"RANSOMWARE" REMOVAL

by Francis Chao
fchao2@yahoo.com

Web location for this presentation:

http://aztcs.org

Click on

“Meeting Notes”

SUMMARY

"Ransomware" is malware that takes over your computer or part of your computer and offers to give you back access to it when you pay a ransom fee. The more sophisicated instances of "ransomware" can only be removed by booting up with a bootable "rescue media" CD-R disc, DVD-R disc, or USB flash drive device.

TOPICS

- What is "Ransomware"?
- Proactive Prevention To Prevent "Ransomware" Infections
- Back Up Your Computer and Its Data Files To Avoid The Losses Caused by "Ransomware"

TOPICS (continued)

- Reactive Removal of "Ransomeware" With "Safe Mode"
- Reactive Removal of "Ransomware" With Bootable Media

TOPICS (continued)

- Using Bootable Media For Computers With "UEFI" with "Secure Boot"
- "ICE Cybercrime Center" Ransomware

WHAT IS "RANSOMWARE"?

- Some "ransomware" takes over your computer and denies you access to it.
- Some "ransomware" takes over one Or more of your Web browsers and denies you access to it.
- Also known as "extortionware".

WHAT IS "RANSOMWARE"? (continued)

- Some examples of "ransomware":


ICE
The ICE Cyber Crime Center
Your IP Address
Your Provider: Undefined
Location:
Your computer has been blocked
The work of your computer has been suspended on the grounds of unauthorized cyber activity.
Possible violations are described below:
Article - 174. Copyright
Article - 163. Pornography
Article - 184. Pornography involving children (under 18 years)
Article - 104. Promoting Terrorism
Article - 66. The distribution of virus programs
An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.
All illegal activities conducted through your computer have been recorded in the police database, including photos and videos from your camera for further identification. You have been registered by viewing pornography involving minors
MoneyPak

PCeU
Police Central e-crime Unit

Specialist Crime Directorate

Police Central e-crime Unit

To unlock your computer and to avoid other legal consequences, you are obligate

All activity of this computer has been recorded
If you use a webcam , videos and pictures were saved for identification

Video-recording: **ON**

You can be clearly identified by resolving your IP address and the associated hostname

Your IP Adress: [redacted]
Your Hostname: **British Telecommunications**
Location: **United Kingdom** [redacted]

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)

Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)

Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)

Article 104 – Promoting Terrorism
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)

Article 297 – Neglect computer use, entailing serious consequences
A fine or imprisonment for the term of up to 2 years
(Your computer has been infected with a virus, which, in turn, infected other computers)

Article 108 – Gambling
A fine or imprisonment for the term of up to 2 years (You have been gambling, but according to the law residents of the your country are not allowed gambling in any format)

In connection with the decision of the Government as of August 22, all of the violations described above could be considered as conditional in case of payment of a fine.

Amount of the fine is 100 GBP. Payment must be made within 48 hours after the discovery

1. 
2. 
3. 

Ukash

You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.

Exchange your cash for a Ukash voucher and use your voucher code in form below.

Code: [ ]

1 2 3 4 5 6 7 8 9 0

Submit

paysafecard

Paysafecard is available from 450,000 sales outlets worldwide, in the United Kingdom, exclusively from all PayPoint outlets

Exchange your cash for a Paysafecard voucher and use your voucher code in form below.

Code: [ ]

1 2 3 4 5 6 7 8 9 0

Submit

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

PCeU
Police Central e-crime Unit

Your IP-address: [redacted]
Your Provider: British Telecommunications
Location: United Kingdom , London

Your Computer has been locked

You have broken the law, your actions are illegal and will lead to criminal liability.

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Possible violations are described below:

Article – 174. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files). A fine from 18,000 up to 23,000 GBP.

Article - 183. Pornography
Imprisonment for the term of up to 2-3 years
(The use or distribution of pornographic files). A fine from 18,000 up to 25,000 GBP.

Article – 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files). A fine from 20,000 up to 40,000 GBP.

Article – 104. Promoting Terrorism
Imprisonment for the term of up to 25 years without appeal
(Visiting the websites of terrorist groups). A fine from 35,000 up to 45,000 GBP with property confiscation.

Article – 68. The distribution of virus programs
Imprisonment for the term of up to 2 years
(The development or distribution of virus programs, which have caused harm to other computers). A fine from 15,000 up to 28,000 GBP.

Article – 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software). A fine from 10,000 up to 22,000 GBP.

Article - 99. Cheating with payment cards, carding
Imprisonment for the term of up to 5 years
(The operation with the use of payment card or its details which was not initiated or not confirmed by the holder). A fine from 30,000 up to 75,000 GBP with property confiscation.

Article – 156. Spamming pornographic content
Imprisonment for the term of up to 2 years
(Spamming pornographic content by means of e-mail or social Networks). A fine from 16,000 up to 38,000 GBP.

All illegal activities conducted through your computer have been recorded in the police database, including photos and videos from your camera for further identification. You have been registered by viewing pornography involving minors.

Video-recording: ON

An attempt to unlock the computer by yourself will lead to the full formatting of all your data except the files which may be considered as evidences of criminality.

A first-time violation may not lead to imprisonment. In the case of a first-time violation you just need to pay the fine according the Law Of Loyalty To The People as of December, 04, 2012.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of 100 GBP.

Ukash | paysafecard

You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.

Exchange your cash for a Ukash voucher and use your voucher code in form below.

Code: [ ] SUBMIT

1 2 3 4 5 6 7 8 9 0

Status: Waiting for Payment 47:55:25

Where can I buy Ukash

epay payzone PayPoint

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires. In this case a criminal case against you will be initiated automatically.

CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
http [redacted].exe

Approximate destruction time of your private key:
10/18/2013 10:35 PM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

FBI

FEDERAL BUREAU OF INVESTIGATION

All activity of this computer has been recorded.
If you use a webcam, videos and pictures were saved for identification.

Your IP Address:
Your Hostname:

You can be clearly identified by resolving your IP address and the associated hostname.

Your Computer has been locked!

Illegally downloaded material (MP3's, Movies or Software) has been located on your computer.

By downloading, those were reproduced, thereby violating a criminal offence under **Section 106 of the Copyright Act.**

The downloading of copyrighted material via the Internet or music sharing networks is illegal and is in accordance with **Section 106 of the Copyright Act** subject to a **fine or imprisonment for a penalty of up to 3 years.**

Furthermore, possession of illegally downloaded material is punishable under **Section 184 paragraph 3 of the Criminal Code** and may also lead to the **confiscation of the computer**, with which the files were downloaded.

MoneyPak

Please follow the instructions on the right.

Code: Submit

Please enter your Code utilizing the Pin Pad below.

1 2 3 4 5 6 7 8 9 0 ←

Please note: This fine may only be paid within 48 hours. If you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.

1. Take your cash to one of these retail locations:

Walmart

2. Pick up a MoneyPak and purchase it with cash at the register.

3. Come back and enter your MoneyPak code to unlock your Computer.

McAfee SecurityAlliance

This site is secure

unlock computer:

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **$200**. Payable through **GreenDot Moneypak**. After successful payment, your computer will automatically unlock.
Failure to adhere to the request could involve criminal charges and possible imprisonment.

To perform the payment, enter the acquired **GreenDot Moneypak** code in the designated payment field and press the "Submit" button.

WHAT IS "RANSOMWARE"? (continued)

- See http://www.superantispyware.com/blog/2013/08/all-you-need-to-know-about-ransomware/

WHAT IS "RANSOMWARE"? (continued)

- See http://en.wikipedia.org/wiki/Ransomware and http://www.sophos.com/en-us/support/knowledgebase/119006.aspx and

PROACTIVE PREVENTION TO PREVENT "RANSOMWARE" INFECTIONS

- Your computer has greatly reduced odds of contracting an ransomware infection if you use an antivirus program that is up to date.
- With all of the the great free and not-free antivirus programs that are available, you have no excuse not to run a quality antivirus program.

PROACTIVE PREVENTION TO PREVENT "RANSOMWARE" INFECTIONS (continued)

- For advice about selecting and installing a free antivirus program, see http://aztcs.org/meeting_notes/winhardsig/antivirus/antivirus-compare.pdf

BACK UP YOUR COMPUTER AND ITS DATA FILES TO AVOID THE LOSSES CAUSED BY RANSOMWARE

- Use free or not-free software programs to back up your computer to facilitate recovering it from a "ransomware" infection. See http://aztcs.org/meeting_notes/winhardsig/backup/hd-imaging-win7-8-8.1.pdf

BACK UP YOUR COMPUTER AND ITS DATA FILES TO AVOID THE LOSSES CAUSED BY RANSOMWARE (continued)

- Store copies of your data files on external hard drives and removable media to provide you access to data files in the event of a ransomware infectionr

REACTIVE REMOVAL OF "RANSOMWARE" USING "SAFE MODE"

- If your computer is infected with "ransomware", you can restart your computer and hit F8 while it is start up. Then you can select "Safe Mode" from the "Advanced Startup Menu". After the Windows "Desktop" is displayed, you might be able to remove the "ransomware" infection.

REACTIVE REMOVAL OF "RANSOMWARE" USING "SAFE MODE" (continued)

- Once you get into "Safe Mode", you then usually will have to go to another uninfected computer to research what needs to be done to remove the "ransomware" infection.

REACTIVE REMOVAL OF "RANSOMWARE" USING BOOTABLE MEDIA

- If your computer is infected with "ransomware", you use a free, bootable CD-R disk, a free bootable DVD-R, or a bootable USB flash drive device to scan for and remove the "ransomware" infection.

REACTIVE REMOVAL OF "RANSOMWARE" USING BOOTABLE MEDIA (continued)

- To create bootable media for removing a "ransomware" infection, use an uninfected computer to access the free instructions at one of the following Web sites:

REACTIVE REMOVAL OF "RANSOMWARE" USING BOOTABLE MEDIA (continued)

- To create and use a free "Bitdefender Rescue CD", see http://www.bitdefender.com/support/how-to-create-a-bitdefender-rescue-cd-627.html

REACTIVE REMOVAL OF "RANSOMWARE" USING BOOTABLE MEDIA (continued)

- To create and use a free "Kaspersky Rescue Disc", see http://support.kaspersky.com/us/4162

REACTIVE REMOVAL OF "RANSOMWARE" USING BOOTABLE MEDIA (continued)

- A list of hyperlinks to other Web sites that offer free bootable media disc downloads can be found at http://www.askvg.com/download-free-bootable-rescue-cds-from-kaspersky-bitdefender-avira-f-secure-and-others/

REACTIVE REMOVAL OF "RANSOMWARE" USING BOOTABLE MEDIA (continued)

- Another list of hyperlinks to other Web sites that offer free bootable media disc downloads can be found at http://pcsupport.about.com/od/system-security/tp/free-bootable-antivirus-software.htm

USING BOOTABLE MEDIA ON A COMPUTER WITH A "UEFI" WITH "SECURE BOOT"

- If you have an older computer that has a legacy BIOS (Basic Input/Output System) firmware, you can disregard this section.

USING BOOTABLE MEDIA ON A COMPUTER WITH A "UEFI" WITH "SECURE BOOT" (continued)

- If you have a newer computer that has a new-fangled UEFI (Unified Extensible Firmware Interface) firmware with "Secure Boot", have two "gotchas" to consider:

USING BOOTABLE MEDIA ON A COMPUTER WITH A "UEFI" WITH "SECURE BOOT" (continued)

- "Gotcha 1":
  You will have to disable "Secure Boot" before you can boot up with bootable media
  See http://aztcs.org/meeting_notes/winhardsig/BIOStoUEFI/BIOStoUEFI.pdf

USING BOOTABLE MEDIA ON A COMPUTER WITH A "UEFI" WITH "SECURE BOOT" (continued)

- "Gotcha 2":

  Most of the free "Rescue Media" CD/DVD/USB thumb drives in the previous section will not with work with a "UEFI" computer.

USING BOOTABLE MEDIA ON A COMPUTER WITH A "UEFI" WITH "SECURE BOOT" (continued)

- "Gotcha 2" (continued):
  We expect most antivirus software developers to update their free "Rescue Media" CD-R/DVD-R/USB flash drive software to work for secure boot.

USING BOOTABLE MEDIA ON A COMPUTER WITH A "UEFI" WITH "SECURE BOOT" (continued)

- "Gotcha 2" (continued):
  At the present time, only the "Bitdefender Rescue CD" can boot up a computer that has a UEFI. To create a "Bitdefender CD", see http://www.bitdefender.com/support/how-to-create-a-bitdefender-rescue-cd-627.html

"ICE CYBERCRIME CENTER" RANSOMWARE

- The latest in-the-wild variant of "ICE Cybercrime Center" blocks most of the existing procedures for removing "ransomware":
  It does not allow booting into "Safe Mode".
  It does not allow "regedit" or "msinfo32" to start up
  It blocks the startup of all antivirus programs for manual scanning.


ICE
The ICE Cyber Crime Center
Your IP Address
Your Provider Undefined
Location United States
Your computer has been blocked
The work of your computer has been suspended on the grounds of unauthorized cyber activity.
Possible violations are described below:
Article - 174. Copyright
Article - 163. Pornography
Article - 184. Pornography involving children (under 18 years)
Article - 104. Promoting Terrorism
Article - 66. The distribution of virus programs
An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.
All illegal activities conducted through your computer have been recorded in the police database, including photos and videos from your camera for further identification. You have been registered by viewing pornography involving minors
MoneyPak

"ICE CYBERCRIME CENTER" RANSOMWARE (continued)

- All of these remediation techniques used to work for removing the "ICE Cybercrime Center" ransomware virus.

"ICE CYBERCRIME CENTER" RANSOMWARE (continued)

- We have discovered two ways to remove the "ICE Cybercrime Center":
  Method 1: Boot up and scan the computer with a free "Bitdefender Rescue CD"
  Method 2: Boot up and scan the computer with a free "Kaspersky" Rescue Disc"

"ICE CYBERCRIME CENTER" RANSOMWARE (continued)

- If you have a UEFI computer that is infected with "ICE Cybercrime Center" ransomware, only "Method 1" works because a "Bitdefender Rescue CD" is able to boot up a UEFI computer while a "Kaspersky Rescue Disc" is unable to do so.

"ICE CYBERCRIME CENTER" RANSOMWARE (continued)

- However, prior to using a "Bitdefender Rescue CD" to expunge the infection, you will have to disable the "Secure Boot" portion of the "UEFI" by using one of the two methods described at http://aztcs.org/meeting_notes/winhardsig/BIOStoUEFI/BIOStoUEFI.pdf