again, that's PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a √ïrûs has infected your system. Now what do
you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and
remember, there is NO cure for

AIDS
```

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."

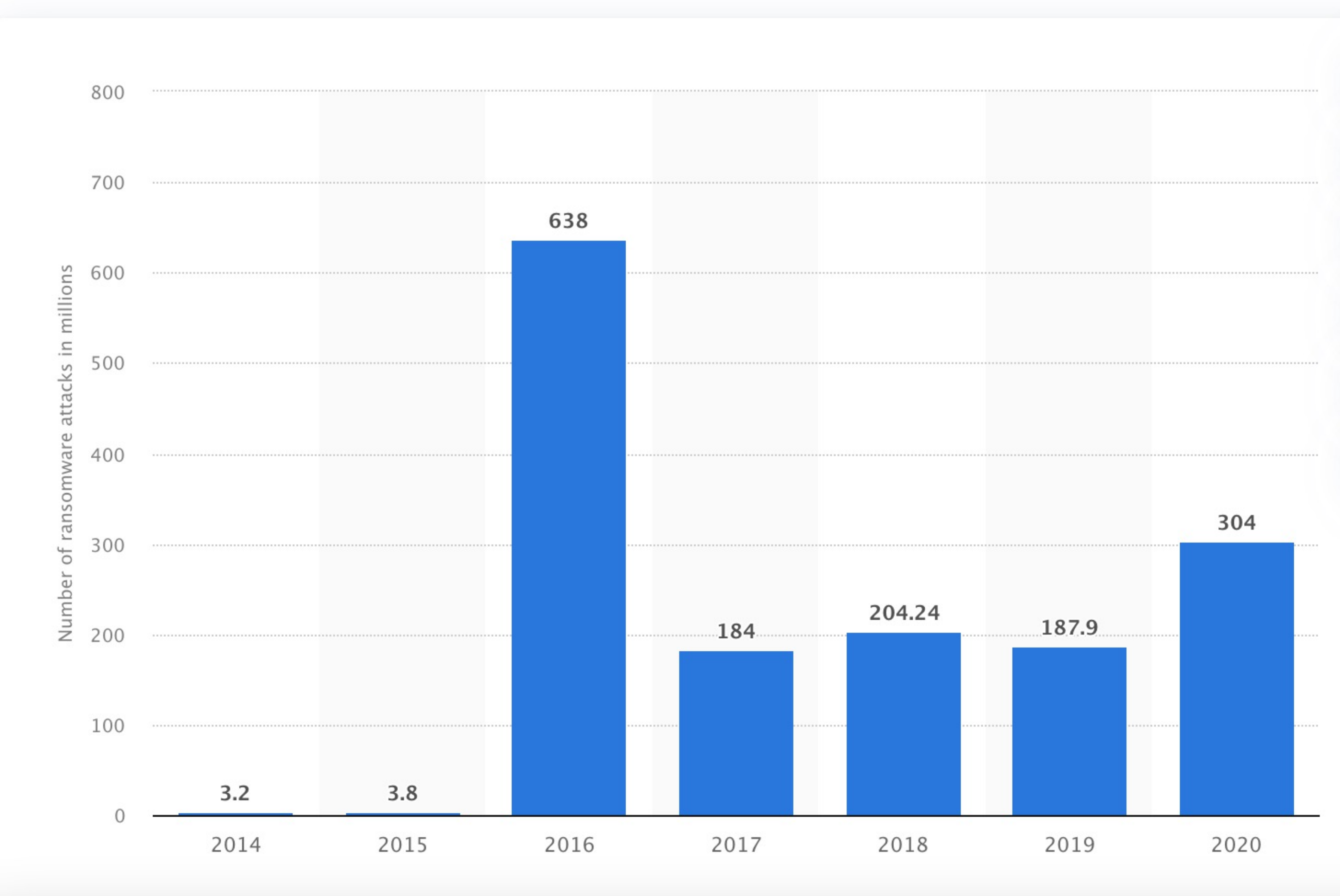
Some known Ransomware as Service (RaaS) organization names…



Place	RaaS Name
1	Avaddon RaaS Operator(s)
2	Conti RaaS Operator(s)
3	REvil/Sodinokibi RaaS Operator(s)
4	Mespinoza/Pysa RaaS Operator(s)
5	Babyk RaaS Operator(s)

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.

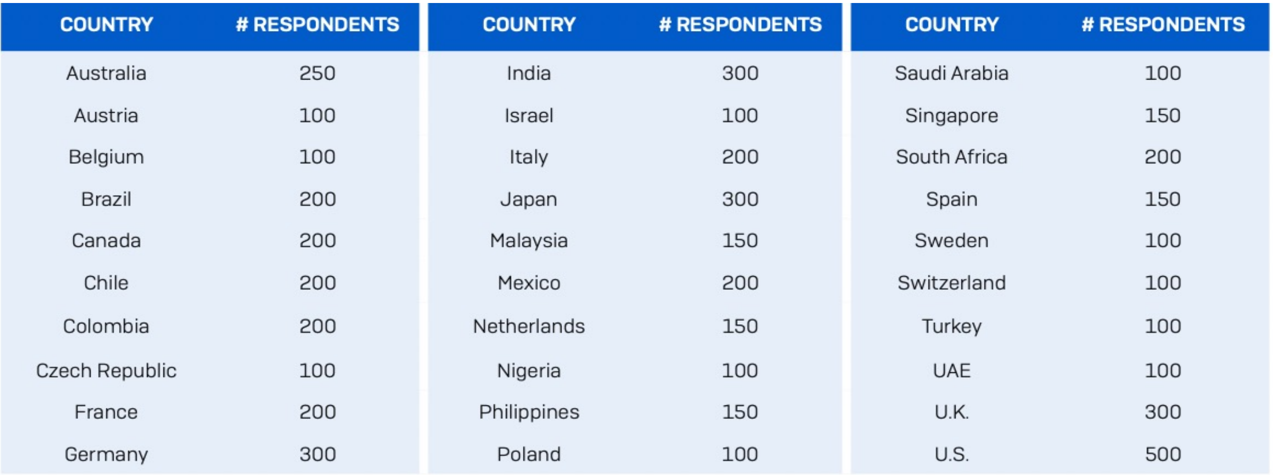
- **37%** of respondents' organizations were hit by ransomware in the last year
- **54%** that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack
- **96%** of those whose data was encrypted got their data back in the most 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)

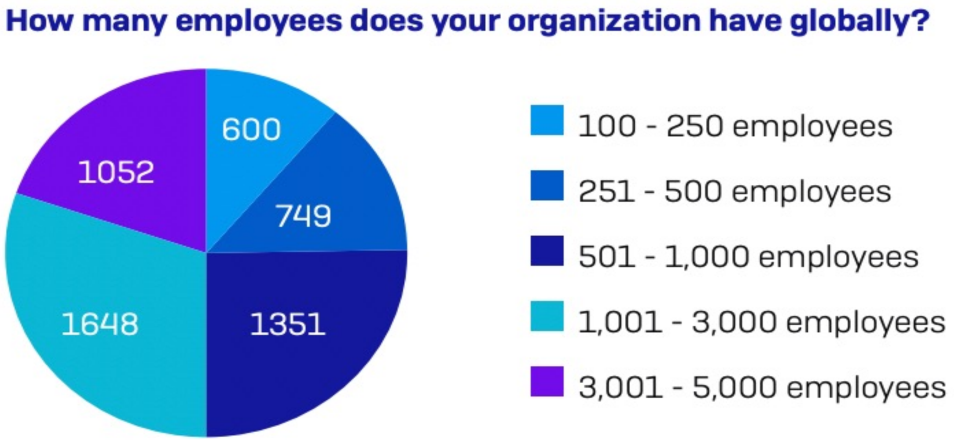
Ransomware Stats in Brief

Based on the Sophos research- The State of Ransomware 2021

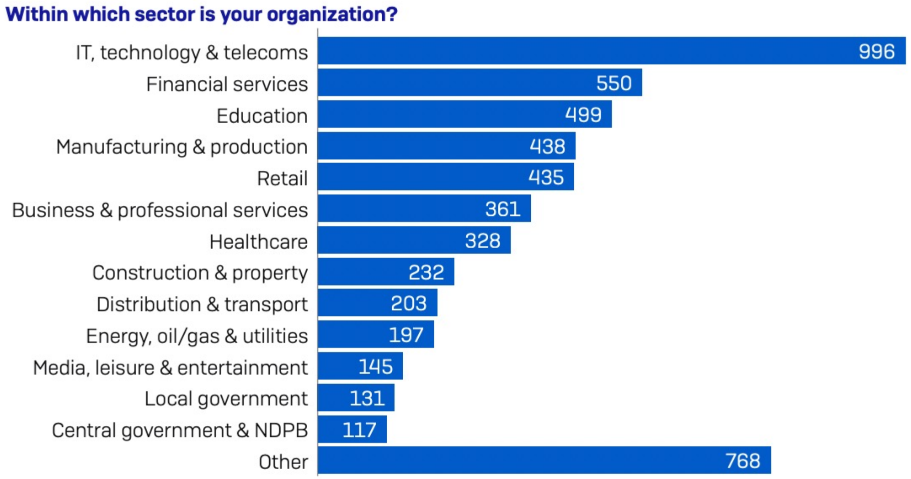
Sophos commissioned an independent research house Vanson Bourne to survey 5400 IT decision makes across 30 countries from all sectors.



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



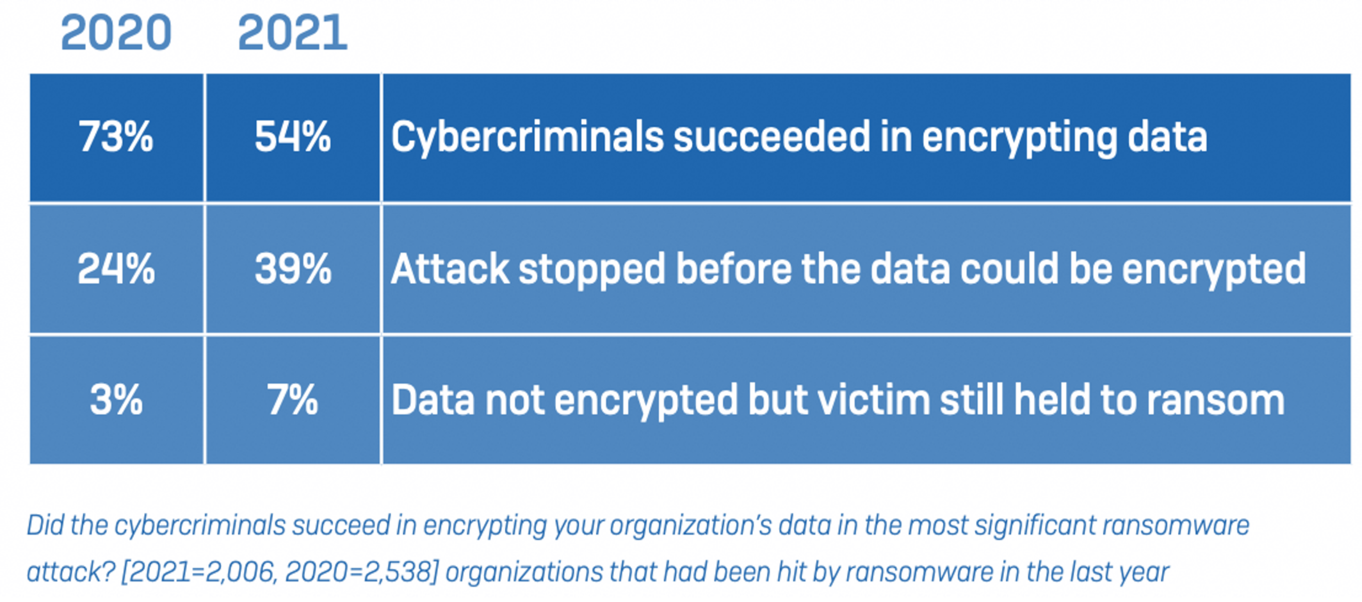
How many employees does your organization have globally?



Within which sector is your organization?

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***

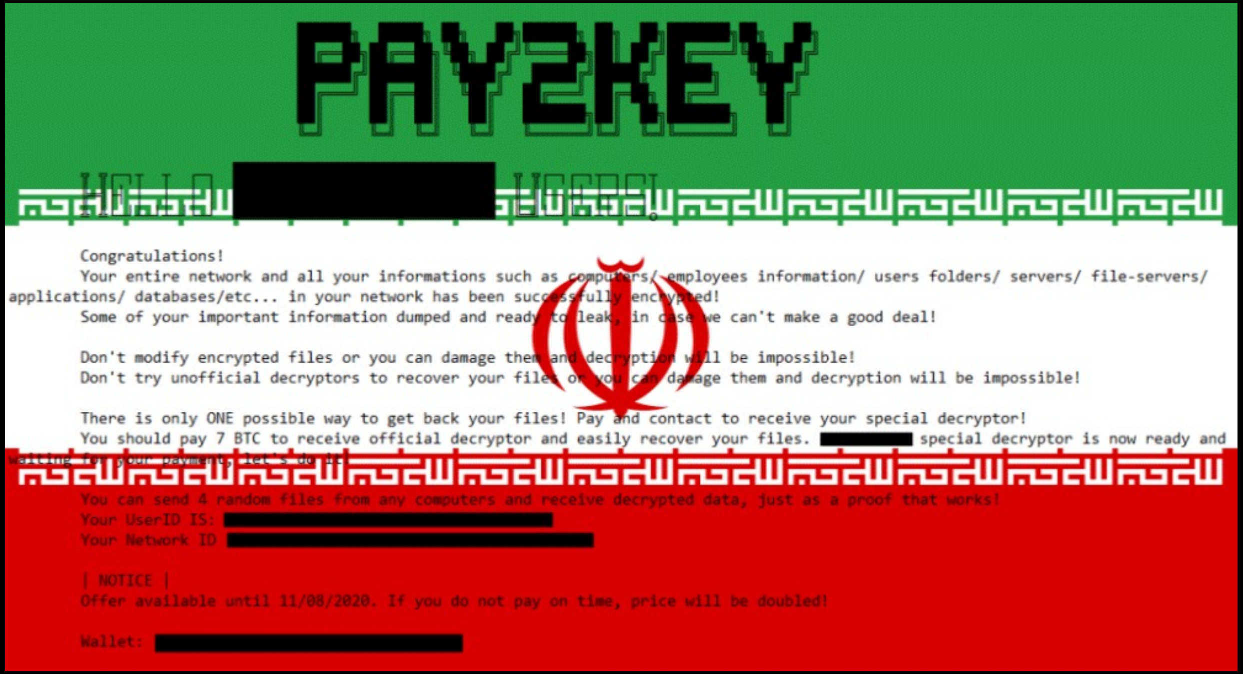


2020	2021	
73%	54%	Cybercriminals succeeded in encrypting data
24%	39%	Attack stopped before the data could be encrypted
3%	7%	Data not encrypted but victim still held to ransom

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.

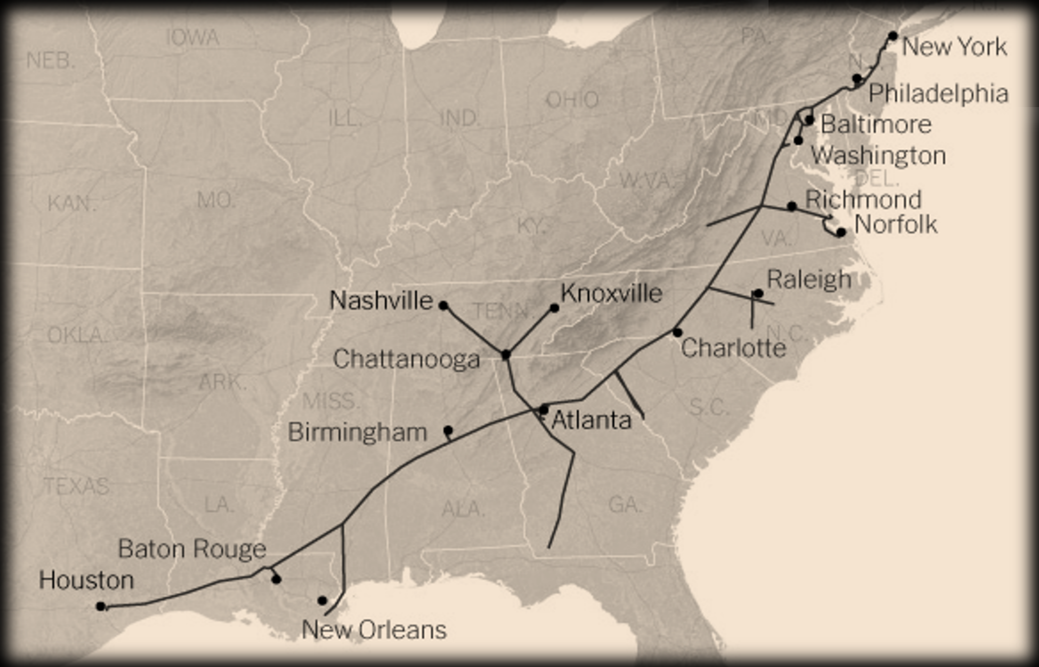


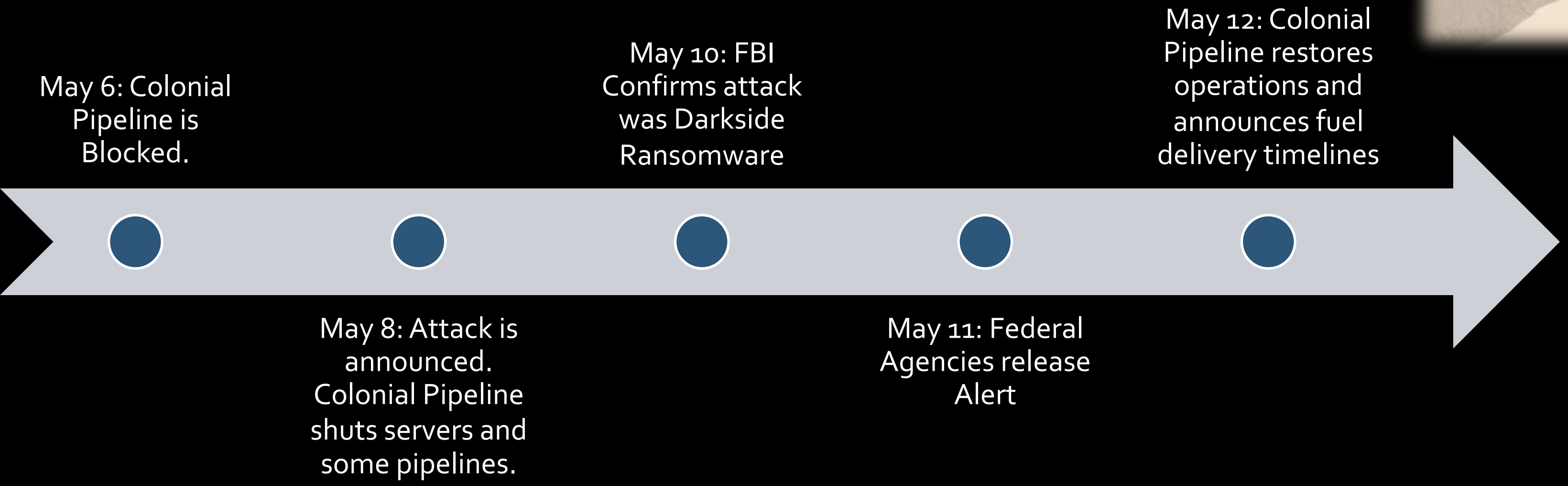
HELLO [redacted] USERS!

```
        Congratulations!
        Your entire network and all your informations such as computers/ employees information/ users folders/ servers/ file-servers/
applications/ databases/etc... in your network has been successfully encrypted!
        Some of your important information dumped and ready to leak, in case we can't make a good deal!

        Don't modify encrypted files or you can damage them and decryption will be impossible!
        Don't try unofficial decryptors to recover your files or you can damage them and decryption will be impossible!

        There is only ONE possible way to get back your files! Pay and contact to receive your special decryptor!
        You should pay 7 BTC to receive official decryptor and easily recover your files. [redacted] special decryptor is now ready and
waiting for your payment, let's do it!
        You can send 4 random files from any computers and receive decrypted data, just as a proof that works!
        Your UserID IS: [redacted]
        Your Network ID [redacted]

        | NOTICE |
        Offer available until 11/08/2020. If you do not pay on time, price will be doubled!

        Wallet: [redacted]
```

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





May 6: Colonial Pipeline is Blocked.

May 8: Attack is announced. Colonial Pipeline shuts servers and some pipelines.

May 10: FBI Confirms attack was Darkside Ransomware

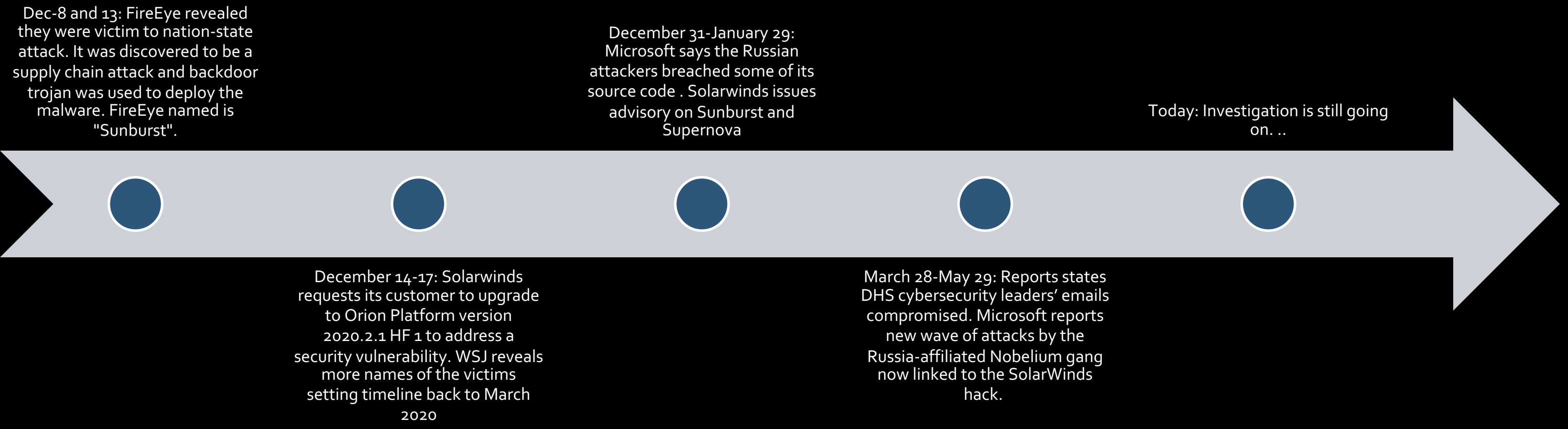
May 11: Federal Agencies release Alert

May 12: Colonial Pipeline restores operations and announces fuel delivery timelines

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 is "Sunburst".

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

December 31-January 29: Microsoft says the Russian attackers breached some of its source code . Solarwinds issues advisory on Sunburst and Supernova

March 28-May 29: 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.

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 7 that it was working "through the night" to push out an update.

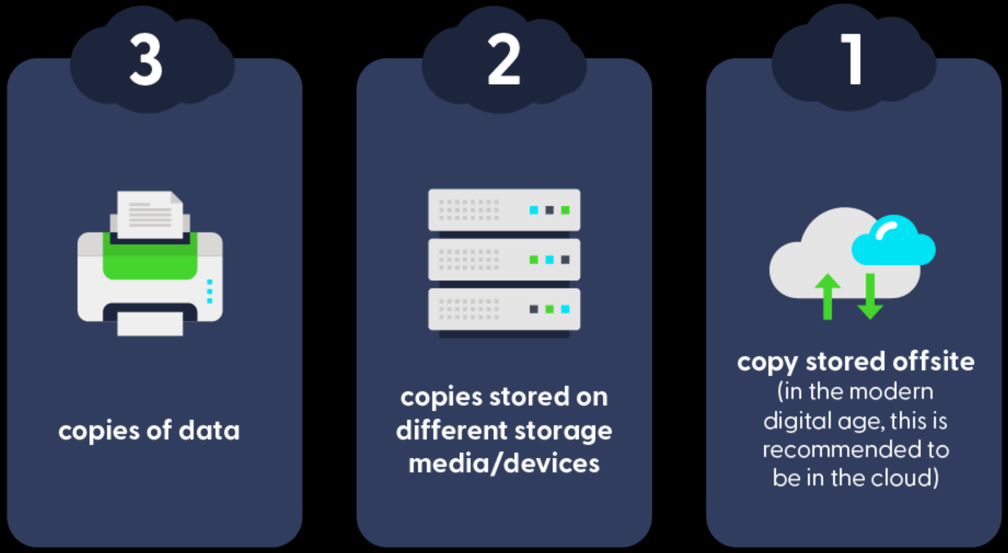
  - The REvil ransomware group said affected organizations could negotiate independently with them for a decryption key, or someone could pay $70 million worth of virtual currency to buy a key that works to decrypt all systems compromised in this attack.

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

copies of data

2

copies stored on different storage media/devices

1

copy stored offsite
(in the modern digital age, this is recommended to be in the cloud)

3-2-1 Backup Rule

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

This Photo CC BY-NC

Appendix

- References:

1. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ Statista Research
2. https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf, Sophos Survey and Research
3. https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html State Sponsored Attack Information
4. https://www.nozominetworks.com/blog/colonial-pipeline-ransomware-attack-revealing-how-darkside-works/
5. https://www.bbc.com/news/technology-57826851
6. https://www.youtube.com/watch?v=EkL1JjQ6F7w&ab_channel=KevinGergely
7. https://www.knowbe4.com/aids-trojan
8. https://www.cisa.gov/stopransomware
9. https://www.forbes.com/sites/servicenow/2021/06/09/the-destructive-rise-of-ransomware-as-a-service/?sh=3189a731e16c