



Ransomware



Presented by:
Kemar Wilks EnCE, CHFI, CEH, CMPFOR, CBE, ACE
Senior Digital Forensic Examiner

OVERVIEW

- What is Ransomware?
- Signs of an attack
- To pay or not to pay
- Recommendations for prevention



WHAT IS RANSOMWARE?

DEFINITION:

- *Ransomware* is a type of malicious software, or malware, designed to deny access to a computer system or its data until a ransom is paid.



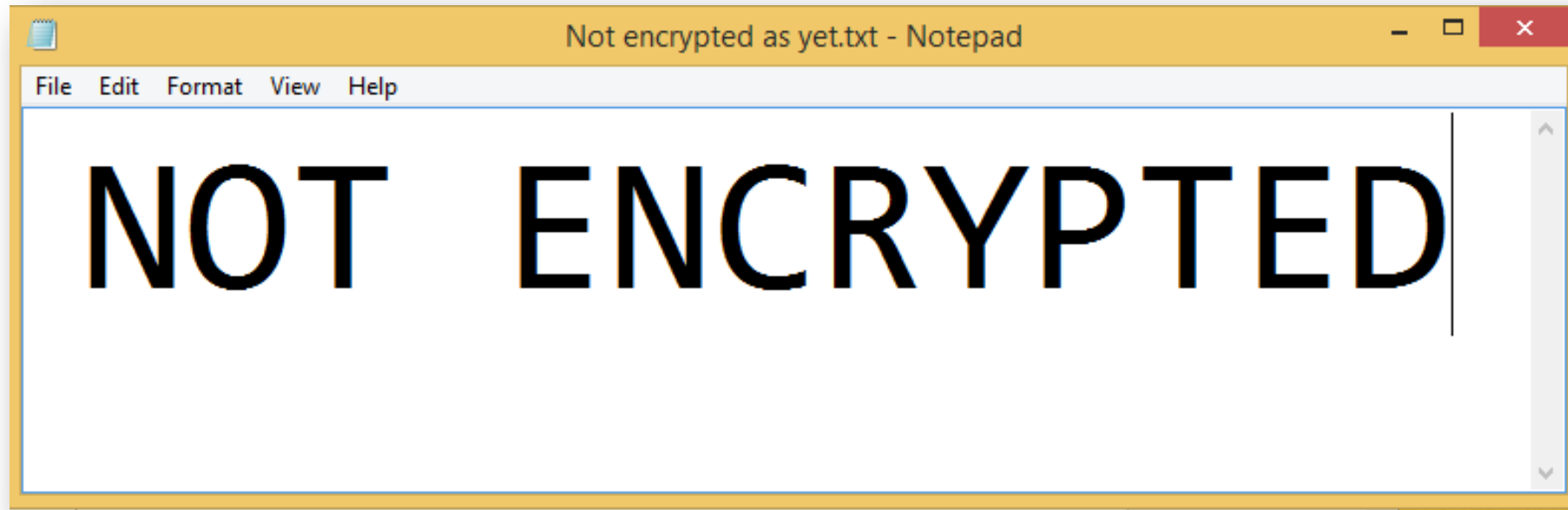
WHAT IS ENCRYPTION?

It is the process of:

- Changes the content of the data using an algorithm
- Cannot be bypassed and requires a key
- Varies in type and difficulty



WHAT AN ENCRYPTED FILE LOOKS LIKE?

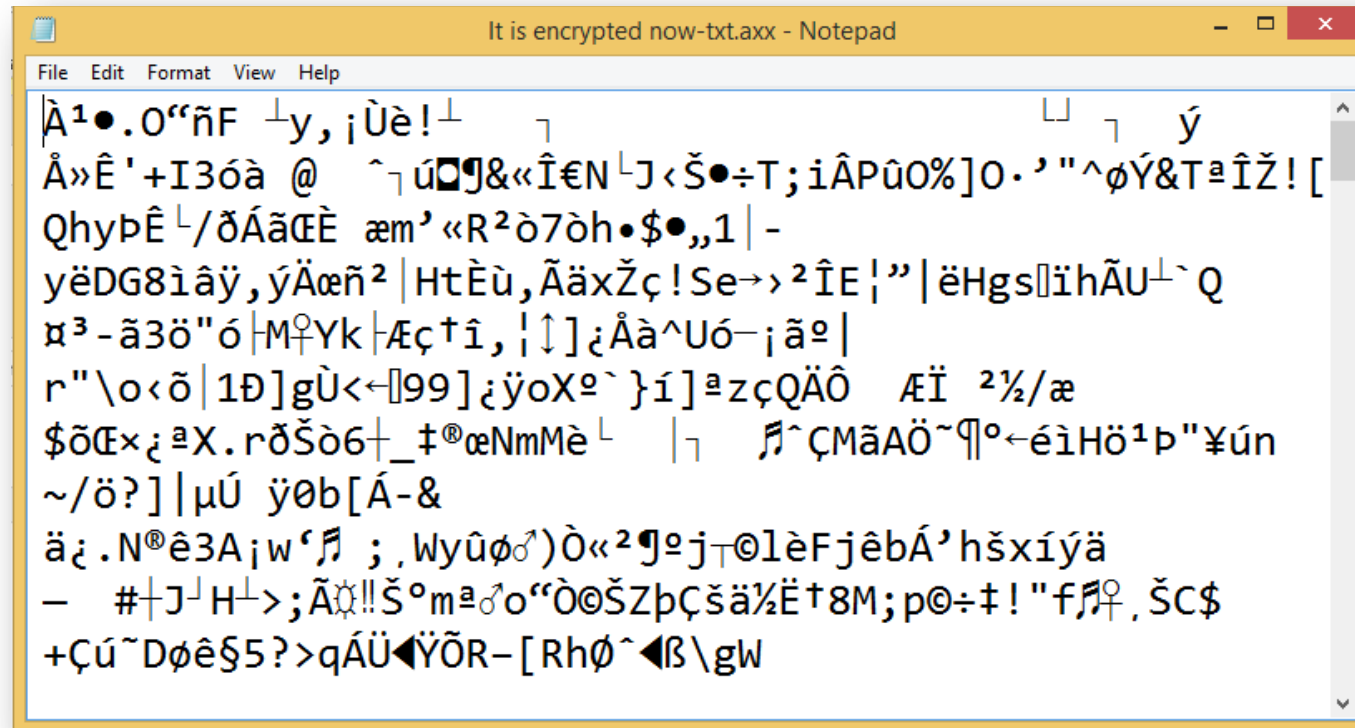


- Content can be viewed in notepad
- Contains only 2 words or 13 characters (including the space)



WHAT AN ENCRYPTED FILE LOOKS LIKE?

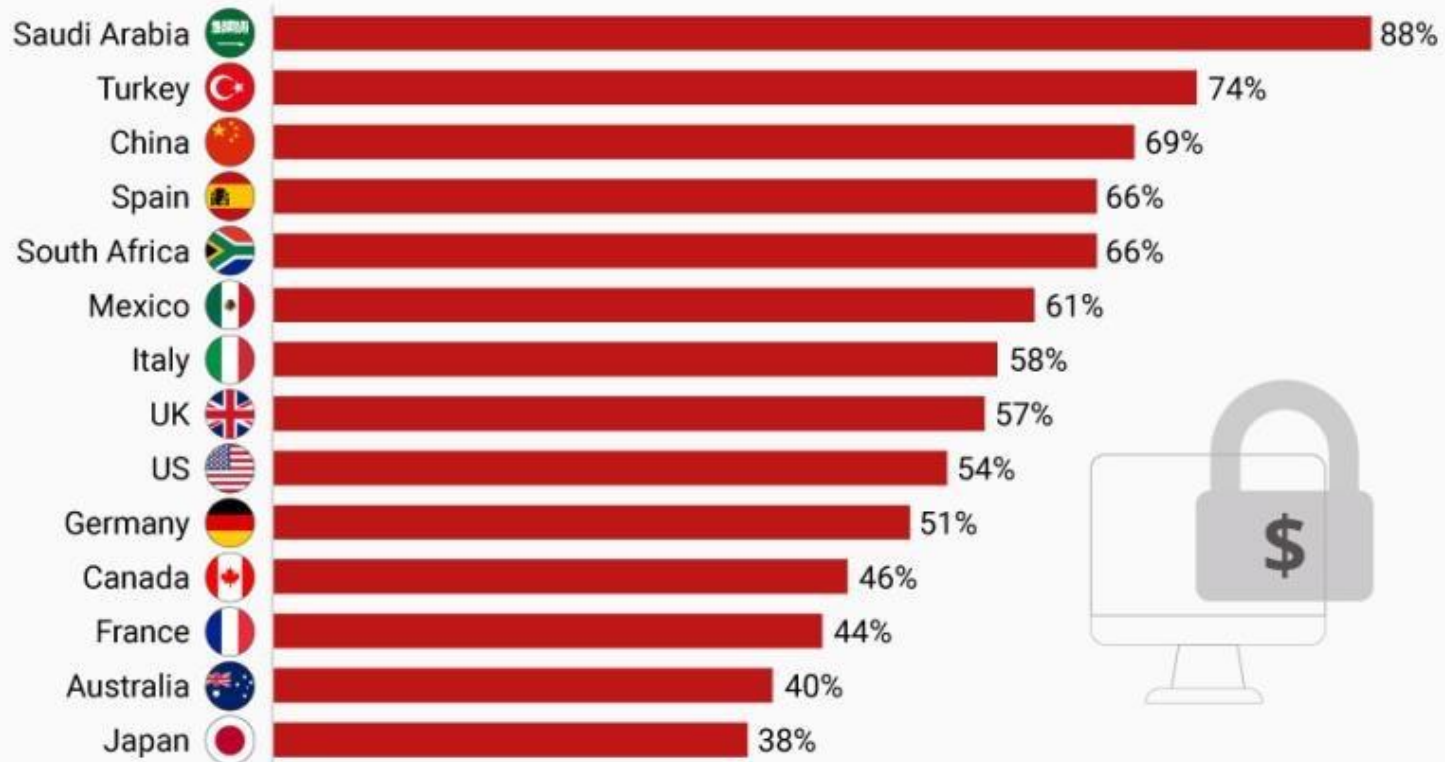
- The exact same file from the previous slide after being encrypted



WHY IS THIS IMPORTANT?

Saudi Arabia Hardest Hit by Ransomware

Percent affected by ransomware in the past 12 months



@StatistaCharts

Over 1,000 information security professionals at organizations with over 500 employees were surveyed online in November 2018.

Source: Cyber Edge



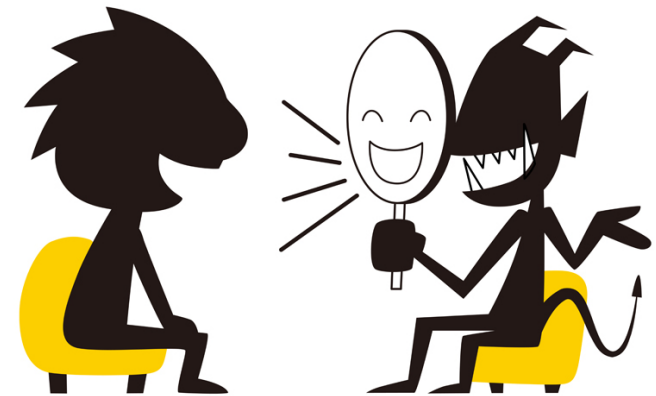
statista

WHY IS THIS IMPORTANT?

Hidden intent

Ransomware is sometimes used to hide the true intent of an attacker:

- They encrypt the files and you think their objective is for you to pay them
- They probably stole your data before encrypting and placed it on the web for sale



WHY IS THIS IMPORTANT?

Mandatory data breach reporting

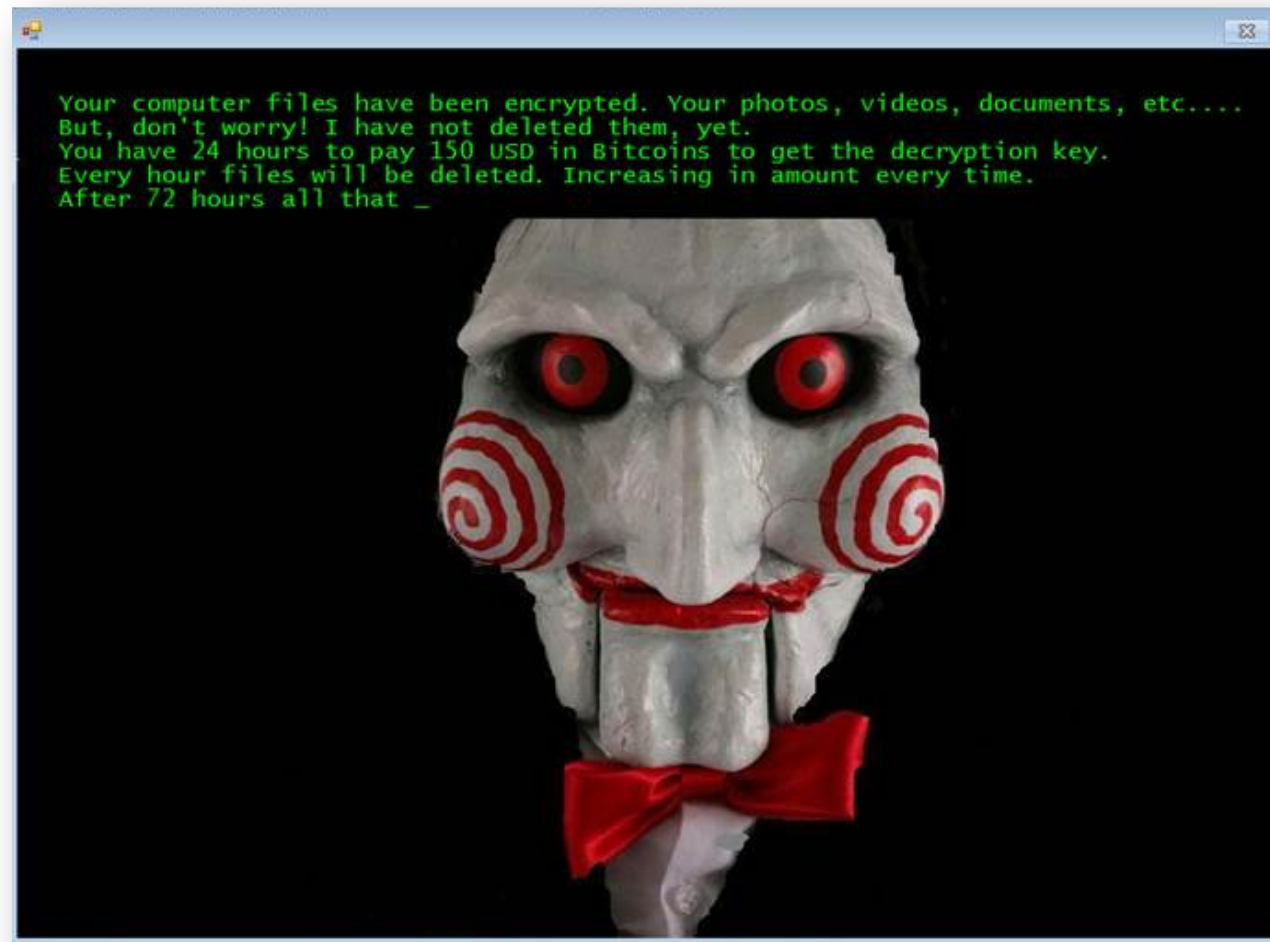
Effective November 1, 2018 companies must report any:

- Loss of;
- Unauthorized access to; or
- Disclosure of “personal information which is information about an identifiable individual.”



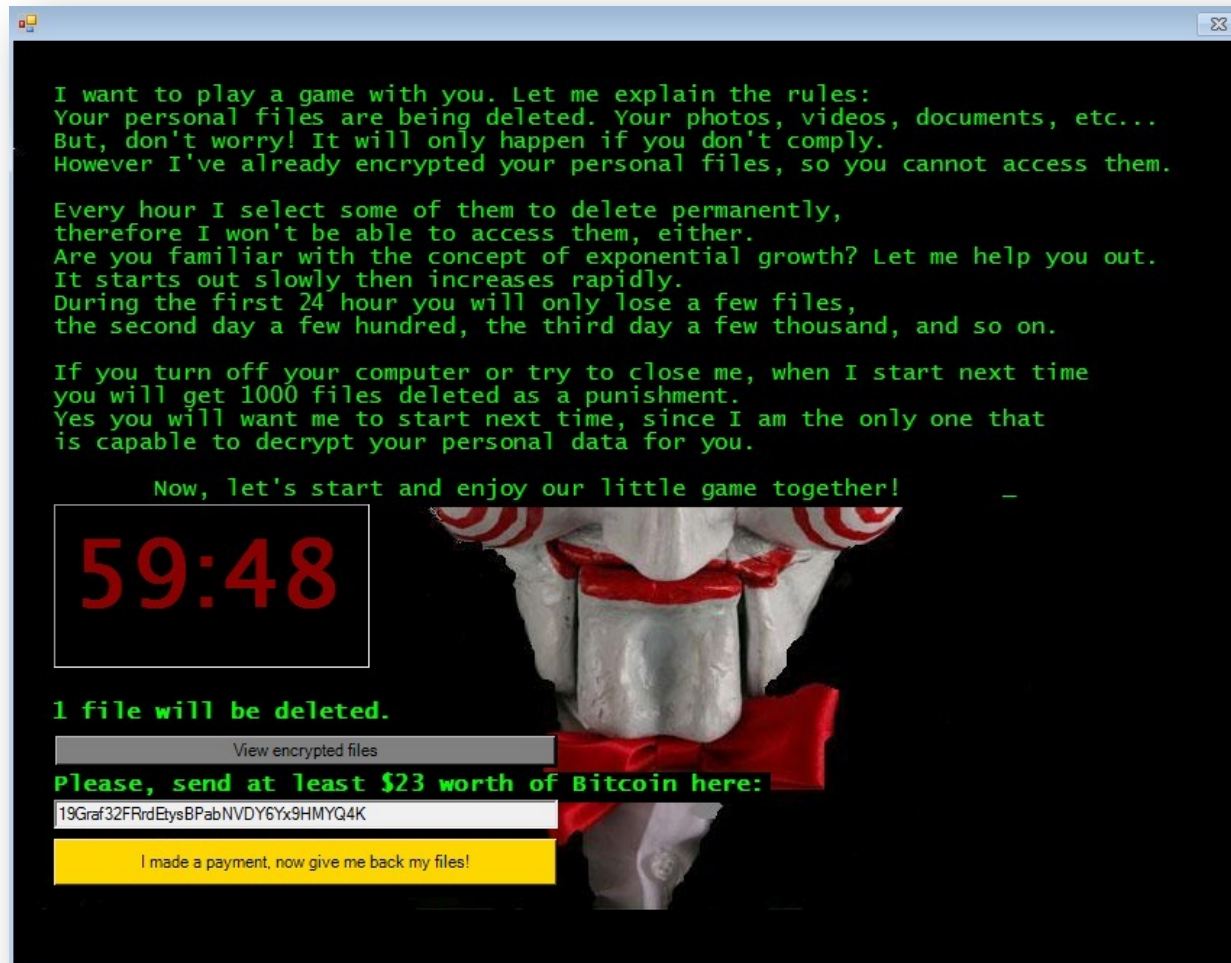
SIGNS OF A RANSOMWARE ATTACK ?

Jigsaw



SIGNS OF A RANSOMWARE ATTACK ?

Jigsaw



I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hour you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted as a punishment.
Yes you will want me to start next time, since I am the only one that
is capable to decrypt your personal data for you.

Now, let's start and enjoy our little game together!

59:48

1 file will be deleted.

[View encrypted files](#)

Please, send at least \$23 worth of Bitcoin here:

19Graf32FRrdElysBPabNVDY6Yx9HMYQ4K

[I made a payment, now give me back my files!](#)



SIGNS OF A RANSOMWARE ATTACK ?

Dharma



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 veracrypt@foxmail.com

Write this ID in the title of your message [REDACTED]

In case of no answer in 24 hours write us to these e-mails: veracrypt@foxmail.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 us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

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.



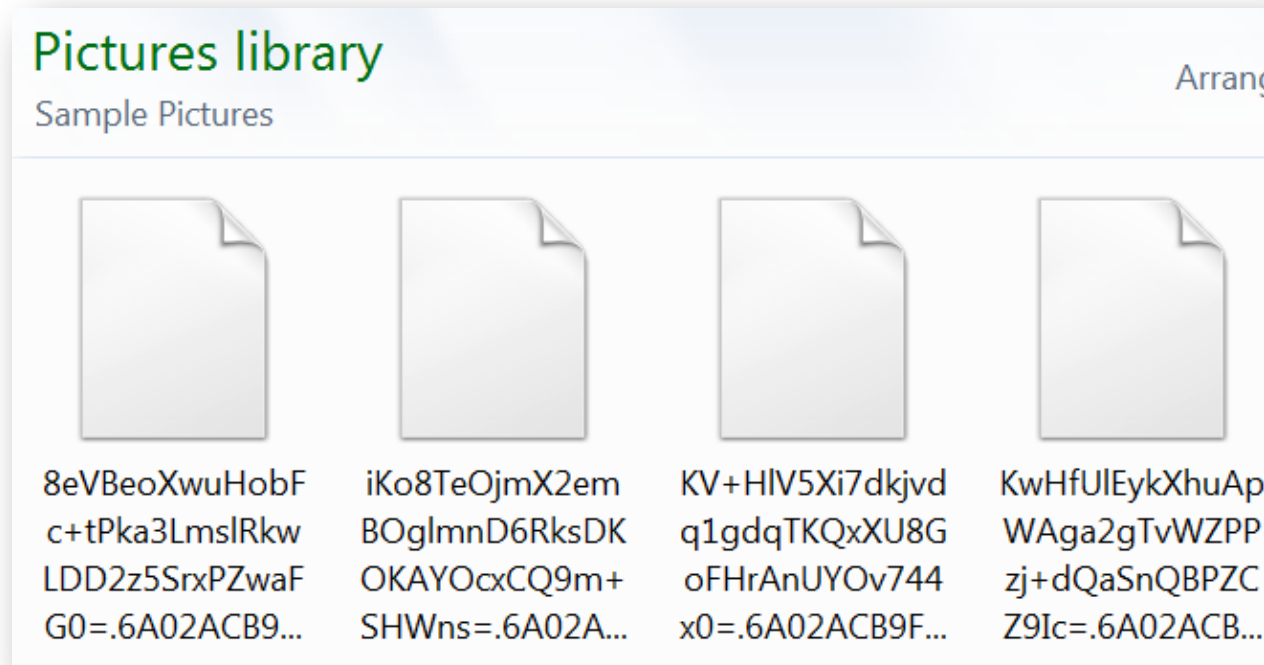
SIGNS OF A RANSOMWARE ATTACK ?

WannaCry



SIGNS OF A RANSOMWARE ATTACK ?

Filenames may be completely different

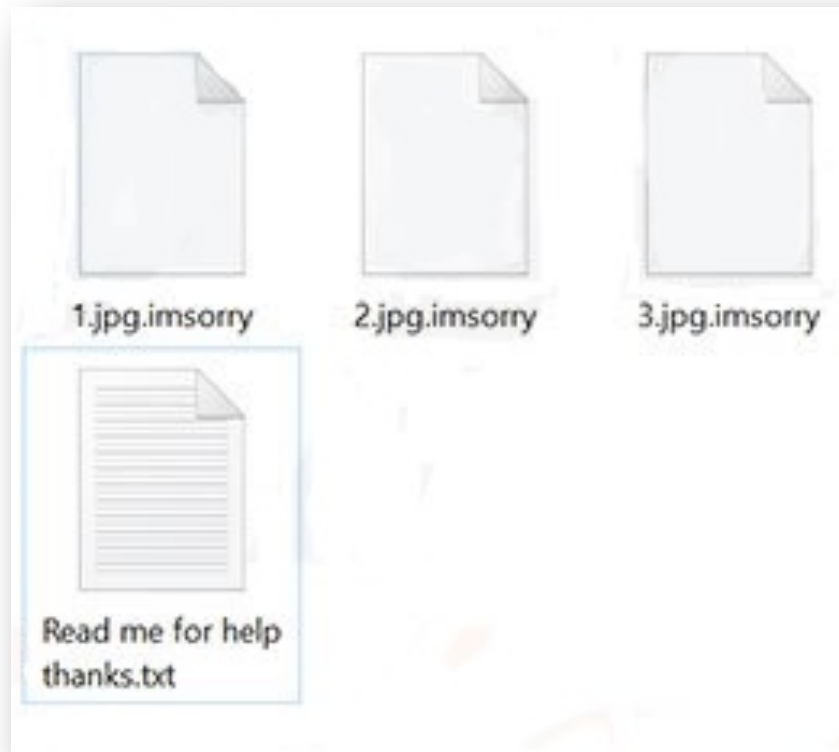


Shade Ransomware



SIGNS OF A RANSOMWARE ATTACK ?

Filenames may have an extra extension



HOW IT ALL HAPPENS

Most ransomware attacks are initiated through:

- Drive by downloads
- Phishing emails
- Clicking malicious links
- Downloading malicious files



HOW IT ALL HAPPENS

Drive-by attack

- User accessed a website that contains malware
- Malware is silently downloaded/installed
- Files become encrypted
- Panic starts!



HOW IT ALL HAPPENS

Phishing emails' links and attachments

- User receives phishing email
- Email is engineered to trick the user into clicking a link or downloading the attachment
- Files become encrypted
- Panic starts!



HOW IT ALL HAPPENS

Clicking malicious links on websites

- User visits site with malicious content
- Site is engineered to trick the user into clicking a link
- Files become encrypted
- Panic starts!



Your PC is infected!

Scan now

[Update your antivirus \(free\)](#)



HOW IT ALL HAPPENS

Malicious “FREE” downloads

- User downloads malicious content offered as free and legitimate
- Opens downloaded file and encryption begins
- Panic starts!



HOW IT ALL HAPPENS

Pull the plug

If you are lucky enough to notice that something suspicious occurred, pull the power plug and call a professional



TO PAY OR NOT TO PAY

HMMM....

Cons

- Paying can motivate criminals to keep doing it
- No guarantee that they will honor the deal
- Something can go wrong during the decryption process
- Reinfection can occur



Pros

- Possibility that the data will be returned
- Data may be too valuable to lose



OTHER SOLUTIONS

Cyber Security professionals can help you to:

- Find out if there are decryption keys publicly available that can decrypt your files. (If it is an old version of the attack)
- Assess the type of data and the extent of the damage to help make decision
- Determine if there are backups that you don't know about (System restore files etc.)



PREVENTATIVE MEASURES

Prevent it and avoid the stress

- Have regular offline backups or cloud backups
- Install an up-to-date anti-virus software from a trusted vendor
- Ensure that the latest security patches are installed for all software
- Train employees so that they are aware of phishing attempts and have good security habits – *be suspicious*
- Limit and secure remote connections to computers or disable them completely



SUMMARY

- Protect your assets by sensitizing your employees – *be suspicious*
- Maintain secure offline or cloud backups
- If you are lucky enough to notice that you did something suspicious, pull the power plug and call a professional
- Act quickly

