AMERICAN INTERNATIONAL UNIVERSITY-BANGLADESH

Course: Network Security

Course Faculty:

MD. MANIRUL ISLAM

Section: (A)

Final Term Theory Assingment

Student Name:

ISMAIL HOSSAIN PRANTO

ID: 19-41088-2

QUESTION:

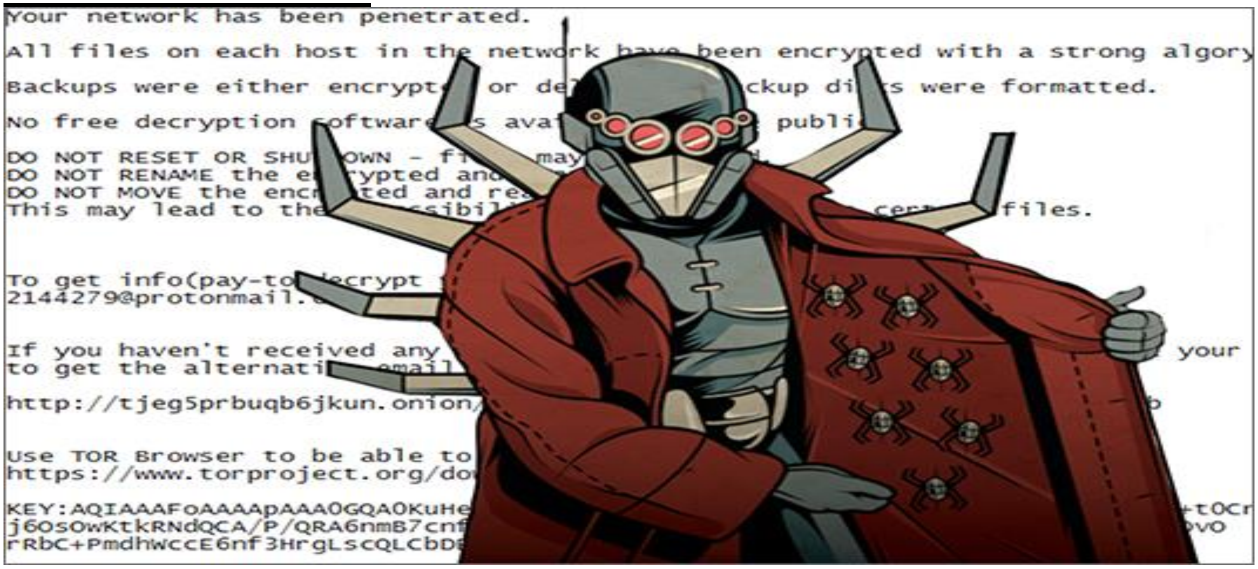
Reports of cyber security failures appear frequently on daily news. Perform a research on 2 (two) ransomware attack that has happened within the last two years, then write a short report with the following main headings:

- Attack Summary
- Exploited Vulnerability
- Remedy Actions Taken
- Recommended Future Mitigation Strategy

Include appropriate figures and tables where applicable. Also, make sure to cite your sources appropriately.

ANSWER:

Ransomware Attack: 1



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algory

Backups were either encrypt   or de      ckup di  s were formatted.

No free decryption software  s avai          publi

DO NOT RESET OR SHU  OWN - fi      may
DO NOT RENAME the e  rypted and
DO NOT MOVE the encr  ted and re
This may lead to the   ssibil               cer     files.


To get info(pay-to decrypt
2144279@protonmail.

If you haven't received any                                            your
to get the alternati    email

http://tjeg5prbuqb6jkun.onion/                                         b

Use TOR Browser to be able to
https://www.torproject.org/do

KEY:AQIAAAFoAAAApAAA0GQA0KuHe                                          +t0Cr
j6OsOwKtkRNdQCA/P/QRA6nmB7cnf                                          bvO
rRbC+PmdhwccE6nf3HrgLscQLCbD
```

- **Attack Summary:**

Cyber attacks hit over 200 organizations including Bangladesh Bank, BTRC

[Records Exposed: 200 | Source: Online Newspaper | Site name: **DhakaTribune** | Type of Ransomeware attack: **SPIDER**]

- **Exploited Vulnerability:**

On Friday April 2nd, 2021, A huge number of Data has been leaked. Which creates a big number of financial chances of loss due to the “SPIDER” Ransomware which is one kind of malware. A malware was inserted through Microsoft Exchange Server.

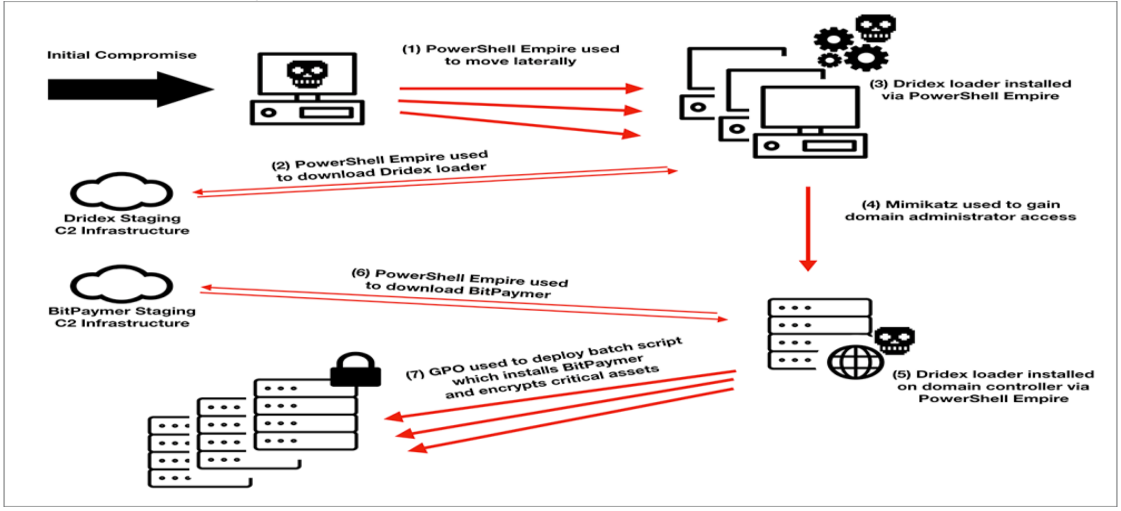
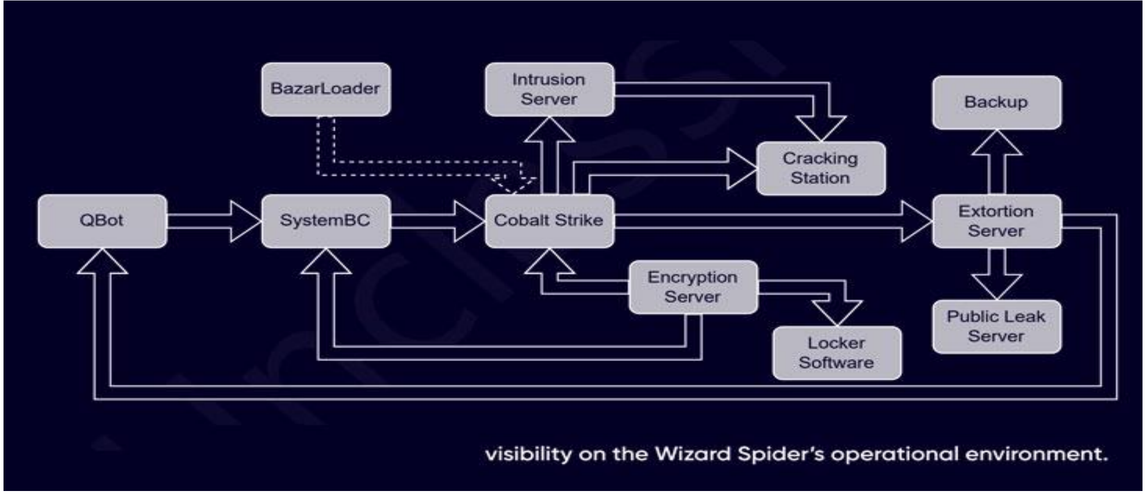

Initial Compromise
(1) PowerShell Empire used to move laterally
(3) Dridex loader installed via PowerShell Empire
(2) PowerShell Empire used to download Dridex loader
Dridex Staging C2 Infrastructure
(4) Mimikatz used to gain domain administrator access
(6) PowerShell Empire used to download BitPaymer
BitPaymer Staging C2 Infrastructure
(7) GPO used to deploy batch script which installs BitPaymer and encrypts critical assets
(5) Dridex loader installed on domain controller via PowerShell Empire

Fig: Spider malware attcak process

Ransomware attack is a process basically initial to last here we have discussed about

The BCC and project director, BGD e-Gov CIRT, told the Dhaka Tribune that they were just trying to see a global attack a global attack after that through research they known that the “HAFNIUM” group was attacked them. Though behind the situation it has several groups with the help of Microsoft Exchange server.



- **Remedy Actions Taken:**

  The company has decided to take action against the attack by using “Hafnium exploit file”. The BGD e-GOV CIRT has asked a number of state and private organizations to do a scan of all the mail servers if in this here any Ransomware is infected or not.

After that according to the Chinese group of hackers they should to increase the tactics and the technique to defend the Ransomware. Then BCC said that if they establish an exact match with another known group, then they will supplement it with their profile. On 15 March the bank of Chile has compromised through Proxy Logon vulnerabilities in

Marcroft Exchange Server with the respect of the Comision Para El Mercado Financiero (CMF).

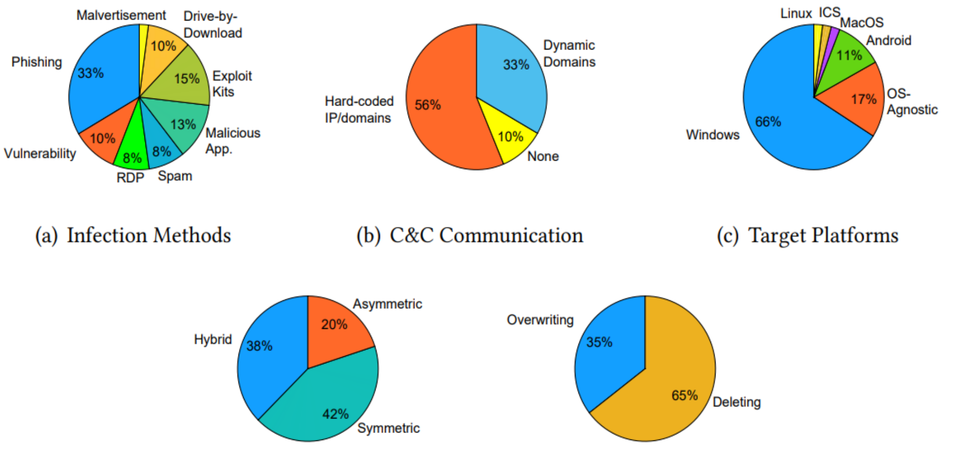
Some of the Bangladeshi Company and organizations are running the Microsoft Exchange Server it also should be compromised by the Cyber-attack like Ransomware attack. (Said BGD e-Govt CIRT in an advisory)

All the organizations should use newly developed tools- Such as Microsoft's "Test-ProxyLogon.ps1 script" and then Safety Scanner "MSERT" to ensure whether their Microsoft Exchange servers are safe or not. (Said BGD e-Gov CIRT)

Always use strong password and always restrict the permission to install unknown software (Said the advisory)

- **Recommended Future Mitigation Strategy:**

If any email comes from the sender, if the attachment is known to the sender and if it is expected, then it should be opened otherwise not. That will be a good one for future activities. Always maintain up-to-date antivirus and the engine also, keep operating system patches up-to-date and the files also. As if in future any of the Ransomware and malware cannot attack. Then the company decided on the future plan that is using "Hafnium Exploit file". And then should established a exact match for the future prediction. Also, you should use Microsoft exchange service which is Comision para El Mercado Financiero (CMF). If it is possible Isolate all the infected files. Also, in future always up-to-date all the software. Paid the Ransom or the fine of the information data it is not ok. We all should get rid of it.



(a) Infection Methods (b) C&C Communication (c) Target Platforms

(d) Encryption Techniques (e) Destruction Methods

Figure: Pie chart distribution of infection

The ratio for OS-agostic ransomware may increase in the following years.
In this pie chart taught about infection method and the C&C Communication and then Target Platforms,
Encryption Techniques, Destruction method.
Here, most of the user are from windows user. They are affected by the ransomware. (a) Infected Site is higher phising site affection happened.Malvertisement is the lowest. Then the second lowest is RDP and spam.

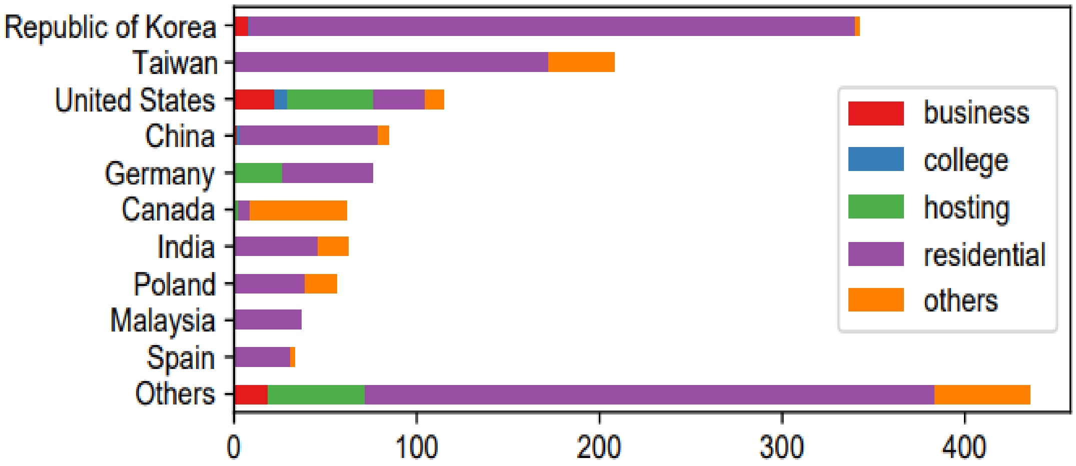


Fig: Number of infected by ransomware IP addresses across countries and ISP types.

The higher number of residential in korea. Then the lowest number is Canada , mid number in germany.

References:

https://archive.dhakatribune.com/bangladesh/2021/04/02/cyber-attacks-hit-over-200-organizations-including-bangladesh-bank-btrc

https://www.datto.com/blog/common-types-of-ransomware]

https://www.cirt.gov.bd/incident-reporting/

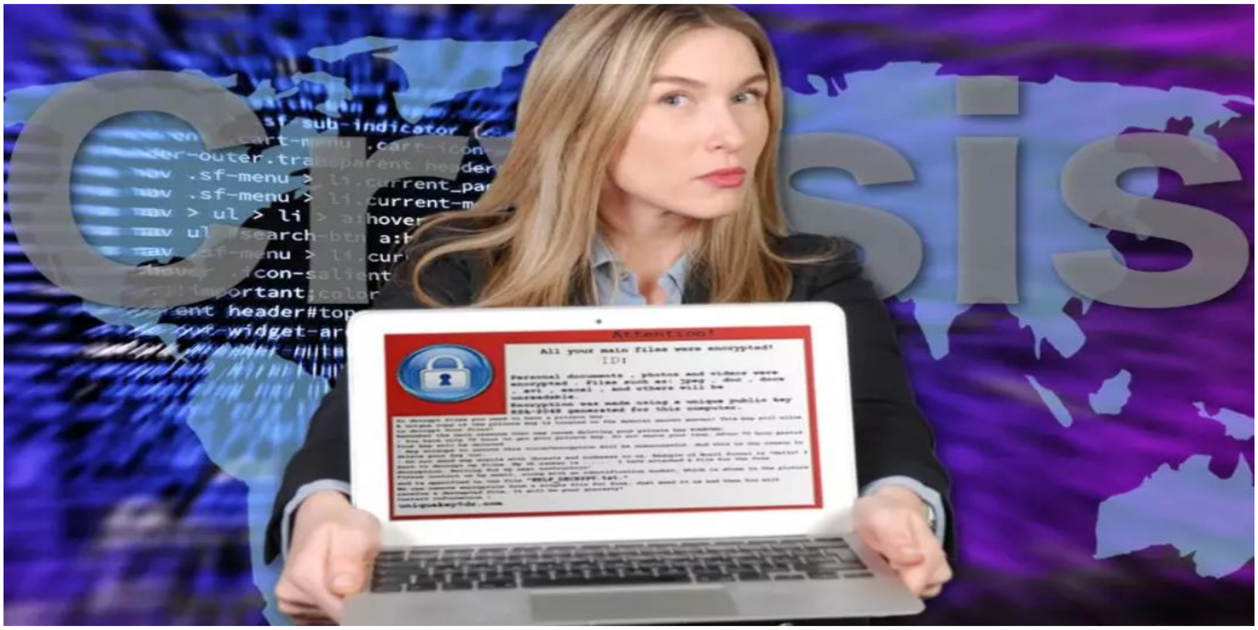
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

https://thehackernews.com/2022/05/researchers-expose-inner-working-of.html

https://arxiv.org/pdf/2102.06249.pdf

https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ce44cbda9fdc061050c1d2a5dec0270874a9dc85.pdf

Ransomware Attack: 2


Crysis
Attention!
All your main files were encrypted!
ID:
Personal documents , photos and videos were encrypted . Files such as: jpeg , doc , docx , avi , excel , and others will be unreadable.
Encryption was made using a unique public key RSA-2048 generated for this computer.

- **Attack Summary:**

  Kaiser Permanente data breach exposes health data of 69K people.

  [Records Exposed: 69k | Source: Online Newspaper | Site name: **BleepingComputer.com** | Type of Ransomeware attack: **CRYSIS**]

- **Exploited Vulnerability:**

  On April 5, 2022, Kaiser Permanent is the health plant of America which is leading non-profit health plans and health care provider. Some of the Kaisar Permanent patients have been affected by an unauthorized access incident. The unauthorized access incident when he got the unauthorized letter sent by Kaiser Permanent. When they accessed it then he lost the data of 69000 people.

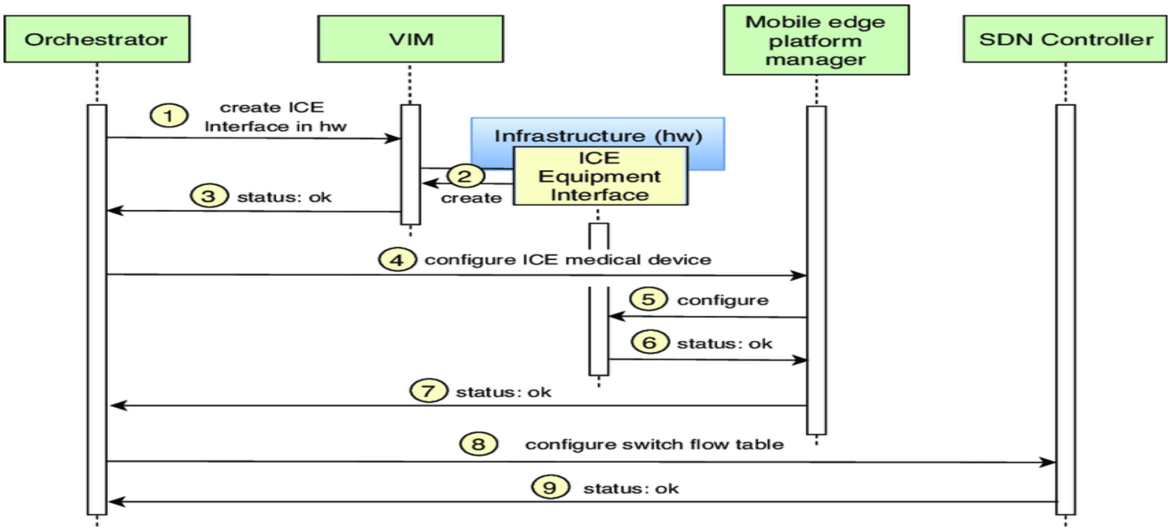


Fig: Process of attacking ransomware.

That was very protective health information.

such as

* Patients first and last name

*Medical record numbers

*Dates of service

*Laboratory test

*Credit, debit card information

Finally, the Kaiser Permanent took the step to gain that and they have the research to get rid of that.

- **Remedy Actions Taken:**

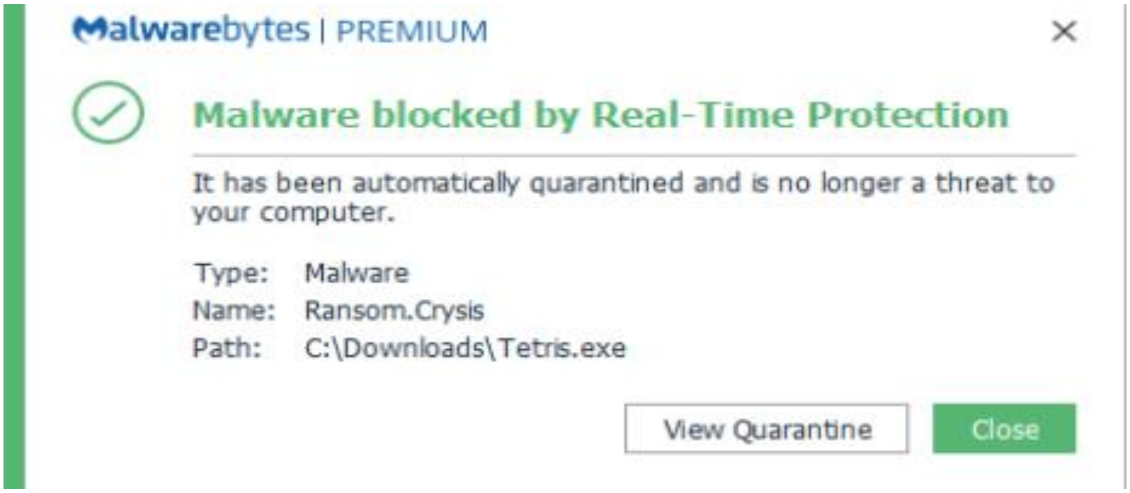
Kaiser Permanent took the proper step and started to research on that.

After following the event, they have quickly taken steps Agins that to terminate the unauthorized party’s access to employee’s emails, “Kaiser permanent added.

Then they were added the system when the ransomware attacks with email attachment then they will be able to reset all the password of this email as soon as possible. (Kaiser permanent took that decision)

After that Kaiser Permanent took the decision to give training for all the employees of the office about to defend the ransomware which is given by email attachment. (Took the decision by kaiser permanent)

When they get the email, they will have to scan all the email attachments.



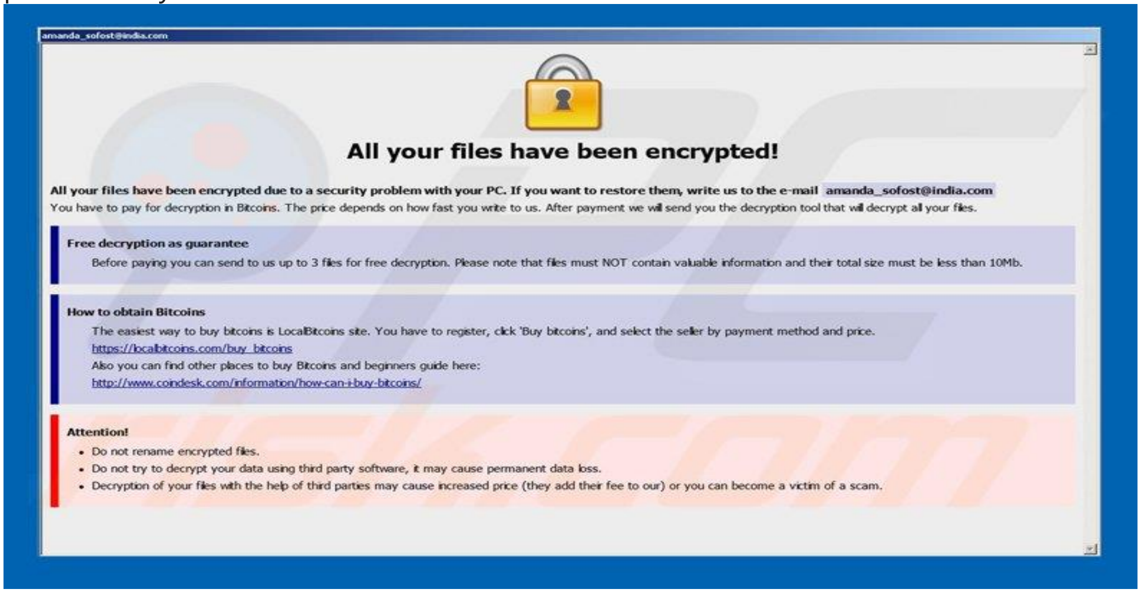
Malware blocked by Real-Time Protection

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Ransom.Crysis
Path: C:\Downloads\Tetris.exe

Fig: Malwarebytes software ransomware detection.

Here we tried to show the process of malware attacking system. Malwarebyte is a scanner which is detect the malware or ransomware . If any malware or ransomware detect in computer then it gives the signal. After that we can qurantine that. So, this kind of premium scanner we can use for scan as if it can detect the the system.Also, they are offering potentially involved individuals access to free credit monitoring and identity protection systems.



amanda_sofost@india.com

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail amanda_sofost@india.com

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send to us up to 3 files for free decryption. Please note that files must NOT contain valuable information and their total size must be less than 10Mb.

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Fig: This is basically figure of encryption time.

When the ransomware have done its work and it will encrypt , after that they will ask for the ransom.

Always should be updated with all the tools like antivirus and detection tools etc.

If it is possible Isolate all the infected files.

- **Recommended Future Mitigation Strategy:**

All the emails should be scanned all the time as if any ransomware or other malicious

software cannot infect our files.

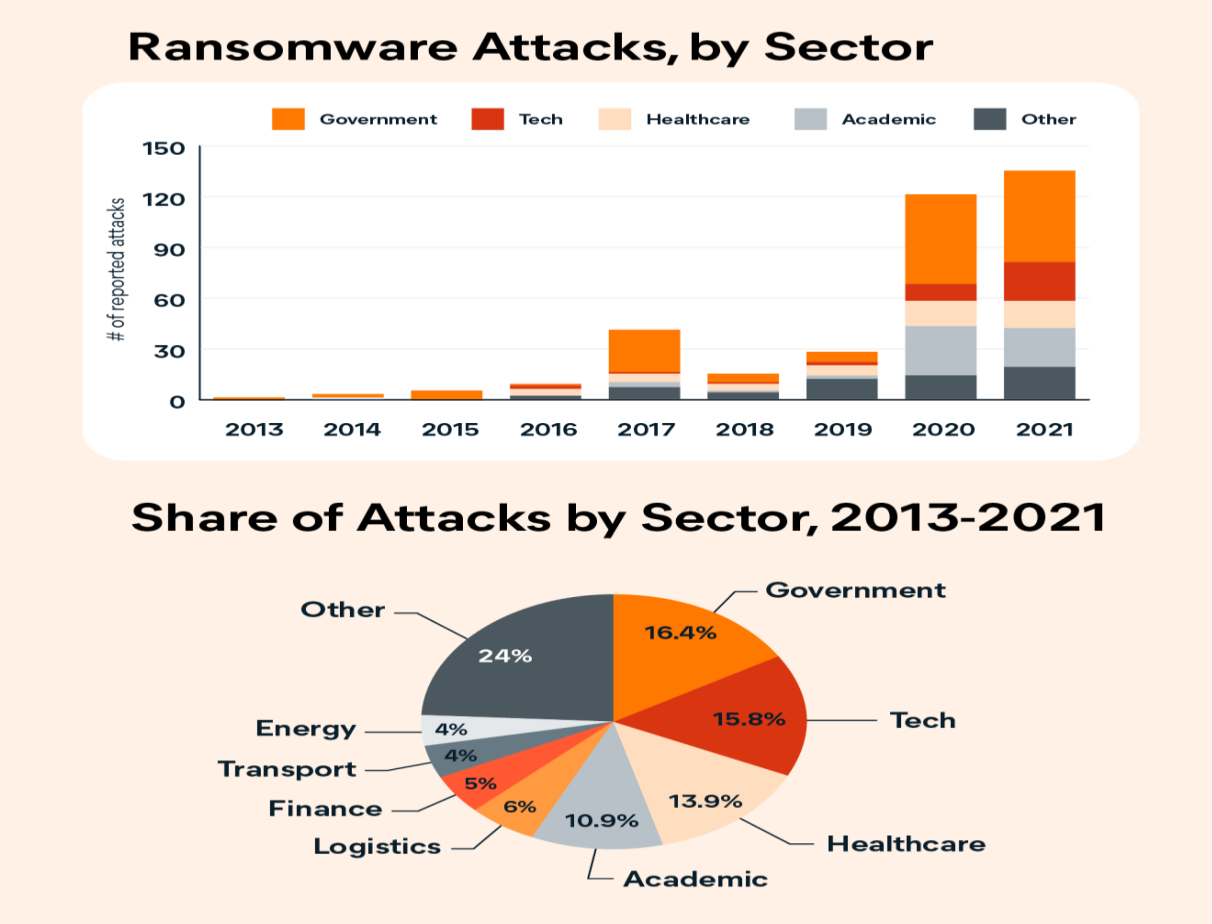
All the employees should take the training for the future attack.

How the employee recognizes it they all should have practical knowledge.

After the infection how they will overcome and defend this they all should know this. Always install some tools which can defend it.

In the future this type of message should always be in the spam folder and we should skip it.

Buy a new computer if your computer is getting too old.


Ransomware Attacks, by Sector

Share of Attacks by Sector, 2013-2021

Data Source: Information is Beautiful

Fig: Ransomware attack by sector

While attacks overall have been increased, recent economical growth is really targeted. Technical company, healthcare , government site, academic sector are arbsorbed bulk of attacks. All the reported attacks looked at those four area alone account for the 57 percentage of all attacks.

During this time tech sector was under the attacksand increasing the threat. From 2019 to 2021 only 7 percent of reported ransomware attacks in the tech companies. Over the past one years it has gone for 20 percentage amount.
Mostly attack site is government site and then lowest is energy and transport site. Second higher is tech company then healthcare.

This kind of email should always be prohibited because it is always sent by Cyber Criminals.

ransomware: cryptoblazer@asia.com, webmafia@asia.com, amanda_sofost@india.com, gcaesar2@aol.com, alex-king@india.com, DIGITALKEY2@163.com, quentin77@163.com, supermanluter@aol.com, supportfriend@india.com, calipso.god@aol.com, helphomeless@india.com, Space_rangers@aol.com, Ceri133@india.com, Melme@india.com, Milarepa.lotos@aol.com, Batman_good@aol.com, f_tactics@aol.com, diablo_diablo2@aol.com, legioner_seven@aol.com, donald_dak@aol.com, seven_legion@aol.com, Meldonii@india.com,Opencode@india.com and last_centurion@aol.com,bitcoinpay@india.com, bitcoinrush@aol.com, drew_ranger@india.com, grand_car@aol.com, Drow_ranger@india.com, opencode@india.com, a_princ@aol.com,

This type of email always send's by the attacker and it always should spam message.

Reference:

https://www.datto.com/blog/common-types-of-ransomware

https://cloudian.com/ransomware-attack-list-and-alerts/

https://www.bleepingcomputer.com/news/security/kaiser-permanente-data-breach-exposes-health-data-of-69k-people/

https://healthy.kaiserpermanente.org/content/dam/kporg/final/documents/member-services-information/policies/substitute-notice-wa-en.pdf

https://www.identitytheft.gov/#/assistant

https://www.pcrisk.com/removal-guides/9541-virus-encoder-ransomware

https://www.2-spyware.com/remove-crysis-ransomware-virus.html

https://www.researchgate.net/figure/Sequence-diagram-to-mitigate-a-ransomware-attack-to-a-medical-device_fig4_331534694

https://www.avast.com/c-biggest-ransomware-attacks