



Our webinar will begin shortly.



**The Wild Wild West: How Ransomware Is
Changing The Face Of Cyber Security**

July 25, 2017

*Mark Stoudemire & Luke Nesman
Clark Schaefer Consulting*





The Wild Wild West: How Ransomware Is Changing The Face Of Cyber Security

July 25, 2017

Mark Stoudemire & Luke Nesman
Clark Schaefer Consulting



Questions

- How to ask a question during today's webinar?
- Use the "Chat" or "Question" feature on the GoToWebinar panel.
- You can also email DeAnna Bird at dbird@clarkschaefer.com.
- Questions will be addressed at the end of the webinar.

CPE

- CPE is available for this event.
- You will receive an email by the end of the day that will contain today's presentation & CPE form.
- You will receive 3 CPE codes during today's presentation.
- Record those 3 CPE codes to complete the CPE form.

Introductions



Mark Stoudemire, CCNA, CEH, CHFI Consultant, Columbus Office

- IT Networking and Sys Admin background
- Masters in IT Security and Assurance from Western Governors University
- Marks hobbies include gaming (like any good cyber security expert), playing sports and movies every weekend

Introductions



Luke Nesman, GSEC Consultant, Cincinnati Office

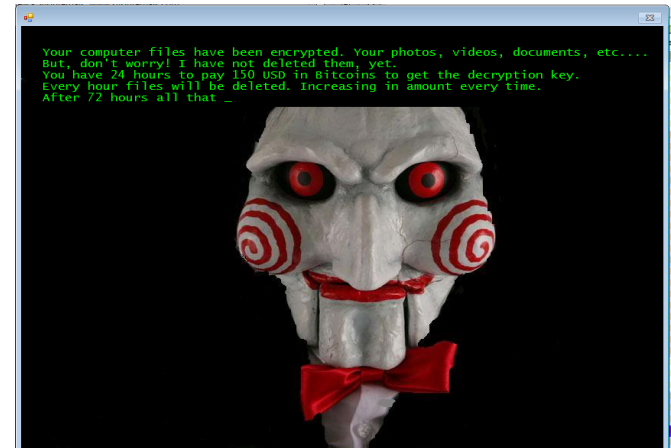
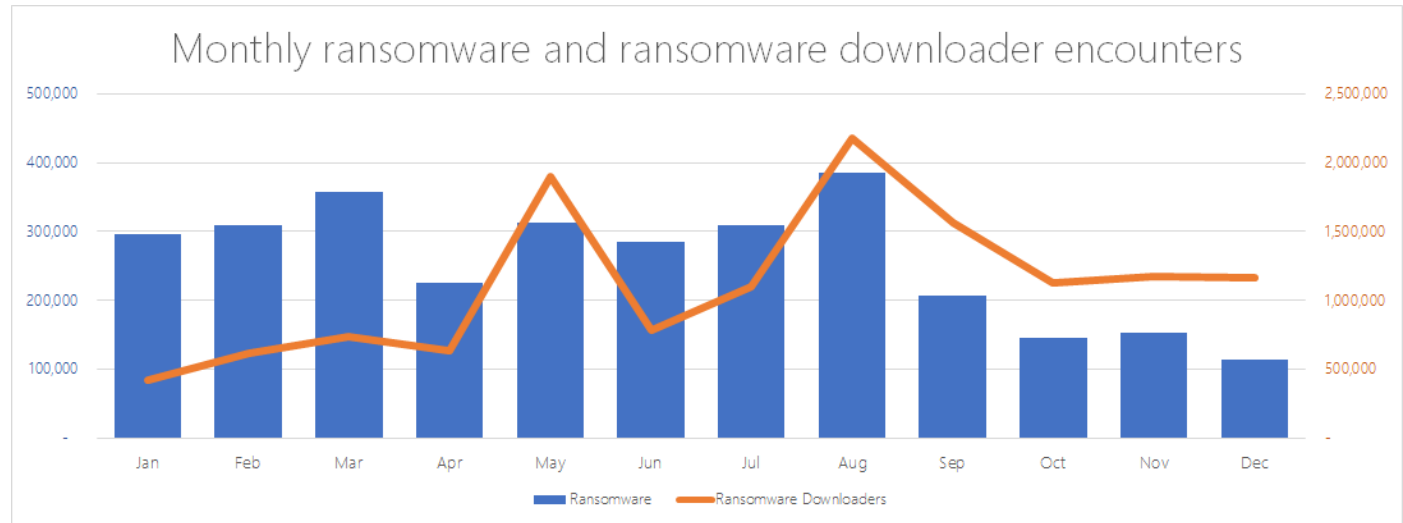
- IT/Network Security background in non-profit and large businesses.
- Experience with networking, monitoring, IR, and audit projects both in the internal and consulting side
- Passionate about the intersection of IT, Security, and people.
- Expert napper, anytime, any place.

What is Ransomware?

- Malicious software
- Distributed via phishing emails & exploit kits
- Typically runs out of the `%AppData%` or `%Temp%` folders
- Achieves persistence on infected systems
- Encrypts data
- Leaves ransom note with instructions on how to pay ransom with bitcoin
- No guarantee that paying ransom will get you your data back

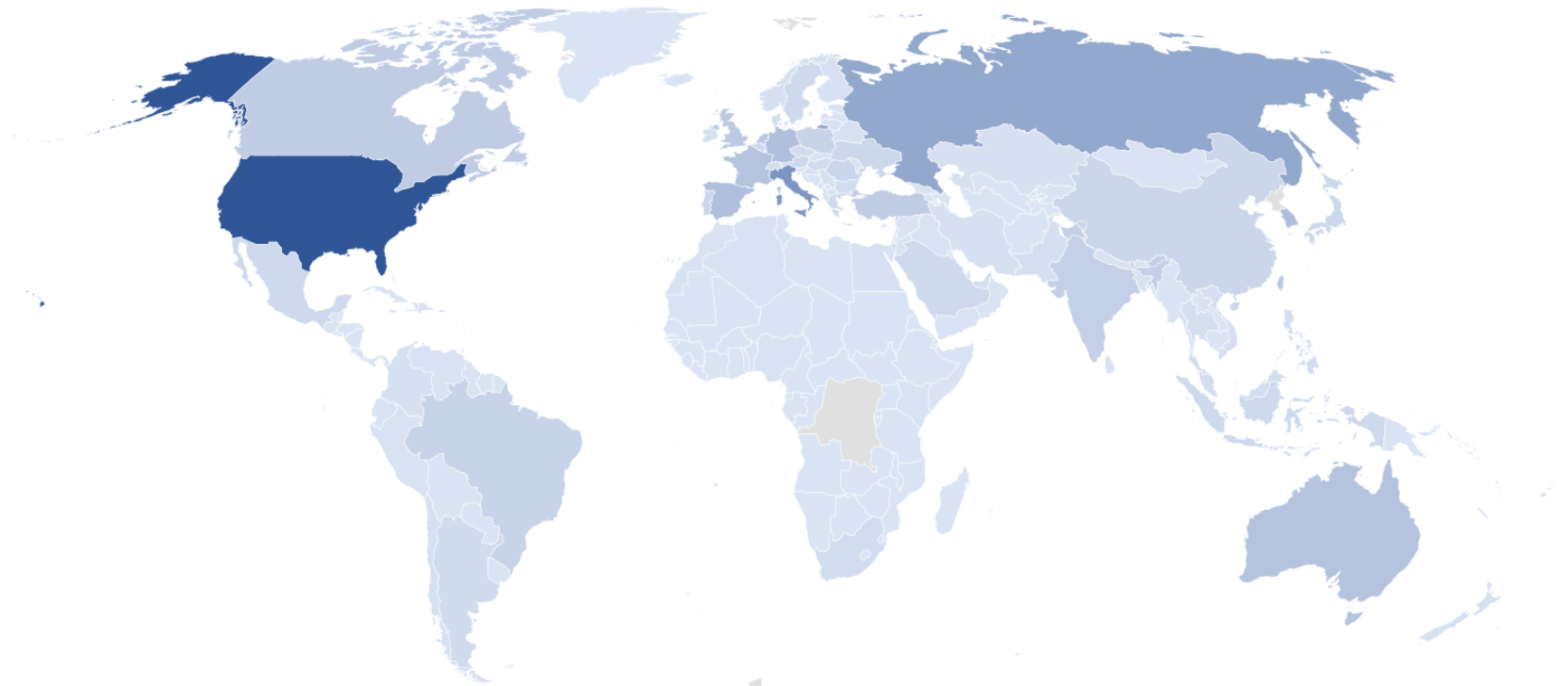


What is Ransomware?



Ransomware Attack Distribution

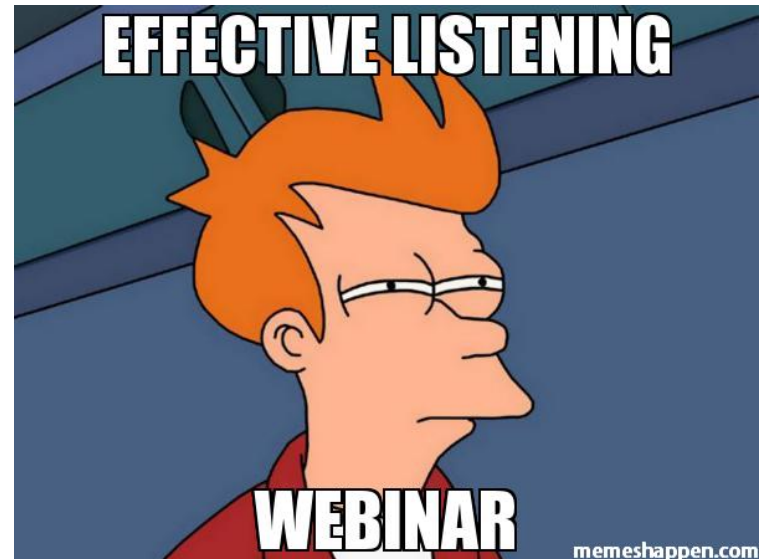
Geographic distribution of ransomware encounters 2016



Powered by Bing
© DSAT for MSFT, GeoNames, Microsoft, Navteq, Thinkware Extract, Wikipedia

Agenda

- Brief History of Ransomware
- Preparing for the storm
- “We Must Protect this house”
- Recovery
- Cyber Insurance
- Conclusion



History of Ransomware: 1989, AIDS Virus

I N T R O D U C T I O N

Welcome to the interactive computer program called AIDS Information. This program is designed to provide up-to-date information about you and the fatal disease AIDS (Acquired Immune Deficiency Syndrome). The health information provided to you by this program could save your life.

Here is how the program works: First, the computer will ask you a series of questions about your personal background, behaviour and medical history. Then the program will calculate your chances of being infected with the AIDS virus and inform you about your present degree of risk. Then it will provide you with advice on what you can do to reduce your risk of future infection, based on the details of your own lifestyle and history. Finally, it will give you the chance to ask questions or to make comments.

Press ENTER to continue or

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

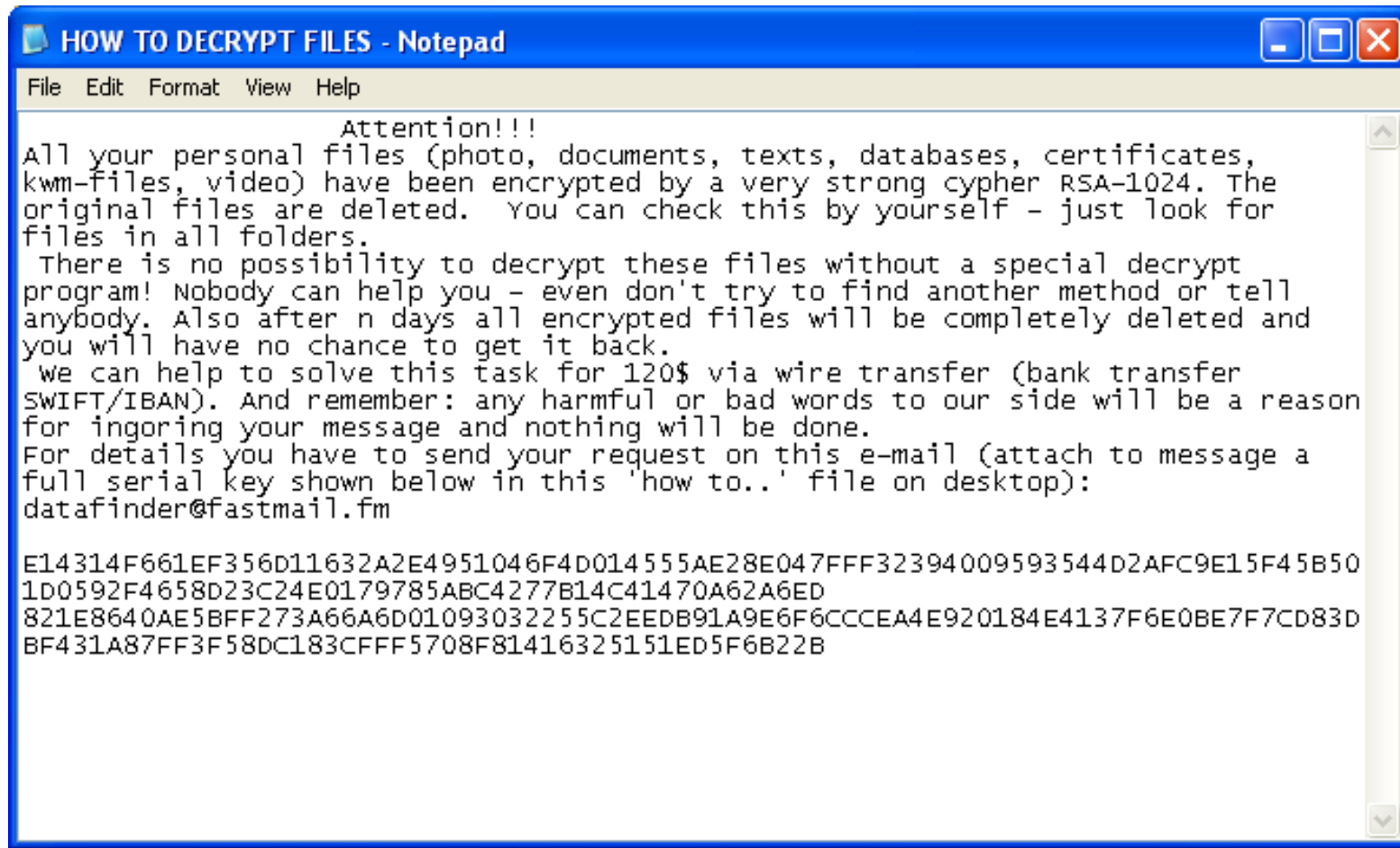
- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: 1234567890

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

History of Ransomware: 2006, Archiveus & GPcode Trojan



HOW TO DECRYPT FILES - Notepad

File Edit Format View Help

Attention!!!
All your personal files (photo, documents, texts, databases, certificates, kwm-files, video) have been encrypted by a very strong cypher RSA-1024. The original files are deleted. You can check this by yourself - just look for files in all folders.
There is no possibility to decrypt these files without a special decrypt program! Nobody can help you - even don't try to find another method or tell anybody. Also after n days all encrypted files will be completely deleted and you will have no chance to get it back.
We can help to solve this task for 120\$ via wire transfer (bank transfer SWIFT/IBAN). And remember: any harmful or bad words to our side will be a reason for ignoring your message and nothing will be done.
For details you have to send your request on this e-mail (attach to message a full serial key shown below in this 'how to..' file on desktop):
datafinder@fastmail.fm

E14314F661EF356D11632A2E4951046F4D014555AE28E047FFF32394009593544D2AFC9E15F45B50
1D0592F4658D23C24E0179785ABC4277B14C41470A62A6ED
821E8640AE5BFF273A66A6D01093032255C2EEDB91A9E6F6CCCEA4E920184E4137F6E0BE7F7CD83D
BF431A87FF3F58DC183CFFF5708F81416325151ED5F6B22B

History of Ransomware: 2007, Winlock

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 I, Section 8, Clause 8; 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 to 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.

 Enter

MoneyPak

Where I can buy MoneyPak?

Walmart Walgreens



History of Ransomware: 2012, Citadel



Attention!

This operating system is locked due to the violation of the federal laws of the United States of America! 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 \$ 100.

You must pay the forfeit through Paysafecard:

To do this, you should enter the 16 digits resulting code (if necessary with a password) 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 cybercrime@worldinternetpolice.net



 **Where can I buy Paysafecard?**
paycash, paysafe.

Paysafecard is available from 350,000 sales outlets worldwide, in the United States from iPP, ePAY, precash and blackhawk outlets.



 **Ukash**

 **paysafecard**
paycash, paysafe.

History of Ransomware: 2013, Cryptolocker

- Spread via phishing emails & compromised websites
- Attachment is an executable
- 4 day time limit on payment of ransom
- Distributed by the Gameover Zeus Botnet



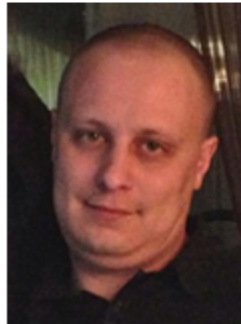
Evgeniy Mikhailovich: Zeus & Cryptolocker Author



**WANTED
BY THE FBI**

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud



DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhailovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	Hair: Brown (usually shaves his head)
Eyes: Brown	Height: Approximately 5'9"

History of Ransomware: 2014, Cryptowall

- Gained popularity and notoriety after Zeus and Cryptolocker were taken down with Operation Tovar and the arrest of Evgeniy Mikhailovich
- Distributed via exploit kits, spam campaigns and malvertising.
- Employed the tactic of allowing 1 file to be unencrypted “free of charge” to increase credibility and income from their ransomware campaigns.

History of Ransomware: 2015, Ransomware as a service



The screenshot displays the user interface for 'Tox - Viruses', a ransomware as a service. The interface is dark-themed with green accents. At the top left is a biohazard icon. The title 'Tox - Viruses' is in large green font, with the identifier 'toxicola7qww37qj.onion' below it. A 'Summary' section shows statistics: 1 Virus, 6 Infected, and 0 Of which paid. It also displays 'Total profit' as 0.00 \$ and 'To withdraw (net)' as 'Currently unavailable'. A 'Withdraw' button is present next to a 'Your BTC address' input field. Below the summary is a 'Create a virus' section with three input fields: 'Ransom - \$' (with a note 'Ransom in dollars (min. 50)'), 'Notes' (with a note 'Optional, ex: For Mr. Smith'), and 'Captcha'.

Tox - Viruses
toxicola7qww37qj.onion

Summary

Viruses	1	Total profit	0.00 \$
Infected	6	To withdraw (net)	Currently unavailable
Of which paid	0	Your BTC address	<input type="text"/>

Create a virus

Ransom - \$ Ransom in dollars (min. 50)

Notes Optional, ex: For Mr. Smith

Captcha

History of Ransomware: 2016, Locky

We present a special software - **Locky Decrypter** -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.



2. You should register BitCoin wallet ([simplest online wallet](#) OR [some other methods of creating wallet](#))
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

4. Send - **0.5** BTC to Bitcoin address:

1

(Payment pending up to 30 mins or more, be patient...)

5. Refresh the page and download decoder.

4. Send - **1.00** BTC to Bitcoin address:

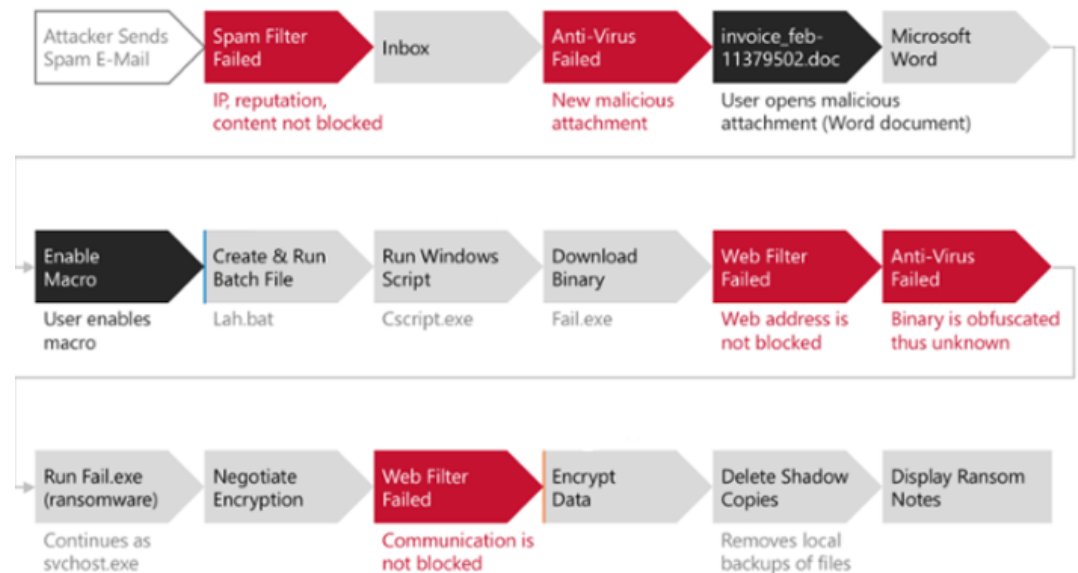
1

5. Refresh the page and download decoder.

Different ransom demands by "Locky" at different times

History of Ransomware: 2016, Locky

- Spread originally via phishing campaigns
- Emails typically contain a word document with a malicious macro that infects you if the user is duped into enabling macros
- Anti-sandbox technology built in



History of Ransomware: 2017, Samas, Wanacry, Peyta

- **Samas** is known for being highly aggressive and attempts to infect all machines on your network through vulnerable JBOSS applications
- Uses stolen credentials to gain access to networks and infect machines with Samas
- **Wanacry** uses the leaked NSA vulnerability EternalBlue that exploits a SMBv1 Vulnerability
- **Peyta 2.0** = wiper

Preparing for the Storm

- Backups, backups, and more backups
 - Offline backups;
 - Cloud Services
 - Continuous File Backups
 - Network Attached Storage
- Patching
 - Keep Software up to Date



Protect this House

- System-Level Protection
 - Whitelisting
 - Anti-Virus/Anti-Malware
 - Access Controls
- Network-Level
 - Firewall
 - Email



Protect this House Cont.

- End-Users
 - Awareness training
 - Prevention steps
 - Security testing



"MAYBE WE NEED TO RETHINK OUR PRESENTATION."

Recovery



- Find the infected device or devices
 - Disconnect from network
 - Recover files from backups
 - Resume business operations
-
- Review logs or full packet capture to determine attack vector and security holes
 - Patch vulnerabilities/educate users
 - Investigate any evidence of further compromise or lateral movement

Latest Threats : NotPetya

■ What is NotPetya?

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

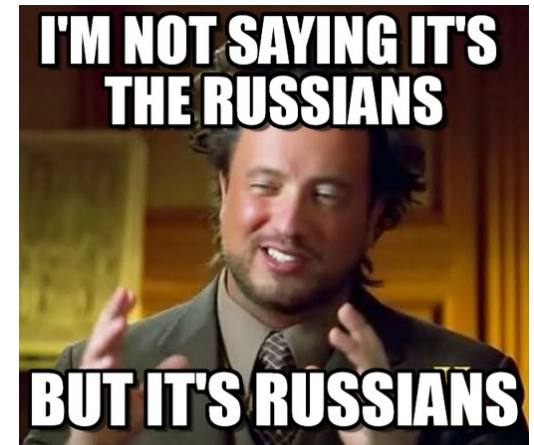
74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizU-gUeUMa

If you already purchased your key, please enter it below.

Key: _

Latest Threats: NotPeyta

- Spread through MeDoc software update used by 80% of Ukrainian business.
- Infected companies like pharmacy giant Merk to the shipping company Maersk to Ukraine's electric utilities



Latest Threats: NotPetya

■ How NotPetya works?

```
Repairing file system on C:
```

```
The type of the file system is NTFS.  
One of your disks contains errors and needs to be repaired. This process  
may take several hours to complete. It is strongly recommended to let it  
complete.
```

```
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD  
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED  
IN!
```

```
CHKDSK is repairing sector 41024 of 303584 (13%)
```

```
Oops, your important files are encrypted.
```

```
If you see this text, then your files are no longer accessible, because they  
have been encrypted. Perhaps you are busy looking for a way to recover your  
files, but don't waste your time. Nobody can recover your files without our  
decryption service.
```

```
We guarantee that you can recover all your files safely and easily. All you  
need to do is submit the payment and purchase the decryption key.
```

```
Please follow the instructions:
```

```
1. Send $300 worth of Bitcoin to following address:
```

```
1Mz7153HMuxXTuR2R1t70mGSdzaftNbBWX
```

```
2. Send your Bitcoin wallet ID and personal installation key to e-mail  
wowsmith123456@posteo.net. Your personal installation key:
```

```
74f296-2Nx1Gw-yHQRMr-S0gaN6-8Bs1fd-U2DKui-ZZpRJE-kEGsSN-o8tizU-gUeUMa
```

```
If you already purchased your key, please enter it below.
```

```
Key: _
```

Latest Threats: NotPetya

Mitigation Techniques

- Don't pay the Ransom
- Install Patch MS017-10
- Power off machine immediately
- Update Antivirus Signatures

Reasons to Consider Cyber Insurance

- Dollar values can be assigned to an the organization's cyber risk.
- Insurance underwriters can assist organizations with identifying cyber security gaps and weaknesses.
- Other benefits cyber insurance brings to the organization

Types of Coverages

Network Security

First-party

- Business Interruptions*
- Data Replacement*
- Cyber Extortion
- Crisis Management
 - Public Relations
 - Forensic
 - Legal

Third-party

- Customer suits
- Other Third-party suits

* May be subject to sub-limits

Privacy

First-party

- Notification Costs*
- Credit Monitoring*
- Crisis Management
 - Public Relations
 - Forensic
 - Legal

Third-party

- Consumer suits
- Regulatory
 - Defense
 - Fines
 - Penalties
- Charges levied by Credit Card Issuers
- PCI-DSS fines*

* May be subject to sub-limits

Good Security Resources

- Cisco's video, "Anatomy of an attack"
- KnowBe4 blog
- Talos, threat research blog
- SANS Internet Storm Center
- Krebs on Security
- Black Hills Information Security Blog

Questions?

If you wish to discuss any aspect of this presentation in more detail, please feel free to contact me:

Luke Nesman

lnesman@clarkschaefer.com

(513) 371-5648

Mark Stoudemire

mstoudemire@clarkschaefer.com

(614) 607-5716

