IT HAPPENED TO US…

…and yes, it can happen to you

February 2016 Ransomware Event at Horry County Schools

Charles C. Hucks, Jr.
chucks@horrycountyschools.net

Ransomware is on track to be a $1 billion business in 2016, despite the fact that the FBI recommends victims not pay their attackers but contact law enforcement instead.

CNBC

HACKERS

Hollywood hospital hit by ransomware attack, hackers demand $3.6M

FOX NEWS Tech

Ransomware spiked 6,000% in 2016 and most victims paid the hackers, IBM finds

CNBC

Monday, February 8, 2016

Horry County Schools struck by 'ransomware' virus

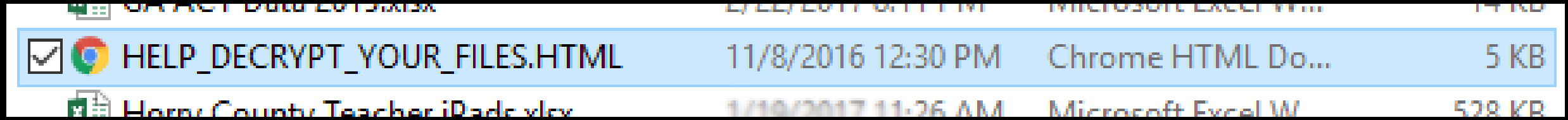
WMBF NEWS

A day which will live in infamy

'Ransomware' crime wave growing

by David Fitzpatrick and Drew Griffin @CNNTech

It began with an early morning phone call and instant fear for the technology director of Horry County, South Carolina's school district.


HELP_DECRYPT_YOUR_FILES.HTML
11/8/2016 12:30 PM
Chrome HTML Do...
5 KB


RANSOMWARE • RANSOMWARE • RANSOMWARE

THE NOTE

#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us 1.5 Bitocin for each affected PC OR 22 Bitocin to receive ALL Private Key for ALL affected PC.

Step2: After you send us 1.5 Bitocin, Leave a comment on our blog with this detail: Just write Your "Computer name" in your comment

*Your Computer name is:AHFS1

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our blog address: https://helpbyangel0.wordpress.com

*Our Bitcoin address: 1ETLG9xnFwZ1H9xaHz6u4MX8KYvWJesMab

(If you send us 22 Bitocin For all PC, Leave a comment on our blog with this detail: Just write "For All Affected PC" in your comment)

#What is Bitcoin?

Bitcoin is an innovative payment network and a new kind of money.
You can create a Bitcoin account at https://blockchain.info/ and deposit some money into your account and then send to us

#How to buy Bitcoin?

There are many way to buy Bitcoin and deposit it into your account,
You can buy it with WesternUnion, Bank Wire, International Bank transfer, Cash deposit and etc

https://www.bitquick.co/buy-2.php ---> Buy Bitcoin Fast and secure in one hour with cash deposit

https://coincafe.com/buybitcoinswestern.php ---> Buy Bitcoin fast and Secure with WesternUnion and Cash deposit

https://localbitcoins.com/country/US ---> Buy Bitcoin with WesternUnion or MoneyGram or Cash Deposit

https://localbitcoins.com/buy-bitcoins-online/usd/western-union/ ---> Buy Bitcoin with WesternUnion or MoneyGram

https://coinchimp.com ---> Buy Bitcoin with bank wire, Locally, Western Union

https://www.kraken.com ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

https://www.ccedk.com ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

https://bitcurex.com/ ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

If you want to pay with your Business bank account you should create a business account in exchangers
they don't accept payment from third party

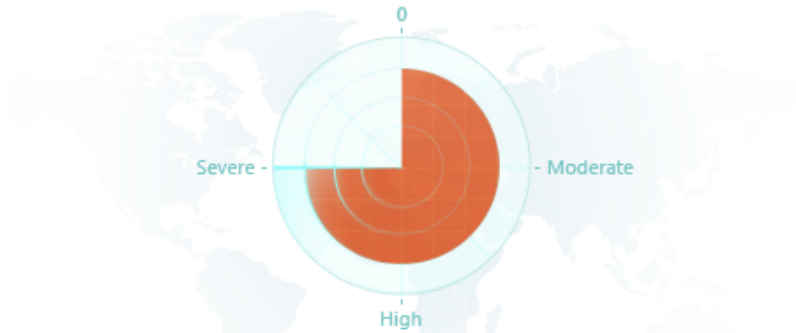
#deadline

You just have 7 days to send us the Bitcoin after 7 days we will remove your private key and it's impossible to recover your files

WHAT HIT US

Ransom: MSIL/Samas.A

Also detected as:



Ransom:MSIL/Samas.A
Alert level: **Severe**

First published: Oct 14, 2014
Latest published: Jul 06, 2016

Summary | What to do now | Technical information | Symptoms

Windows Defender detects and removes this threat.

This ransomware family encrypts the files on your PC. It shows you a message that says you must pay for decryption software to get access to your files again.

You can read more about this type of threat on our ransomware page.

HOW IT HAPPENED

- Old server, kept for historical data access ONLY
- Application not updated/support not paid
- OS updated but application support components could not be
- Exploit in JBOSS
  - Right Place, Right Time
- Obtained access to Domain Administrator account
- Spread across district encrypting files

GENERAL INFO

- Always at least two parts to a malware infection
  1. Entry point
     - Email
       - Malicous Attachment
       - Social Engineering
     - Online link
     - Vulnerability in publicly accessible resources
  2. Execution/spread of the malicious intent
     - Data encryption and/or deletion
     - Data extraction
       - Via malware
       - Via deceived humans

PREVENTION

TO: District Superintendents

FROM: Kenneth B. Puett, CISSP
Chief Information Security Officer

DATE: February 19, 2016

RE: Ransom-ware Infection

While no one security system can protect our educational institutions from viruses, malware, and even ransom-ware, the following are widely accepted technology practices which can minimize exposure.

1. Make sure you have updated antivirus software on your computers. Both the signature patterns and engine should be updated frequently.

2. Enable automated patches for your operating system and Web browser. Additionally, 3rd party software such as Java, Adobe Flash, etc., should be kept up to date and older software removed.

3. Have strong passwords, and don't use the same passwords for everything. Passwords should be changed on a frequency between 30 to 90 days and privilege user management passwords should be changed more often.

4. Use a pop-up blocker.

5. Only download software—especially free software—from sites you know and trust (malware can also come in downloadable games, file-sharing programs, and customized toolbars). Poor browsing habits are a leading contributor to malware infections.

6. Do not open attachments in unsolicited emails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited email, even if you think it looks safe. Instead, close out the email and go to the organization's website directly.

7. To prevent the loss of essential files and systems due to a ransom-ware infection, it is recommended that individuals and businesses always conduct regular system back-ups and store the backed-up data offline. Test the backup frequently to insure that files and systems can be fully restored.

8. Security Awareness and Training. Inform users of common practices of phishing email attacks and unsubscribe to non-business related communications. Many ransomware attacks are committed using email systems.

The South Carolina Department of Education is committed to protecting our students' and teachers' sensitive data by proactively addressing security concerns as well as providing relevant and timely security expertise to our school districts and their technology personnel. Our Chief Information Security Office can offer assistance in a variety of methods and can be reached at (803) 734-8301.

Here are a few tips that will help you keep ransomware from wrecking your day:

1. Back up your data. ...
2. Show hidden file-extensions. ...
3. Filter EXEs in email. ...
4. Disable files running from AppData/LocalAppData folders. ...
5. Use the Cryptolocker Prevention Kit. ...
6. Disable RDP. ...
7. Patch or Update your software. ...
8. Use a reputable security suite.

More items...

11 things you can do to protect against ransomware, including ...
www.welivesecurity.com/.../11-things-you-can-do-to-protect-against-ransomware-includ...

About this result • Feedback

TIMELINE

- 8th
  - malware executed
  - ALL servers shut down
  - recommended paying ransom
- 9th
  - PowerSchool and PeopleSoft (core) operational
  - Login/Network/Internet access available
  - Established first Bitcoin account
- 10th
  - Payroll processed

- 11th
  - Superintendent recommends payment to Board
  - Board approves payment
- 12th
  - Funds wired, attempt to exchange to Bitcoin
  - Discover “safe” Bitcoin transfer not a quick
- 13th
  - Investigate alternative Bitcoin transfer methods
  - Ask culprits for extension, until 22nd granted (how nice of them)
- 14th
  - Enrich, other systems continue to be restored

- 17th
  - Unsolicited contact from Axiom Cyber Solutions
- 19th
  - Agreement with Axiom to pay
- 20th
  - WordPress site taken down for EULA violations
- 21st
  - Send memo with BitCoin transfer?
  - 2:05 pm sent $1.00
  - 6:03 pm email response received from culprit

- 22nd
  - 12:13 am sent 1.5 BitCoin for one key
  - 1:37 am received decryption key
  - 2:00 am confirmed key worked
  - 2:05 am authorized send of balance for all keys
  - 3:26 pm received delay notification
- 23rd
  - 5:10 pm sent 20.5 BitCoin for balance
  - 5:27 pm received remaining keys (all worked)

- 24th
  - Engaged SecureWorks
- 4th
  - Restorations/Rebuilds complete

LESSONS LEARNED

- Backups
  - Not as simple as “do you have”
  - Location
  - Restores
    - Time
    - Permissions
- All it takes is ONE
- Not unlike many other “unpleasant” payments

FEBURARY 8, 2017