



RANSOMWARE

Advice and Guidance – Schools

Contents

Introduction	1
Definitions	2
Variants	2
Propagation method:	2
Email Phishing Campaigns	2
Social Engineering attacks	3
Recent School Infections.....	3
Example Email screenshot – Crypto Locker	4
Activation.....	5
Example Screenshot of notice of Activation and Encryption- Cryptolocker.....	5
Examples of files in shared folders where encryption has occurred – TeslaCrypt 3.0.....	5
Example Screenshot of Activation and Encryption notice – TeslaCrypt 3.0.....	6
Advice	6
Emails.....	6
Suspicious / Unkown web site links sent by email.....	6
Personal Email /webmail	6
Procedure.....	6
In the event of a suspected ransomware virus	7
If there is an activation of a ransomware virus, e.g.....	7
Required information:	7
Additional Advice to customers	8
References.....	8

Document

Document Title	Ransomware
Document Subtitle	Advice and Guidance
Author(s)	Small, Julian
Document Author Company	Coventry City Council
Release Version	1.0

Introduction

In recent years, personal use of computers and the internet has exploded and, along with this massive growth, cybercriminals have emerged to feed off this burgeoning market, targeting innocent

users with a wide range of malware. The vast majority of these threats are aimed at directly or indirectly making money from the victims. Today, ransomware has emerged as one of the most troublesome malware categories of our time. These threats target home users, businesses, and organisations alike.

Definitions

A **Ransomware** infection is a program that ransoms the data or functionality of your computer until you perform an action. This action is typically to pay a ransom in the form of Bitcoins or another payment method. When a computer is infected with ransomware the effects can be either a nuisance or devastating depending on what the infection does. For example, many ransomware just lock you out of your computer, which can easily be fixed with the right tools. Other ransomware, such as Crypto Ransomware, are much more devastating as they will actually encrypt the data on your computer and require you to pay a ransom in order to decrypt your files.

Effects of a ransomware infection include:

Make it so that you cannot execute programs other than ones required to pay the ransom.

Terminate any non-essential programs that may be running.

Encrypt your data so that you can no longer access it or open it with programs.

Remove your ability to browse the Internet other than to locations that will allow you to pay the ransom

Once you pay the requested ransom, the criminals may send you a code that you can input into the Ransomware program that then allows you to use your computer or decrypt your data. In some situations, though, even if you do pay the ransom, the criminals will just take your money and run, with you being left with your problem unresolved.

Though the loss of your data and computer can be devastating, sending the ransom could be even more so. Depending on how the criminals want you to pay the ransom could put you at risk for Identity Theft as the information you send may contain personal information. Therefore, we suggest that you never pay a ransom unless it is absolutely necessary for data recovery. For screenlockers you should never pay a ransom as there are always solutions to remove these infections without paying anything.

Last, but not least, it is important to remember that paying the ransom only continues to fuel the release of new variants of these types of programs.

Variants

At the time of writing, there are many new variants entering circulation.

Previously:

'Locker Ransomware'

TeslaCrypt (Version 3.0 detected Jan 2016)

TorrentLocker

Cryptowall (latest is v4.0)

Cryptofortess

CTB-Locker

Propagation method:

Email Phishing Campaigns

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

Social Engineering attacks

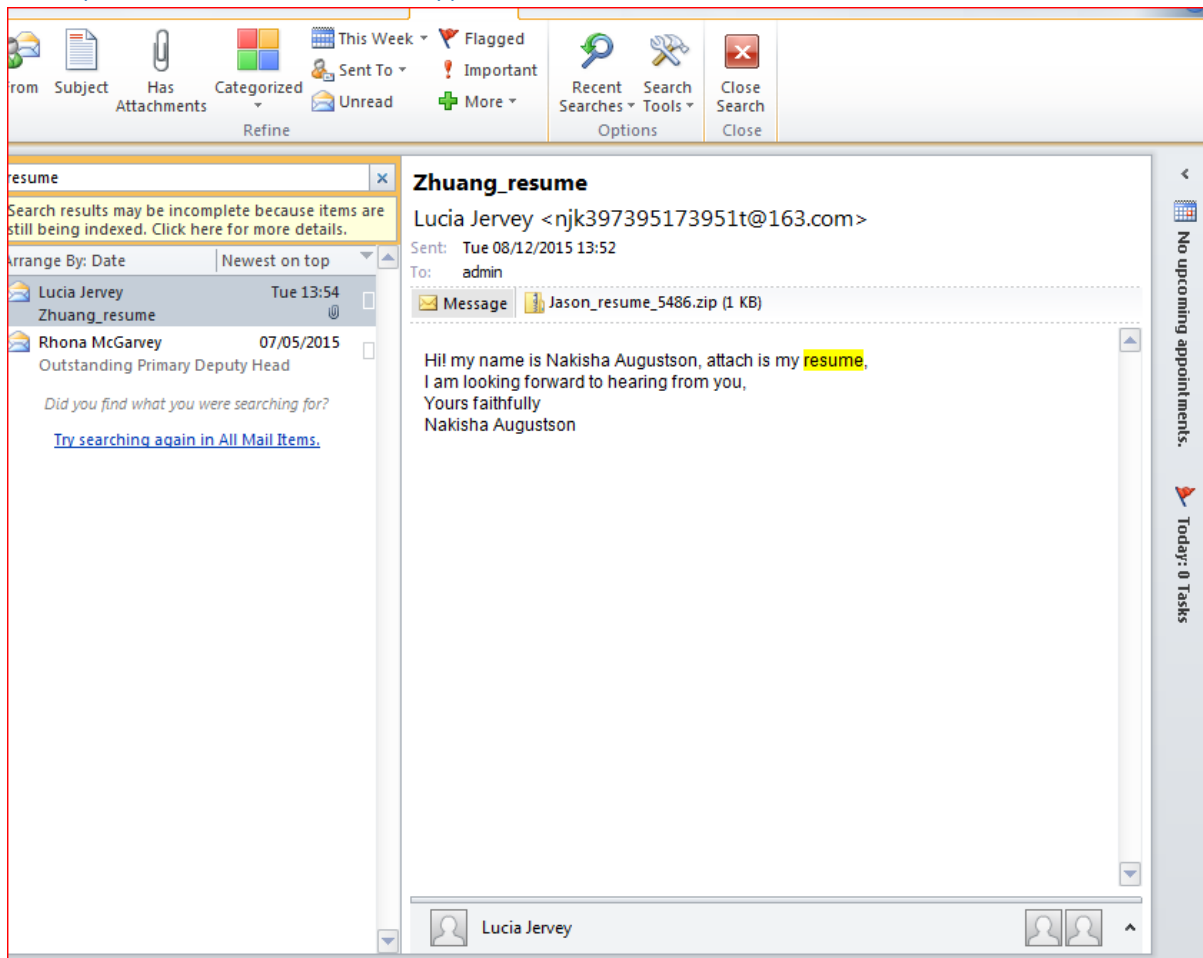
In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Recent School Infections

The majority of the most recent incidents reported at schools have been from the Admin staff, checking the email sent to the 'admin@*' generic email address for the school listed on their website and used for receiving most day- to day emails and vacancies information.

These attacks are delivered by random mass emails, and can be a generic email about a Resume, or a CV, an unpaid invoice, or a delivery note for a parcel. In many instances the email will contain an attachment. In some cases, they include a link to a website.

Example Email screenshot – Crypto Locker



Note in the above screenshot:

Suspicious senders email address

Generic template body message

Poor Grammar

Use of Resume – not CV.

Mismatched names in attachment and signature

The attachment – Notably a ZIP file.

Activation

Once the Zip file is opened and the virus program begins installing and disabling shadow copies, antivirus, and various other protection methods, the software will begin immediately to encrypt local files and files on shared network drives to which the user has write access.

A message will be displayed on screen and this image will be deposited in all encrypted folders (with variations dependant on the ransomware):

Example Screenshot of notice of Activation and Encryption- Cryptolocker

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall
More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

- 3wzn5p2yiumh7akj.praypartnerstodo.com/1YmkNoc
- 3wzn5p2yiumh7akj.allepohe1pto.com/1YmkNoc
- 3wzn5p2yiumh7akj.bark1paypartners.com/1YmkNoc
- 3wzn5p2yiumh7akj.maver1ckpaypartners.com/1YmkNoc

If for some reasons the addresses are not available, follow these steps:

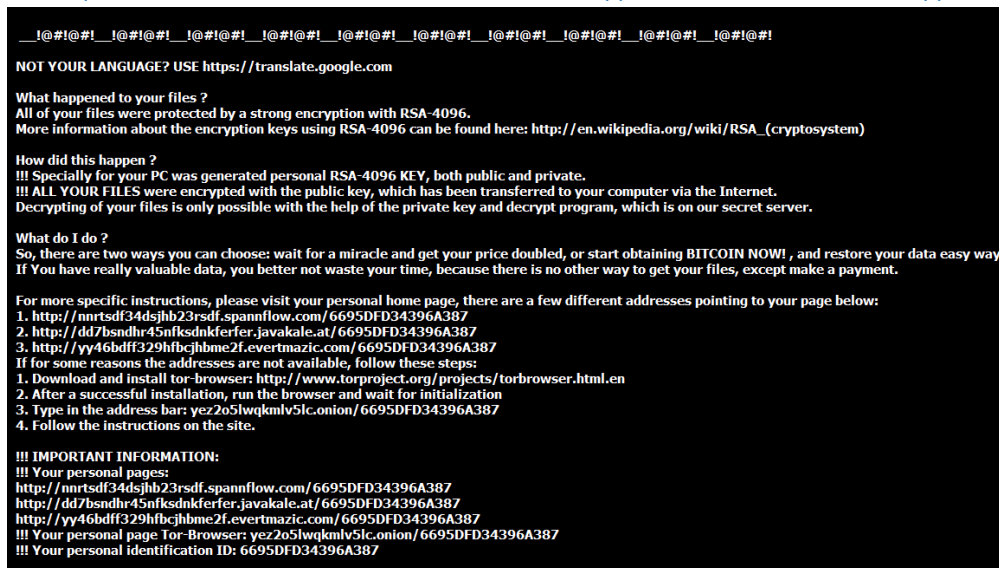
- Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
- After a successful installation, run the browser and wait for initialization.
- 3wzn5p2yiumh7akj.onion/1YmkNoc ◀Type in the address bar
- Follow the instructions on the site.

IMPORTANT INFORMATION:
praypartnerstodo.com/1YmkNoc ◀Your Personal PAGE
3wzn5p2yiumh7akj.onion/1YmkNoc ◀Your Personal PAGE(using TOR)
1YmkNoc ◀Your personal code (if you open the site (or TOR 's) directly)

Examples of files in shared folders where encryption has occurred – TeslaCrypt 3.0

HELP_RECOVER_instructions+bce.html	09/02/2016 12:05	HTML Document	13 KB
HELP_RECOVER_instructions+bce.png	09/02/2016 12:05	PNG Image	68 KB
HELP_RECOVER_instructions+bce.txt	09/02/2016 12:05	Text Document	3 KB
help_recover_instructions+kl.html	10/02/2016 08:55	HTML Document	15 KB
help_recover_instructions+kl.txt	10/02/2016 08:55	Text Document	3 KB
help_recover_instructions+phw.html	08/02/2016 13:27	HTML Document	15 KB
help_recover_instructions+phw.txt	08/02/2016 13:27	Text Document	3 KB

Example Screenshot of Activation and Encryption notice – TeslaCrypt 3.0



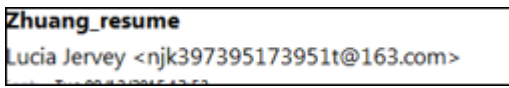
Advice

Emails

If an email is received which contains an attachment, or a link to an external website, check the following:

Is the email from a known contact?

Is there anything suspicious about the email address?

Example: 

Is the email and the attachment expected?

Does the email contain poor grammar or spelling?

Suspicious / Unkown web site links sent by email

Test the link in:

<http://global.sitesafety.trendmicro.com/>

Personal Email /webmail

Be particularly cautious about checking personal emails on a works computer.

Procedure

In the event of a user receiving a suspicious email with an attachment:

Do not open the attachment

Do not forward this on to anyone.

Do not send it to service desk.

Do not save the attachment

If in doubt, delete the email. If you know the sender, contact them by phone and ask them if they sent you the email.

If it was a genuine email, the sender can resend it. This is far less inconvenient than a full system restore for the entire site.

In the event of a suspected ransomware virus

If any of the following circumstances are noticed:

A user opens up a suspicious email attachment /A user opens a suspicious web link

Run a scan on your machine for viruses:



If there is an activation of a ransomware virus, e.g.

A user notices a popup window similar to listed in the screenshot in the sub heading

'Example Screenshot of Activation and Encryption notice – TeslaCrypt 3.0'

'Example Screenshot of notice of Activation and Encryption- Cryptolocker'

A user notices they cannot open frequently used files on their machine or on a network share

A user notices files similar to listed in the screenshot in the sub heading in this document

'Examples of files in shared folders where encryption has occurred – TeslaCrypt 3.0'

Shut down the infected workstation immediately and unplug the network cable.

Contact the Service Desk immediately by phone in office hours – See the below link for details:

[Services for schools - ICT](#)

Provide the following information

Required information:

Users name and contact phone number

Affected machine / machines Asset tag / tags

Affected users account name / names

Date and time suspect email was opened

Receiving email address

Did the user open the attachment or click on any links in the email?

Was the user the sole recipient?

Does anyone one else check that mailbox?

Has the user forwarded the suspect email to anyone?

Determine state of infected machine / machines. If the infected workstation is still on, shut down the workstation and display a sign on it so it is not turned on until attended by a desktop engineer.

Additional Advice to customers

Make sure your backup is working daily, and checked daily.

Ensure any important data is saved in a location that is included in your daily backup.

Regularly check that your antivirus software is up to date.

Never open attachments or embedded links in emails unless you know with 100 per cent certainty that they are safe.

Never visit an unknown website without first checking it is safe:

<http://global.sitesafety.trendmicro.com/>

References

Crypto Ransomware

<https://www.us-cert.gov/ncas/alerts/TA14-295A>

<http://www.bleepingcomputer.com/>

Information on Ransomware

<http://www.bleepingcomputer.com/virus-removal/ransomware>

Social engineering attacks

<https://www.us-cert.gov/ncas/tips/ST04-014>