

# The rise of Ransomware

  
**Martins Saulitis**

IBM X-Force Incident Response Services  
Saulitis@lv.ibm.com

06/10/2016

# Agenda

- Definitions
- Examples
- Can we get files back?
- How does the infection happen?
- How to be proactive?
- Conclusions and recommendations





# Definitions



# Definitions

- **Ransomware** is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key. (Trend Micro)
- **Ransomware** is a type of malware that severely restricts access to a computer, device or file until a ransom is paid by the user. (Kaspersky)

## ransomware

*/ˈrɑns(ə)mweɪ/*

*noun*

noun: ransomware; noun: ransom-ware

a type of malicious software designed to block access to a computer system until a sum of money is paid.

"although ransomware is usually aimed at individuals, it's only a matter of time before business is targeted as well"

# Is it profitable?

PAY UP Or eLSe!

i HAVe enCrYpTeD All  
YOur Files ANd if yOu  
wAnt to sEe thE MAgaziN  
YoU'LL nEed TO PAy Up!

YOu HAVe bEEN wARNeD!

YOuRS sInceRELY, bAD  
GuYs 'N GiRls INc.  
(WorldwidE)

- Initially popular in Russia, grown internationally
- June 2013 McAfee data shows 250,000 samples in Q1 of 2013 (>2x amount of Q1 2012)
- According to FBI, victims in United States have paid more than \$209 million in ransom payments in the first three months of 2016, compared with \$25 million in all of 2015.
- According to Cyber Threat Alliance CryptoWall 3 generated profit of \$325 million by 2015.
- “It estimated it would cost \$5,900 to buy a ransomware kit that could return up to \$90,000 in one month of operation”, BBC reports.



# Examples

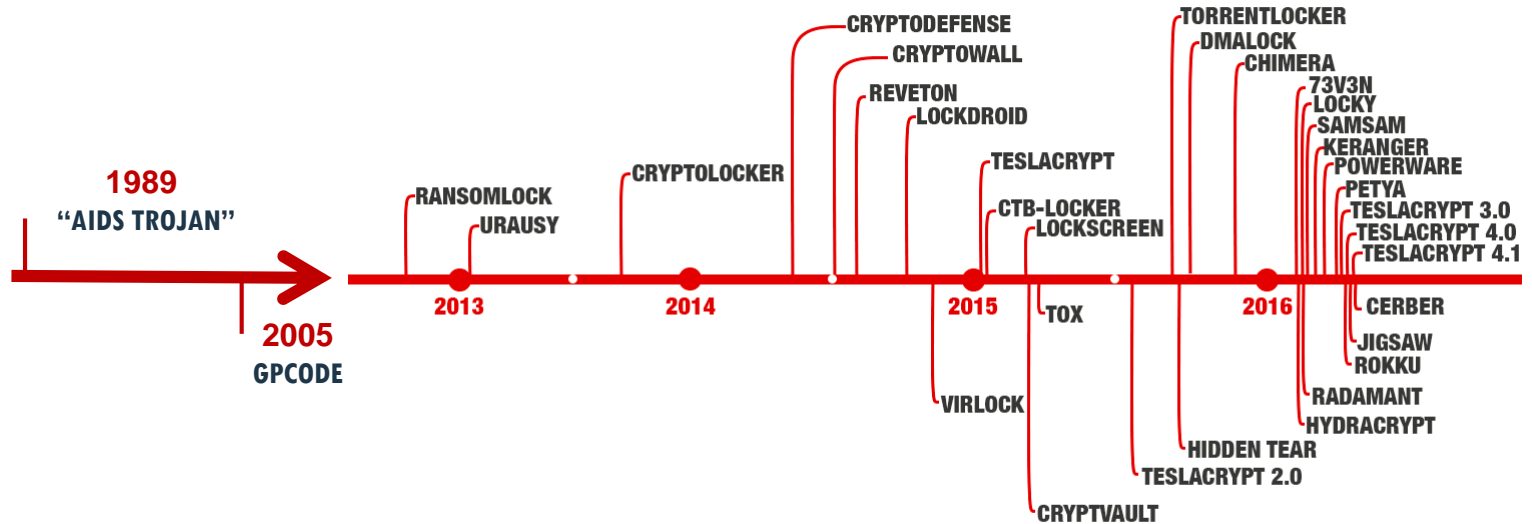


# History

- December 1989, Aids Information Diskette incident.
- 20,000 discs containing Trojan mailed to Europe, Africa, Australia and WHO.
- Addresses stolen from PC Business World database.
- Trojan promised to give a lifestyle evaluation to estimate risk of AIDS.
- After infection and 90 reboots encodes names of all files leaving invoice behind.
- \$189 requested to be sent to PO Box 7 in Panama addressed to Jeseeph Popp.

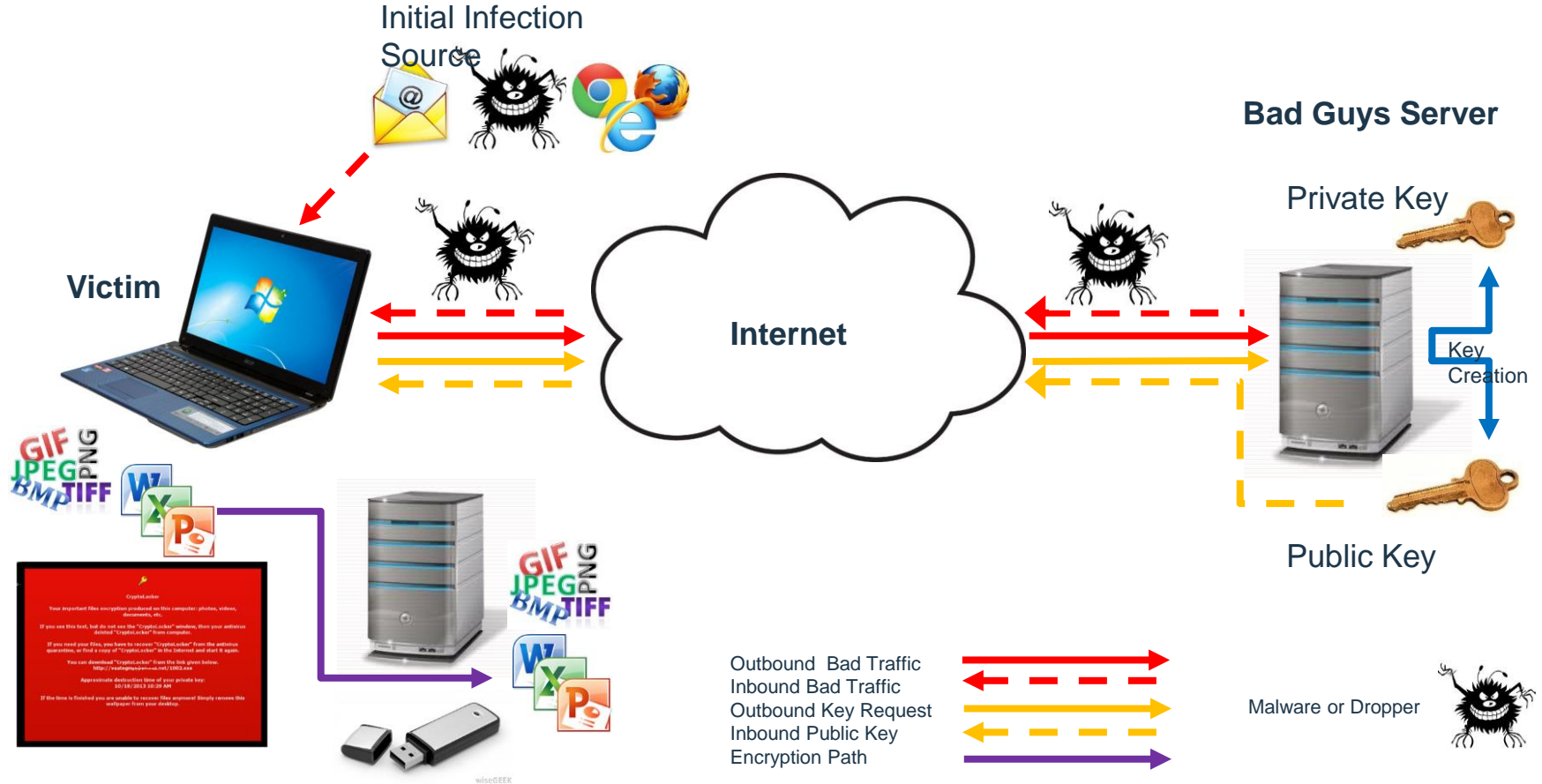


# Modern times





# Modus operandi



# Ransomware in bank

In this example an international bank contacted IBM and asked for assistance in containing ransomware outbreak that had encrypted over 500,000 office documents. IBM investigation proved that source of this infection was unknown at the time variant of CryptoWall that bypassed all existing security measures.

## **Solution:**

Forensic analysis done by IBM identified patient zero and precise manner in which malware bypassed security controls put in place. Customer defenses were analyzed, list of recommendations and weaknesses to be fixed were provided to improve security posture. Non-signature based solutions was offered as part of recommendations.

## **Benefit:**

A roadmap of recommendations for improving security in the customer environment were given to the client with assistance to improve their security posture.





**Can we get files back?**



# Malware researchers are your friends

- <https://noransom.kaspersky.com/>
- <https://download.bleepingcomputer.com/demonslay335/AlphaDecrypter-fp.zip>
  - To extract the decryptor, you need to use the password: **false-positive**.
- [http://www.talosintel.com/teslacrypt\\_tool/](http://www.talosintel.com/teslacrypt_tool/)
- <http://www.tripwire.com/state-of-security/security-data-protection/ransomware-happy-ending-10-known-decryption-cases/>
- <https://www.grahamcluley.com/2016/04/decryption-tool-released-locky-ransomware-impersonator/>
- <https://www.grahamcluley.com/2016/04/petya-ransomware-unlock-tool/>



# How does the infection happen?



# What you would expect

- **Email**

- Attachment (DOC, PDF, ZIP, CAB, etc.)
- Link to a booby-trapped website
- Phishing Emails

- **Drive-by-Download**

- Malvertising
- Compromised web-sites
- Links in social networking posts (FaceBook, Twitter, etc.)

- **Previously Compromised/Infected System**

- Already under the remote control of the bad guys n girls...
- Usually with a bot client (malware)

 Reply  Reply All  Forward

Mon 6/10/2014 4:50 PM



TAX@irs.gov <tax@irs.gov>

Your FED TAX payment (ID:KLBIRS019283639) was Rejected

To

\*\*\* PLEASE DO NOT RESPOND TO THIS EMAIL \*\*\*

Your federal Tax payment (ID: KLBIRS019283639), recently sent from your checking account was returned by the your financial institution.

For more information, please download notification below. (Security PDF Adobe file)

[https://www.cubby.com/pl/Document\\_087341-436175.zip/\\_2c87375e73c440cabe5415ff6ea48019](https://www.cubby.com/pl/Document_087341-436175.zip/_2c87375e73c440cabe5415ff6ea48019)

Transaction Number: KLBIRS019283639

Payment Amount: \$ 5920.23

Transaction status: Rejected

ACH Trace Number: 9209382167

Transaction Type: ACH Debit Payment-DDA

Internal Revenue Service

Metro Plex 1, 8401 Corporate Drive, Suite 300, Landover, MD 20785.

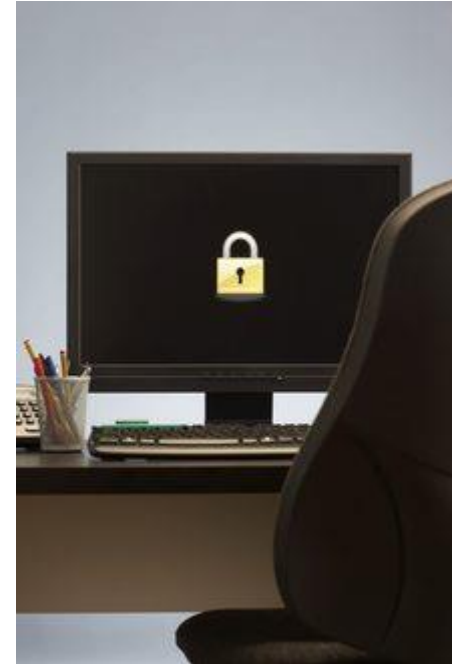


# How to be proactive?



# Work with users

- **User education**
  - Regular test “phishing” campaigns
  - Keep it Simple
  - Back it up with acceptable use and security policies that they can understand and can be held accountable against.
- **Restrict rights**
  - On workstations and especially server/corporate shares
- **Tighten Windows Policies**
  - Use software restriction policies
  - Disable Windows Scripting Host
- **Patch the OS and ALL applications quickly**
  - Especially Adobe Acrobat, Flash and Java
  - Don't forget servers!





## Limit ingress/egress options

- **Improved email and web scanning/URL filtering**
  - Use multiple AV engines and reputational scoring
  - Anti-spam that does SPF and/or DKIM checks
  - Block access to TOR proxies/gateways
  - Investigate all connection attempts to TOR or to TOR proxies/gateways as this should be indicative of an infected system





# Ransomware Response Guide

IBM INCIDENT RESPONSE SERVICES

RELEASE DATE: MAY 2016



- **Use our guide**
  - <https://ibm.biz/BdrUUv>
- **Covers**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication
  - Recovery
  - Post-Incident Activity
- **Available for free**
  - If email address is provided



# Conclusions and recommendations




# Prepare and

- There is NO 100% solution, no Silver Bullet!
- However there are things you can do to help minimise a repeat:
  - Harden systems, reduce rights, disable macros (unless signed or on a whitelist)
  - Disable Windows Scripting Host (stops .JS and .WSH scripts used by bad guys n girls)
  - Train staff (and regularly test them)
  - Use software restriction policies, or AppLocker
  - Use a specific tool
  - Improve URL and email filtering (anti-spam, reputational checks, blacklists, etc.) as well as checking to see if the Message-ID has a valid FULL domain name
  - Use multiple AV engines to scan all e-mail and web content
  - Set up a dedicated reporting email address and monitor it
  - Make your security policy and internet usage policy clearer and enforce it...
  - Ensure that you take regular backups, preferably off-site to optical media/tape, etc.



# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube.com/user/ibmsecuritysolutions](https://youtube.com/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.