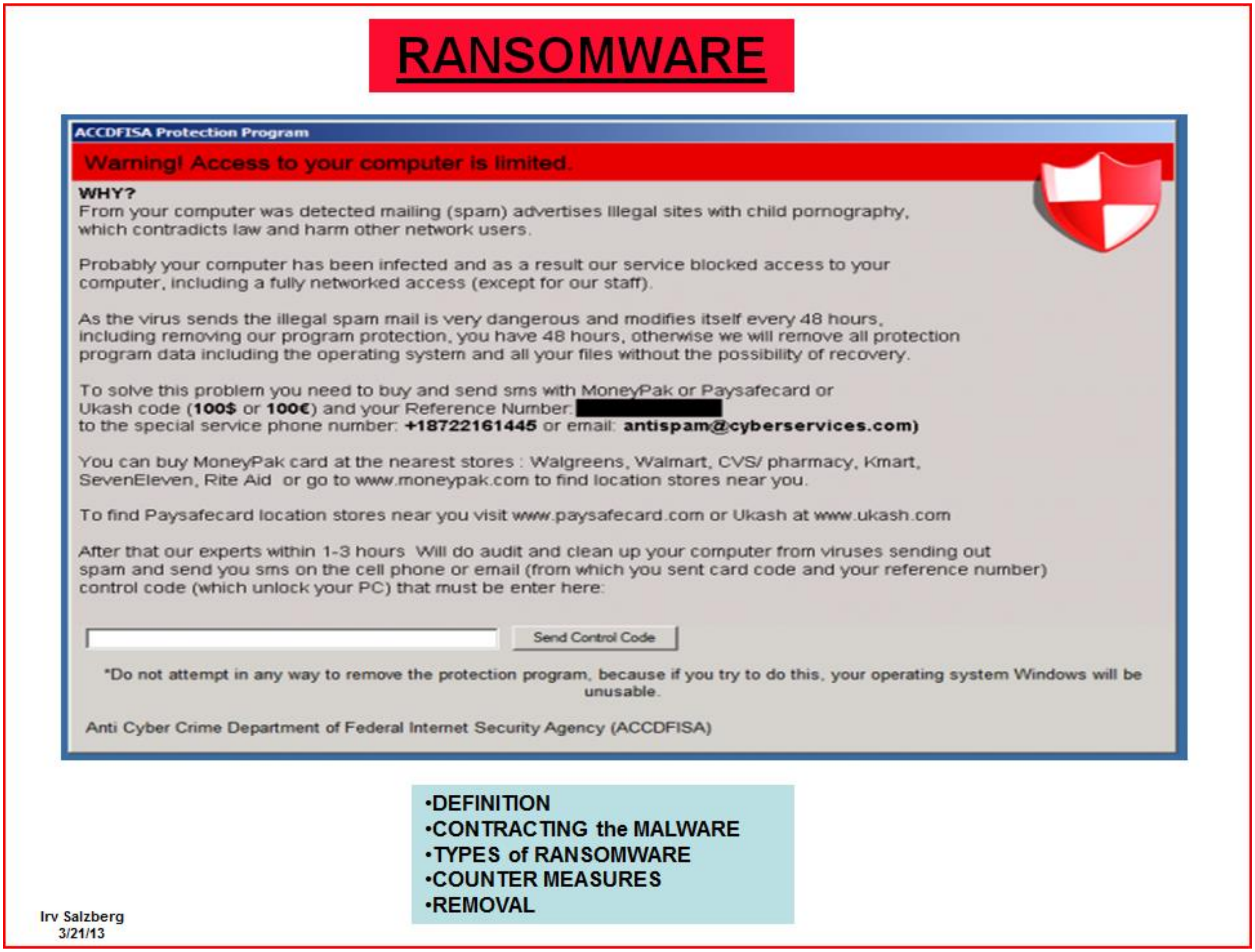
Carl Bulger presided.

Presentation by Irv Salzberg:



RANSOMWARE

ACCDFISA Protection Program

Warning! Access to your computer is limited.

WHY?
From your computer was detected mailing (spam) advertises illegal sites with child pornography, which contradicts law and harm other network users.

Probably your computer has been infected and as a result our service blocked access to your computer, including a fully networked access (except for our staff).

As the virus sends the illegal spam mail is very dangerous and modifies itself every 48 hours, including removing our program protection, you have 48 hours, otherwise we will remove all protection program data including the operating system and all your files without the possibility of recovery.

To solve this problem you need to buy and send sms with MoneyPak or Paysafecard or Ukash code (**100$** or **100€**) and your Reference Number: [redacted]
to the special service phone number: **+18722161445** or email: **antispam@cyberservices.com)**

You can buy MoneyPak card at the nearest stores : Walgreens, Walmart, CVS/ pharmacy, Kmart, SevenEleven, Rite Aid or go to www.moneypak.com to find location stores near you.

To find Paysafecard location stores near you visit www.paysafecard.com or Ukash at www.ukash.com

After that our experts within 1-3 hours Will do audit and clean up your computer from viruses sending out spam and send you sms on the cell phone or email (from which you sent card code and your reference number) control code (which unlock your PC) that must be enter here:

*Do not attempt in any way to remove the protection program, because if you try to do this, your operating system Windows will be unusable.

Anti Cyber Crime Department of Federal Internet Security Agency (ACCDFISA)

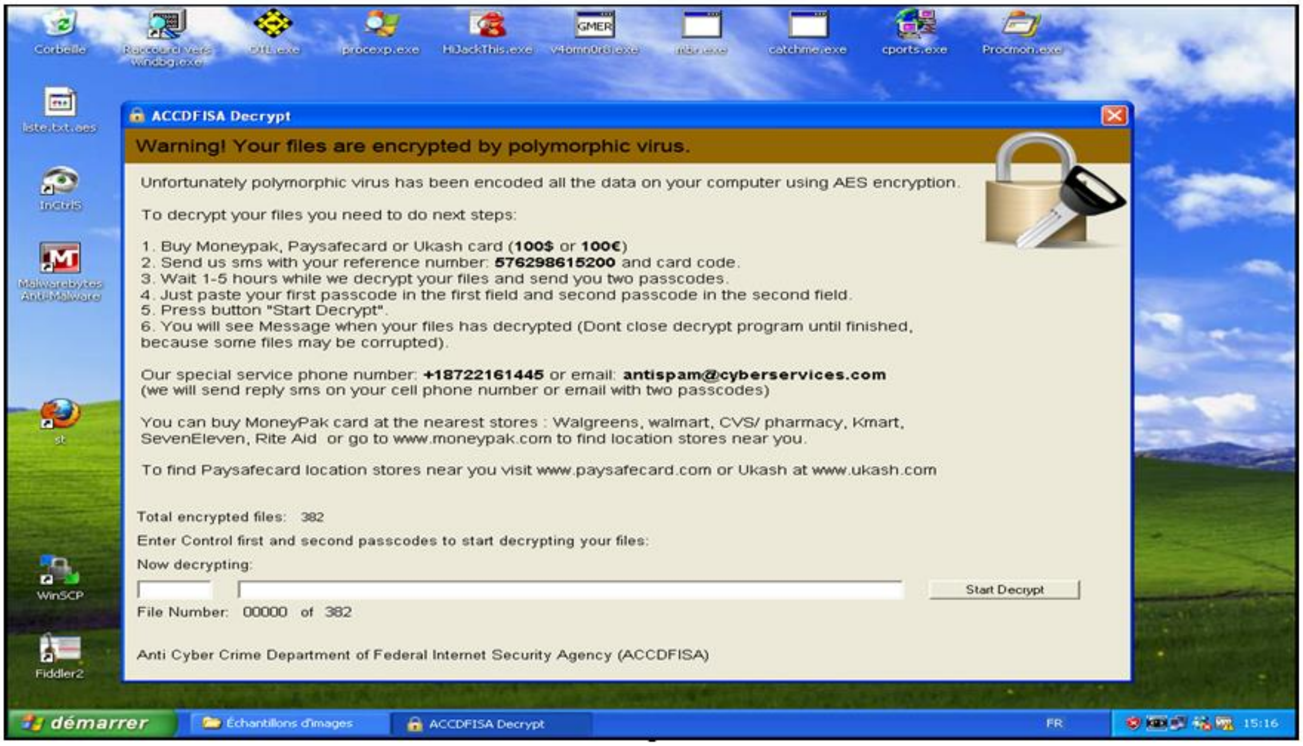
- •DEFINITION
- •CONTRACTING the MALWARE
- •TYPES of RANSOMWARE
- •COUNTER MEASURES
- •REMOVAL

Irv Salzberg
3/21/13

Submitted by Barry Hammond

DEFINITION

Ransomware comprises a class of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed.



ACCDFISA Decrypt

Warning! Your files are encrypted by polymorphic virus.

Unfortunately polymorphic virus has been encoded all the data on your computer using AES encryption.

To decrypt your files you need to do next steps:

1. Buy Moneypak, Paysafecard or Ukash card (**100$** or **100€**)
2. Send us sms with your reference number: **576298615200** and card code.
3. Wait 1-5 hours while we decrypt your files and send you two passcodes.
4. Just paste your first passcode in the first field and second passcode in the second field.
5. Press button "Start Decrypt".
6. You will see Message when your files has decrypted (Dont close decrypt program until finished, because some files may be corrupted).

Our special service phone number: **+18722161445** or email: **antispam@cyberservices.com**
(we will send reply sms on your cell phone number or email with two passcodes)

You can buy MoneyPak card at the nearest stores : Walgreens, walmart, CVS/ pharmacy, Kmart, SevenEleven, Rite Aid or go to www.moneypak.com to find location stores near you.

To find Paysafecard location stores near you visit www.paysafecard.com or Ukash at www.ukash.com

Total encrypted files: 382

Enter Control first and second passcodes to start decrypting your files:

Now decrypting:

File Number: 00000 of 382

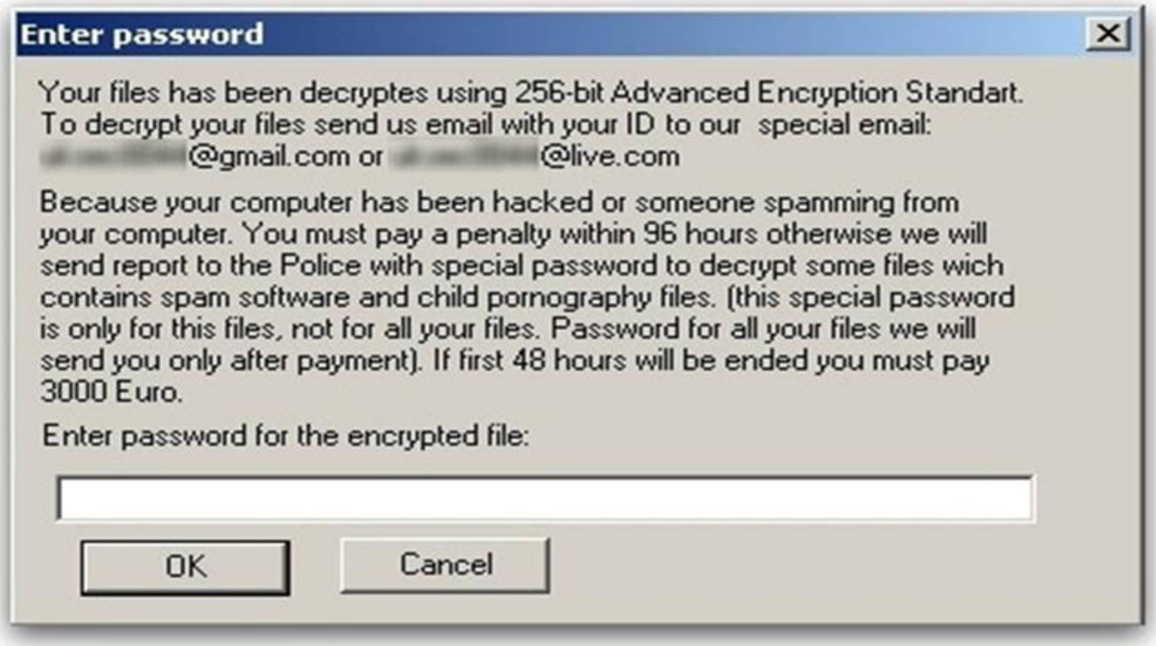
Anti Cyber Crime Department of Federal Internet Security Agency (ACCDFISA)

Submitted by Barry Hammond

HOW IS RANSOMWARE CONTRACTED

- installed from an e-mail attachment,
- an infected program,
- a compromised or malicious web site.

!YOU HAVE TO CLICK ON AN EXECUTABLE FILE OR A DOWNLOAD!



Your files has been decryptes using 256-bit Advanced Encryption Standart.
To decrypt your files send us email with your ID to our special email:
[redacted]@gmail.com or [redacted]@live.com

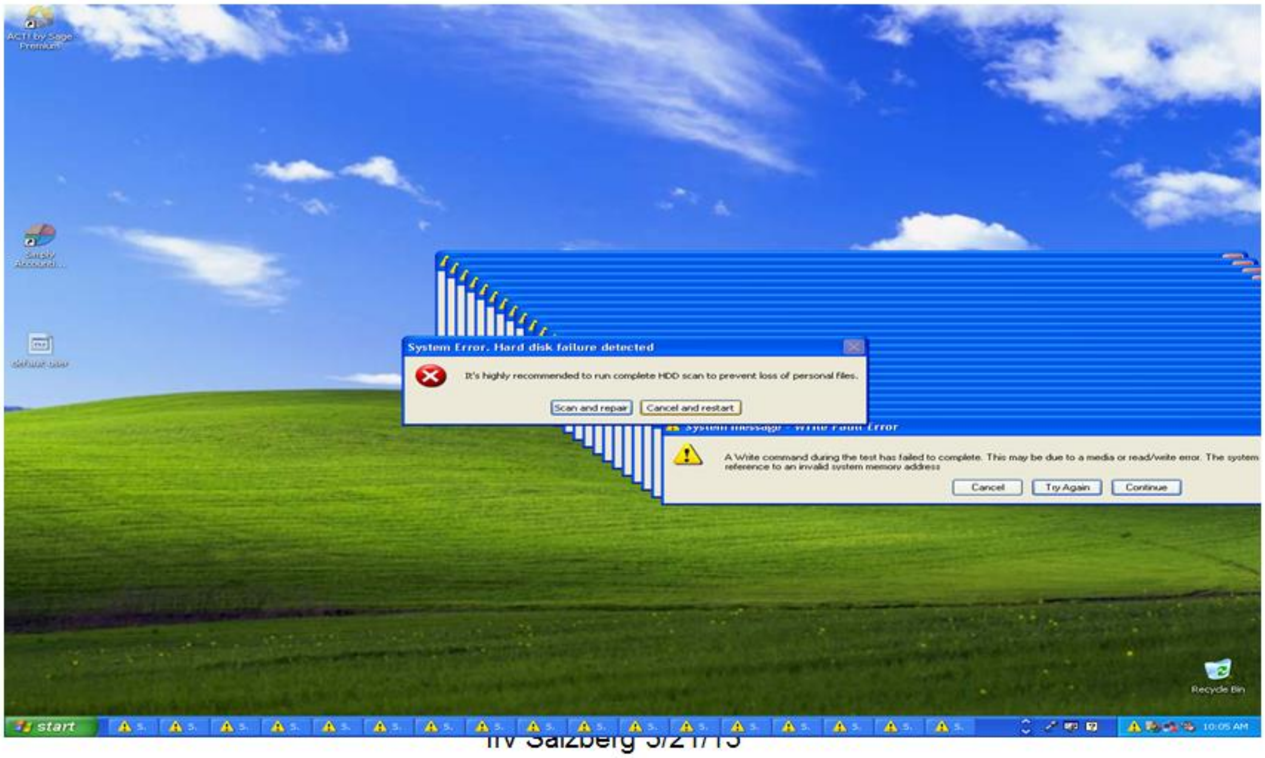
Because your computer has been hacked or someone spamming from your computer. You must pay a penalty within 96 hours otherwise we will send report to the Police with special password to decrypt some files wich contains spam software and child pornography files. (this special password is only for this files, not for all your files. Password for all your files we will send you only after payment). If first 48 hours will be ended you must pay 3000 Euro.

Enter password for the encrypted file:

Submitted by Barry Hammond

TYPES of RANSOMWARE

- Repeating advertising displays. EFFECT: continuously interrupting applications and slowing computer operations.
- Computer screen lockup. EFFECT: Inability to access files or applications.
- MFT (Master File Table) corruption. EFFECT: Doomsday.
- File encryption: EFFECT: Doomsday.



System Error. Hard disk failure detected

It's highly recommended to run complete HDD scan to prevent loss of personal files.

System message - Write Fault Error

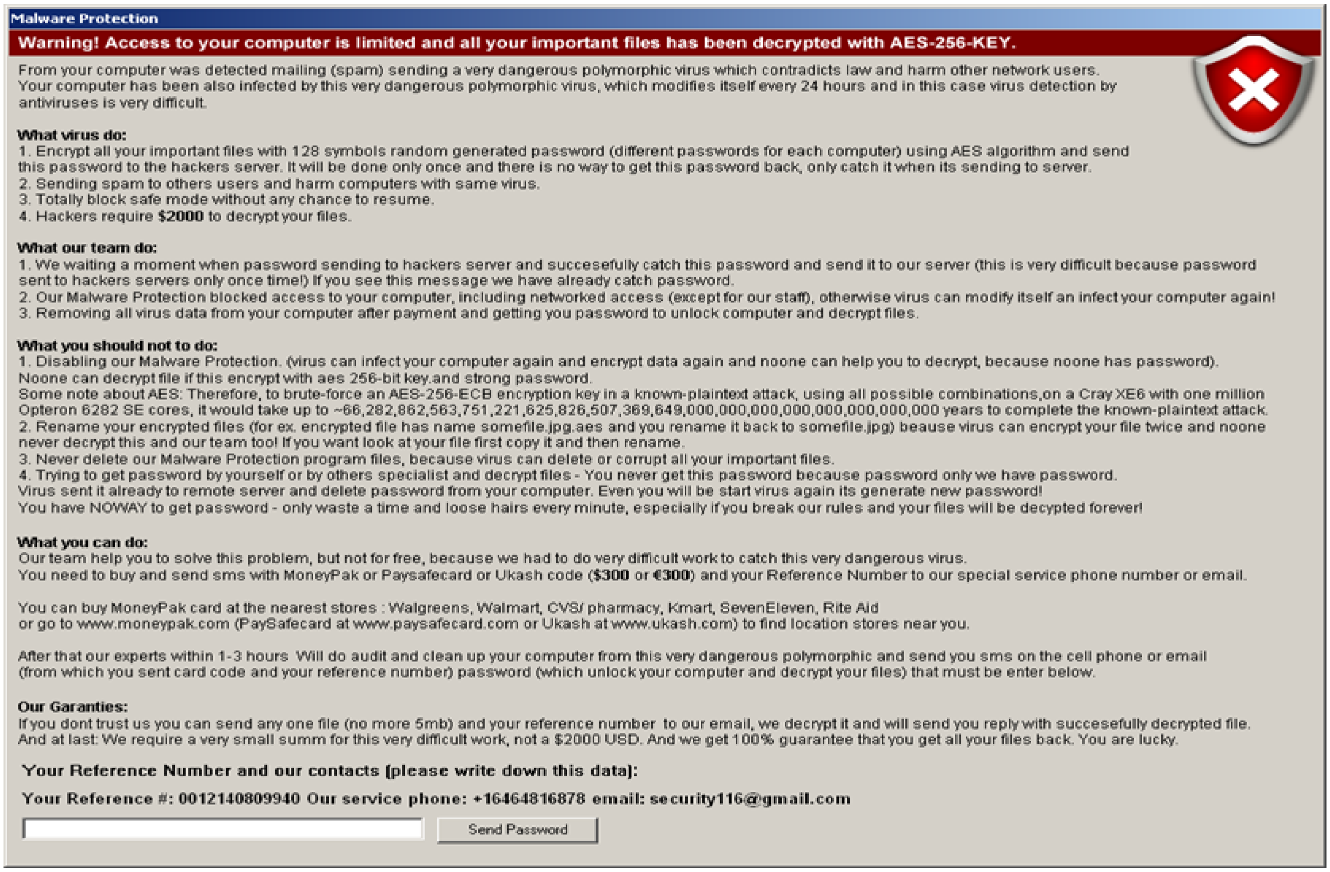
A Write command during the test has failed to complete. This may be due to a media or read/write error. The system reference to an invalid system memory address

Irv Salzberg 3/21/13

Submitted by Barry Hammond

PREVENTIVE COUNTERMEASURES

- Watch where you click.
- Periodic backups.
- Periodic backups.
- Periodic backups.
- Use of antivirus software is no guarantee of protection but its better than nothing.



Warning! Access to your computer is limited and all your important files has been decrypted with AES-256-KEY.

From your computer was detected mailing (spam) sending a very dangerous polymorphic virus which contradicts law and harm other network users.
Your computer has been also infected by this very dangerous polymorphic virus, which modifies itself every 24 hours and in this case virus detection by antiviruses is very difficult.

What virus do:
1. Encrypt all your important files with 128 symbols random generated password (different passwords for each computer) using AES algorithm and send this password to the hackers server. It will be done only once and there is no way to get this password back, only catch it when its sending to server.
2. Sending spam to others users and harm computers with same virus.
3. Totally block safe mode without any chance to resume.
4. Hackers require **$2000** to decrypt your files.

What our team do:
1. We waiting a moment when password sending to hackers server and succesefully catch this password and send it to our server (this is very difficult because password sent to hackers servers only once time!) If you see this message we have already catch password.
2. Our Malware Protection blocked access to your computer, including networked access (except for our staff), otherwise virus can modify itself an infect your computer again!
3. Removing all virus data from your computer after payment and getting you password to unlock computer and decrypt files.

What you should not to do:
1. Disabling our Malware Protection. (virus can infect your computer again and encrypt data again and noone can help you to decrypt, because noone has password).
Noone can decrypt file if this encrypt with aes 256-bit key.and strong password.
Some note about AES: Therefore, to brute-force an AES-256-ECB encryption key in a known-plaintext attack, using all possible combinations,on a Cray XE6 with one million Opteron 6282 SE cores, it would take up to ~66,282,862,563,751,221,625,826,507,369,649,000,000,000,000,000,000,000 years to complete the known-plaintext attack.
2. Rename your encrypted files (for ex. encrypted file has name somefile.jpg.aes and you rename it back to somefile.jpg) beause virus can encrypt your file twice and noone never decrypt this and our team too! If you want look at your file first copy it and then rename.
3. Never delete our Malware Protection program files, because virus can delete or corrupt all your important files.
4. Trying to get password by yourself or by others specialist and decrypt files - You never get this password because password only we have password.
Virus sent it already to remote server and delete password from your computer. Even you will be start virus again its generate new password!
You have NOWAY to get password - only waste a time and loose hairs every minute, especially if you break our rules and your files will be decypted forever!

What you can do:
Our team help you to solve this problem, but not for free, because we had to do very difficult work to catch this very dangerous virus.
You need to buy and send sms with MoneyPak or Paysafecard or Ukash code (**$300** or **€300**) and your Reference Number to our special service phone number or email.

You can buy MoneyPak card at the nearest stores : Walgreens, Walmart, CVS/ pharmacy, Kmart, SevenEleven, Rite Aid
or go to www.moneypak.com (PaySafecard at www.paysafecard.com or Ukash at www.ukash.com) to find location stores near you.

After that our experts within 1-3 hours Will do audit and clean up your computer from this very dangerous polymorphic and send you sms on the cell phone or email (from which you sent card code and your reference number) password (which unlock your computer and decrypt your files) that must be enter below.

Our Garanties:
If you dont trust us you can send any one file (no more 5mb) and your reference number to our email, we decrypt it and will send you reply with succesefully decrypted file.
And at last: We require a very small summ for this very difficult work, not a $2000 USD. And we get 100% guarantee that you get all your files back. You are lucky.

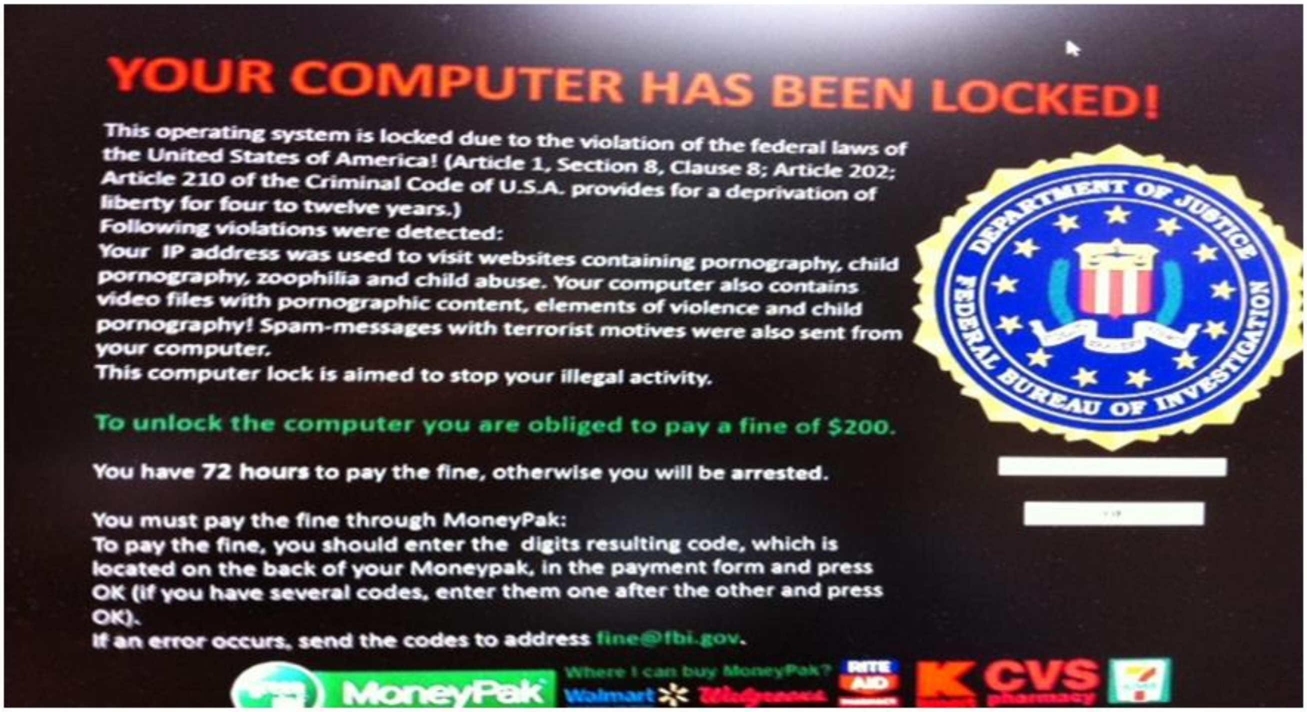
Your Reference Number and our contacts (please write down this data):

Your Reference #: 0012140809940 Our service phone: +16464816878 email: security116@gmail.com

Submitted by Barry Hammond

REMOVAL

- NEVER pay the ransom
- Run antivirus software,
- Identify specific ransomware version and check the internet for removal instructions,
- Safe boot,
- Use computer recovery function,
- Malwarebytes software.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Submitted by Barry Hammond

Presentation No. 2 by Dan Lee:

Dan Lee gave a presentation about how he replaced the screen on a Dell Latitude D520 laptop computer that had been dropped. He showed before and after pictures of the damaged laptop plus a YouTude video of a similar model being repaired by a technician. He said a screen replacement by the Geek Squad or similar company could cost in the $300 range. He paid just $20.95 for a screen from EBay.

Bob Blum brought in and gave away some unneeded items.

Computer Problems:

GwenDoly Yarborough requested assistance with a Compaq Presario 2500 with a wildly flickering screen. When connected to the senior center's projector, the desktop image appeared normal. This was an older computer which also had a dead battery. She was advised that it did not make sense to put more money into it. Besides the obvious issue with the screen, there are other related items that could be causing the screen to not display properly. One suggestion made was that she connect it to a separate monitor and use it like a desktop.

Russ Vaughan asked for advice on how to improve Wi-Fi in his house. Several suggestions were offered by club members. Bob Rapczynski suggested installation of a Wi-Fi "extender" and offered to provide an extra one he had.

Submitted by Barry Hammond