



CYBER SECURITY
SUMMIT 2016

Ransomware Destructive Attack

Jay Spreitzer, Vice President, Cyber Threat Management
Wells Fargo Bank



About - Jay Spreitzer



Has over 18 years information security experience. Over the last 10 years as a senior member of a cyber intelligence team at Wells Fargo. Prior to joining Wells Fargo Jay retired from the US Army, after 23 years of service working in various technology and information security roles. He holds a Masters in Information Assurance and Security as well as multiple computer security certifications.

What is ransomware?

Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction.

Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying.

What is ransomware?

Ransomware wreaking havoc in American and Canadian hospitals
Tech & Science March 23, 2016

Spike in ransomware spam prompts warnings
Technology, March 10, 2015

Ransomware alert issued by US and Canada following recent attacks
April 4, 2016,

Big paydays force hospitals to prepare for ransomware attacks
Tech, April 23, 2016

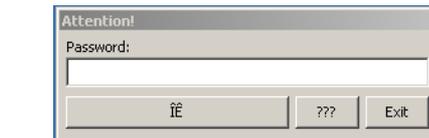
The first known ransomwares and its evolution

- AIDS Diskette ransomware discovered in 1989.
- Contained a warning message in the letter regarding licensing fee and penalty.
- Users were supposed to send a license fee to a PO box in Panama for "corporation."



The first known ransomwares and its evolution

- Gpccoder was ransomware discovered in 2005
 - 2005 encoded 15 different file types
 - 2012 encoded 41 different file types
 - 2015 encoded 228 different file types
- Encryption 1024-bit to 4096-



Creates the file ATTENTION!!!.txt in every folder in which it encoded a file. The textfile contains the following:

Some files are coded. To buy decoder mail:
[user]@yahoo.com
with subject: PGPccoder 00000000032

Hello, your files are encrypted with RSA-4096 algorithm
http://[REMOVED].

You will need at least few years to decrypt these files without our software.

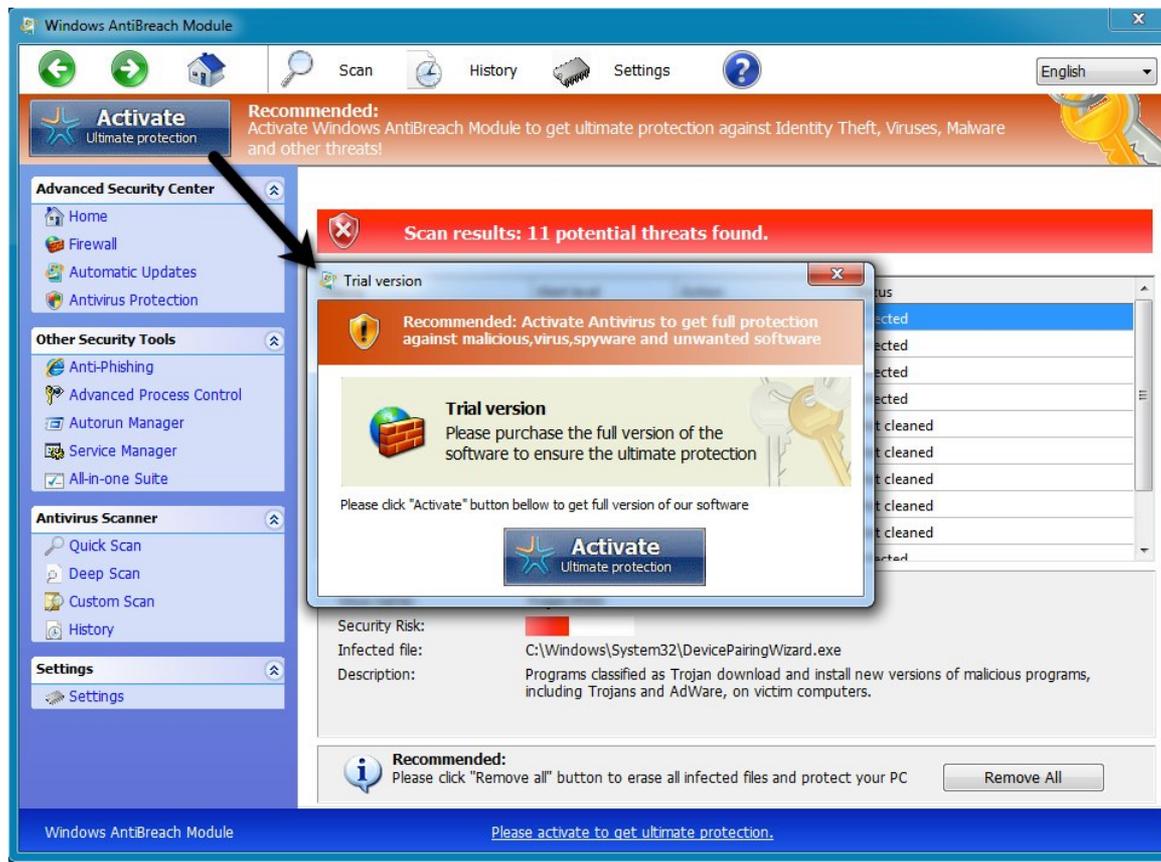
All your private information for last 3 months were collected and sent to us.
To decrypt your files you need to buy our software. The price is \$300.

To buy our software please contact us at: [MAIL ADDRESS] and provide us your personal code [PERSONAL CODE].

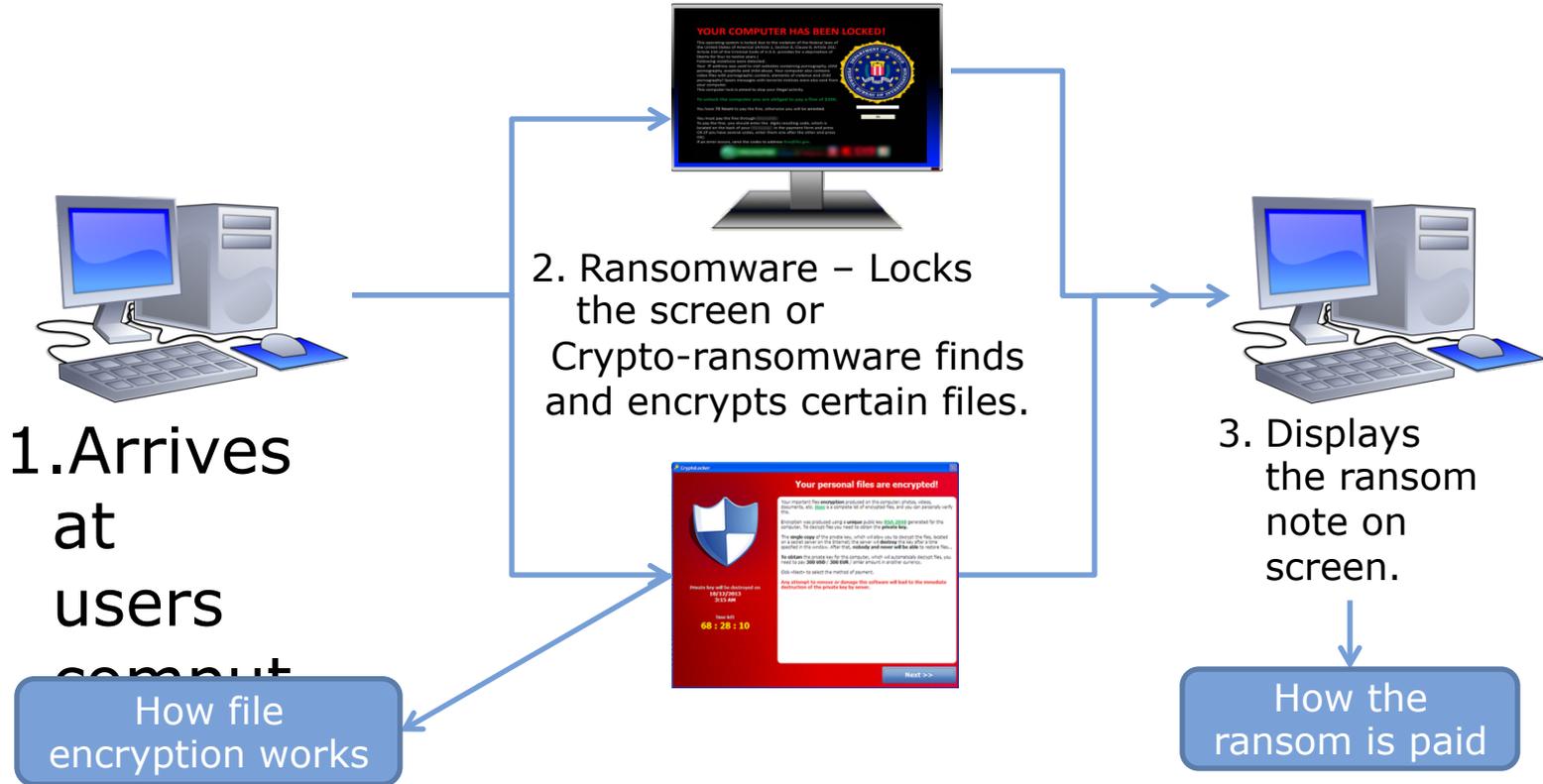
After successful purchase we will send your decrypting tool, and your private information will be deleted from our system.
If you will not contact us until 07/15/2007 your private information will be shared and you will lost all your data.

Glamorous team

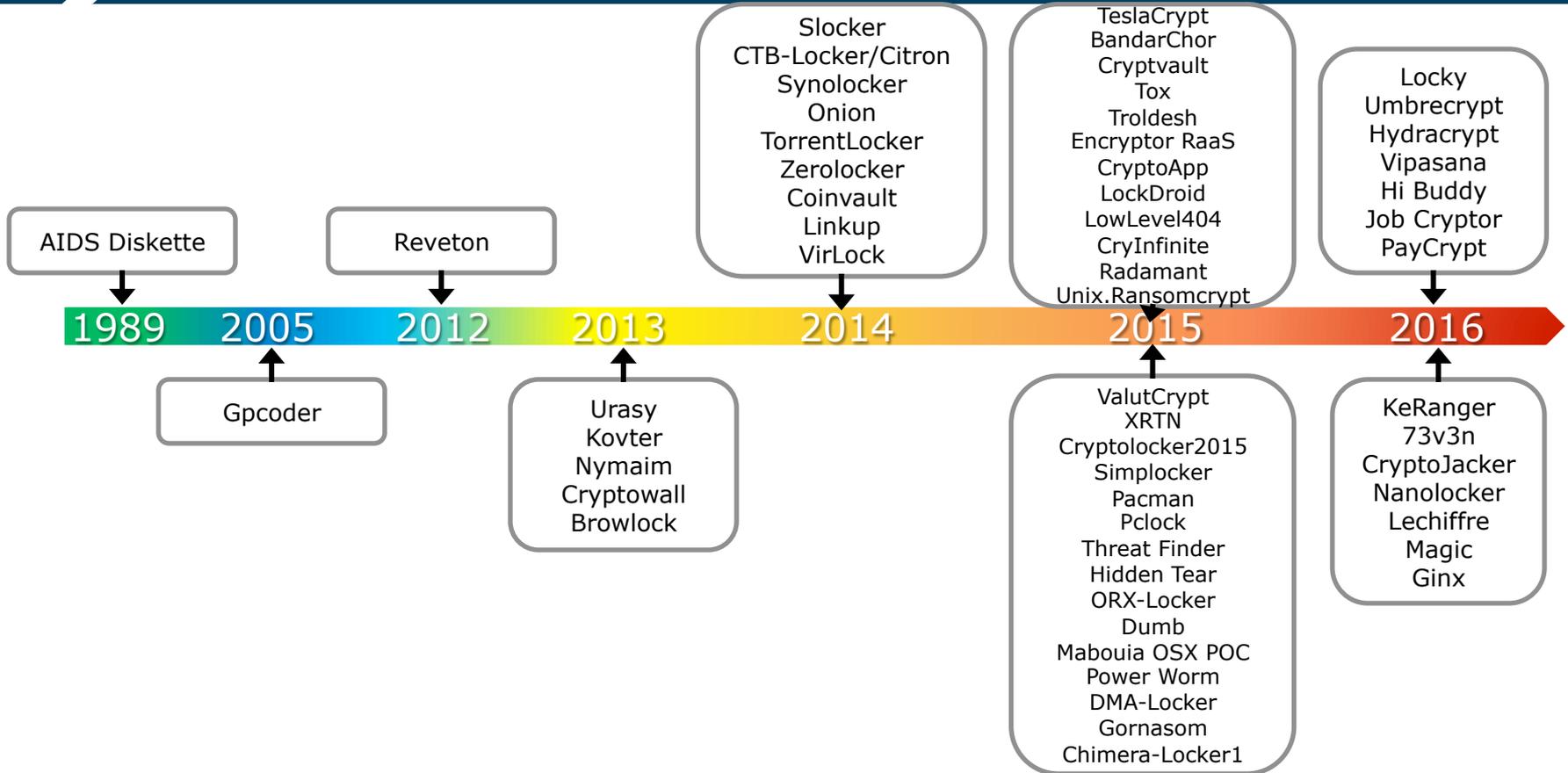
Fake Anti-Virus and Scareware



The way ransomware/crypto-ransomware works



Malware Family Variants Timeline



Lock screen ransomware

THE FBI FEDERAL BUREAU OF INVESTIGATION



ATTENTION !

IP:
Location: **United States**
IPS:

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article 1, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Perno/Zoofilia and etc), Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to \$100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated – first time) may be considered as conditional in case you pay the fine to the State.

Fines may only be paid within 72 hours after the infringement. As soon as 72 hours elapse, the possibility to pay the fine expires, and a criminal case is initiated against you automatically within the next 72 hours!

To unlock the computer, you must pay the fine through MoneyPak of 100\$.

How do I unlock computer using the MoneyPak ?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to \$4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

When you pay the fine, your PC will get unlocked in 1 to 48 hours after the money is put into the State's account.

In case an error occurs, you'll have to send the code by email fine@fbi.gov (Do not forget to specify IP address)

Video Recording
ON



MoneyPak

Code: Sum:

1 2 3 4 5 6 7 8 9 0

Pay MoneyPak

Where I can buy MoneyPak?



FRAUD ALERT: Use your MoneyPak number only with businesses listed at MoneyPak and United States Department of Justice. If anyone else asks for your MoneyPak number? it's probably a scam. If a criminal gets your money, Green Dot is not responsible to pay you back.

Lock screen ransomware

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 [REDACTED]

To pay the fine, you should enter the digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

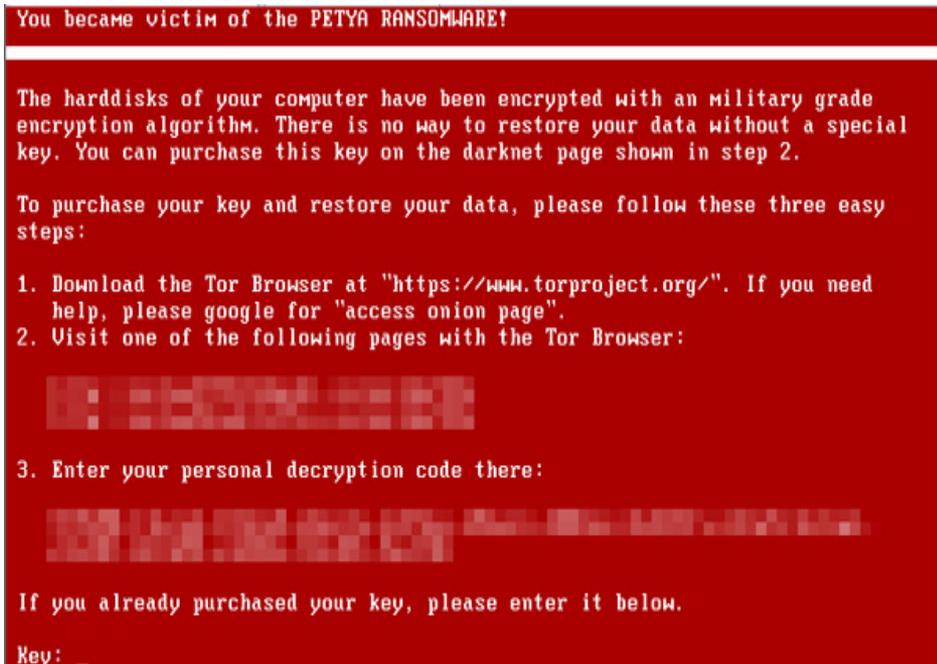
If an error occurs, send the codes to address fine@fbi.gov.



The marked shift from scareware to crypto-ransomware

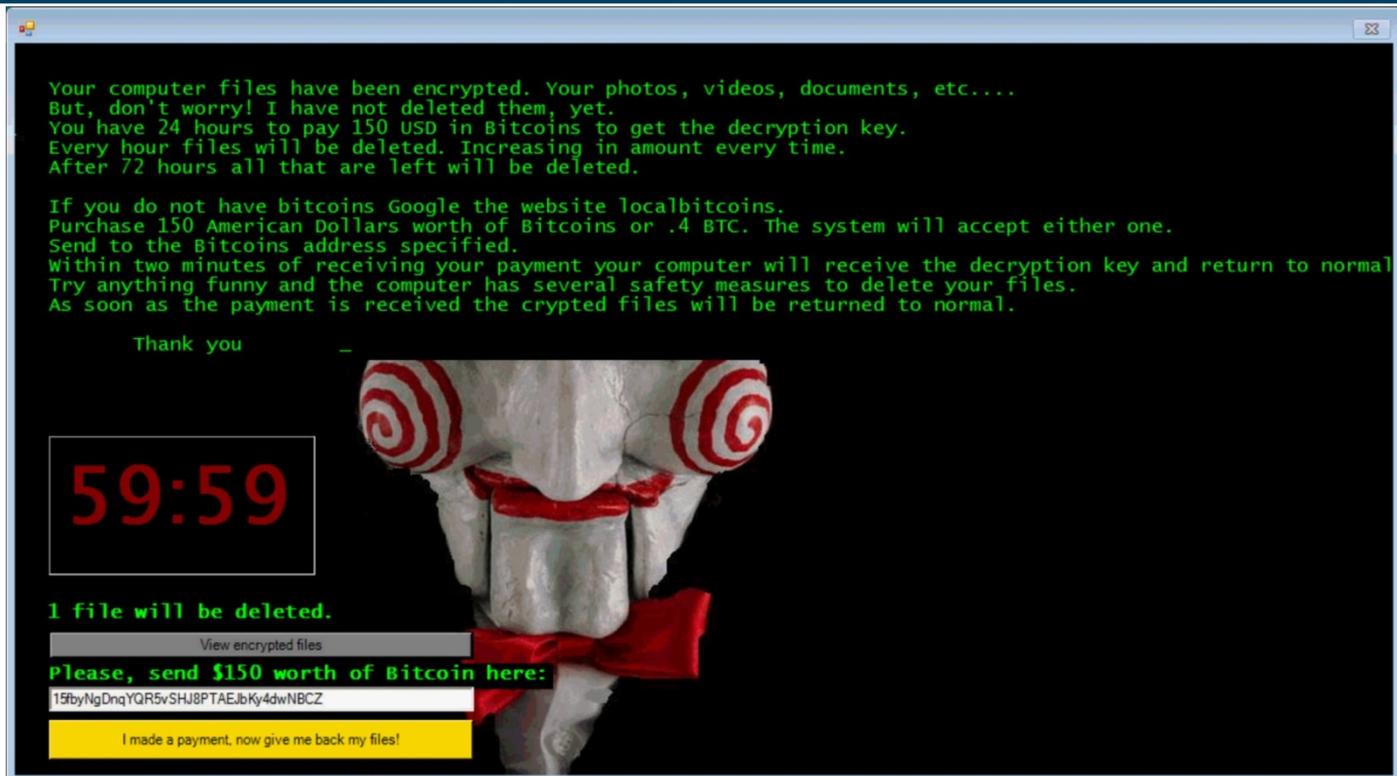


CryptoLocker Ransomware
(2013)



Petya Ransomware
(2016)

File encryption and deletion ransomware



Jigsaw Ransomware
(2016)

Miscellaneous Evolution ~2015

- Ransomware-as-a-Service (RaaS)
 - Tox and Encryptor RaaS
- Targeting – Targeted vs Spammed
- JavaScript Ransomware
- Delayed Execution
- Decrypters

The screenshot shows the Tox RaaS control panel. At the top, there's a navigation bar with 'Tox' and 'Viruses' tabs, and a 'Logout' link. A green notification bar at the top states 'The virus kSp8jrOmDX has been created: Download'. Below this is a 'Create a virus' form with fields for 'Ransom - \$' (set to 'Ransom in dollars (min. 10)'), 'Notes' (set to 'Optional, ex: For Mr. Smith'), and 'Captcha' (with a 'PinKme' captcha image). A green 'Create' button is at the bottom of the form. Below the form is a table with columns: Ransom, Infections, Payments, Profit, Notes, and Actions. The table has two rows of data, both with '0' in the Ransom, Infections, and Payments columns, and '0.00 \$' in the Profit column. The Notes column is empty, and the Actions column contains a 'Download' button for each row.

Ransom	Infections	Payments	Profit	Notes	Actions
0	0	0	0.00 \$		Download
0	0	0	0.00 \$		Download

Current State: 2016 – Present & Impact

- Spike in Media Attention
- Hospitals/targeting
- New Variant ~1-2 weeks
- Targeting enterprises using vulnerably third party applications like JBoss
- New Threat actors with better/newer skills and specializations



18 February 2016

Alert Number

MC-000068-MW

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

FBI Liaison Alert System

This product is released at **TLP: GREEN**. The information in this product is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

The FBI is providing the following information with **high confidence**:

Summary

The threat of ransomware continues to grow due to the relative availability of necessary tools, as well as the potential for extorting large sums of money. Modern ransomware uses strong encryption to render victims' files unreadable until the attackers are paid, often in Bitcoin, and release the

Current State: 2016 – Present & Impact

- Locky
 - Utilized malicious Word macros
 - Dridex distribution
- Petya
 - Overwrites master boot record (MBR)
- KeRanger
 - Second known OS X ransomware variant
- SamSam/Samas/Maktub
 - Attackers used server side vulnerabilities (Jboss) to deliver the ransomware
 - Targeted attacks
 - Not a worm, but shares characteristics...
- JIGSAW
 - File Deletion

Mitigation/Preventions

- Enable the 'Show file extensions' option in the Windows settings on your computer.
- Ensure patches are applied for all vulnerabilities
- Ensure anti-virus/endpoint protection up-to-date
- Ensure end-users are educated to follow security best practices
 - Avoid suspicious email curiosity
 - Do not enable Macros on Office documents
- Ensure regular backups are made to protect data
- Exercise privilege restriction, limit admin access, network segmentation, DMZ hardening, etc.
- Limited open shares
- No more ransomware: <https://www.nomoreransom.org/>

Where could ransomware go from here?

- “Cryptoworms”
- Cloud-specific
- (Even more) Targeted attacks
- (Better) Mobile variants
- Internet of Things (IoT)
- Greater evasion and detection avoidance capabilities

Sources and additional reading

- <https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf>
- https://www.symantec.com/security_response/writeup.jsp?docid=2005-052215-5723-99&tabid=2
- <http://blog.talosintel.com/2016/04/ransomware.html#toc>
- <http://www.trendmicro.com/vinfo/us/security/definition/ransomware>
- <https://www.fbi.gov/news/stories/2012/august/new-internet-scam/new-internet-scam>
- <https://www.fbi.gov/about-us/investigate/cyber/ransomware-brochure>
- <http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/>
- <https://www.comparitech.com/blog/information-security/the-history-of-ransomware/>
- <http://blog.talosintel.com/2016/03/samsam-ransomware.html>
- <http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0WU1GB>

Open discussion and questions

