

Ransomware - All Your Data Are Belong To Us

30 Years into the History of Ransomware



Ransomware - All Your Data Are Belong To Us

What Is Ransomware?



- “Agency” Ransomware
 - Typically received from “shady” sites
 - Will lock a machine, but will not encrypt or damage files
 - Easier to recover from via Safe Mode or a live CD
- Crypto Ransomware
 - Specifically searches for valuable files
 - Uses strong levels of encryption to hold files hostage, until payment is made
 - Often times non-recoverable if there is no backup available
- Why Ransomware?
 - Easier to conduct transactions
 - People have a need for their important files so they are likely to pay
 - Doesn’t involve credit card fraud, which requires cloners, mules, etc.
 - Low maintenance, once the initial package is developed

Ransomware - All Your Data Are Belong To Us



Pakistani Brain

- Used to prevent piracy in software written by two brothers, Basit and Amjad Farooq Alvi
- Had a special "ransom" message, instructing users to call them if they see the warning
- Brain Net is now the largest Internet service provider in Pakistan

1986

1989

2006

2008

2010

2011

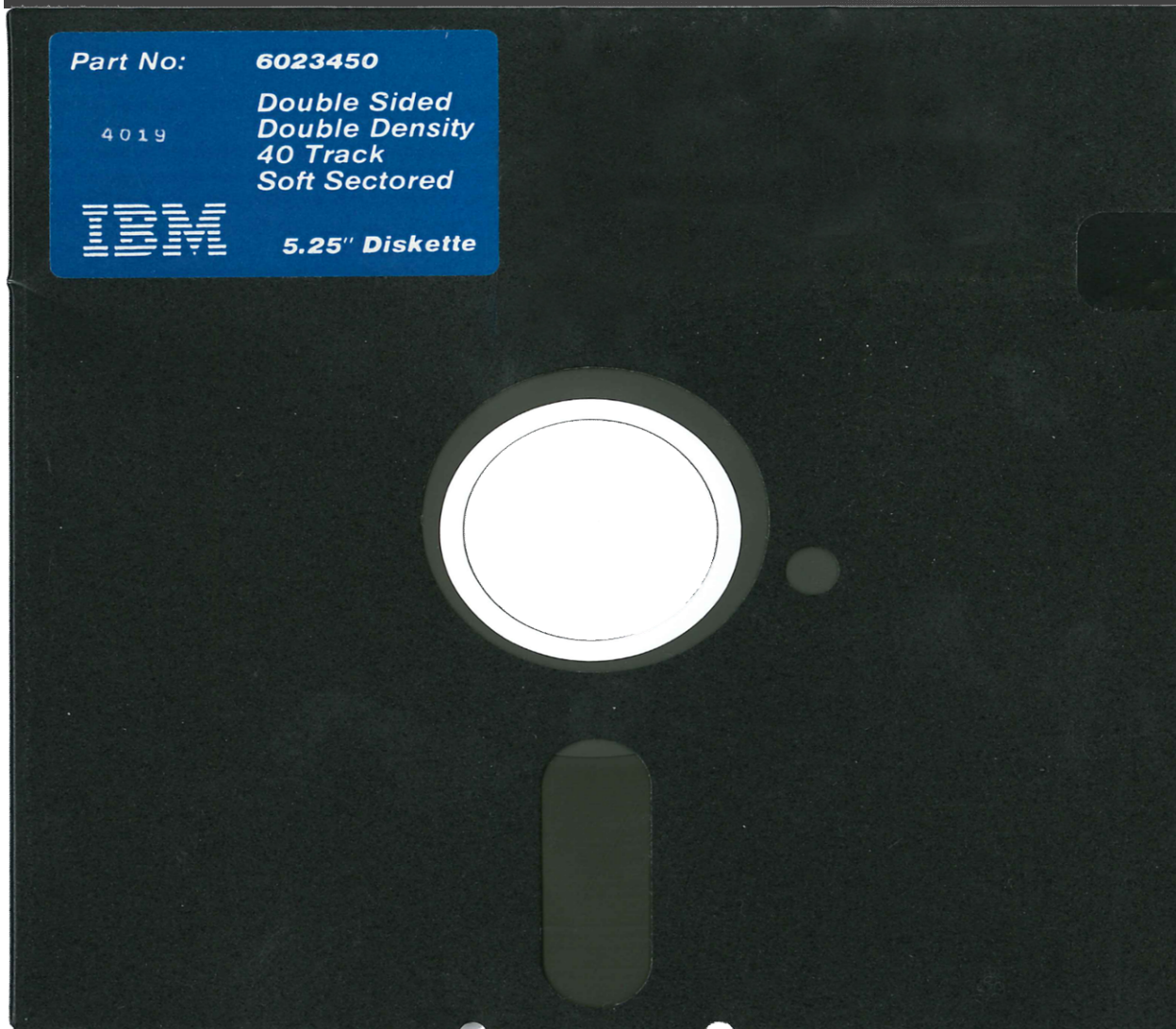
2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



PC Cyborg/AIDS

- More commonly known as the "first" ransomware
- Was delivered manually, via a diskette titled "AIDS Information Introductory Diskette"
- When the boot count reached 90, AIDS hid directories and encrypted the names of all files on the C: drive. It then asked the victim to 'renew the license' and contact PC Cyborg Corporation for payment
- Payment of \$189 sent to a post office box in Panama.

1986

1989

2006

2008

2010

2011

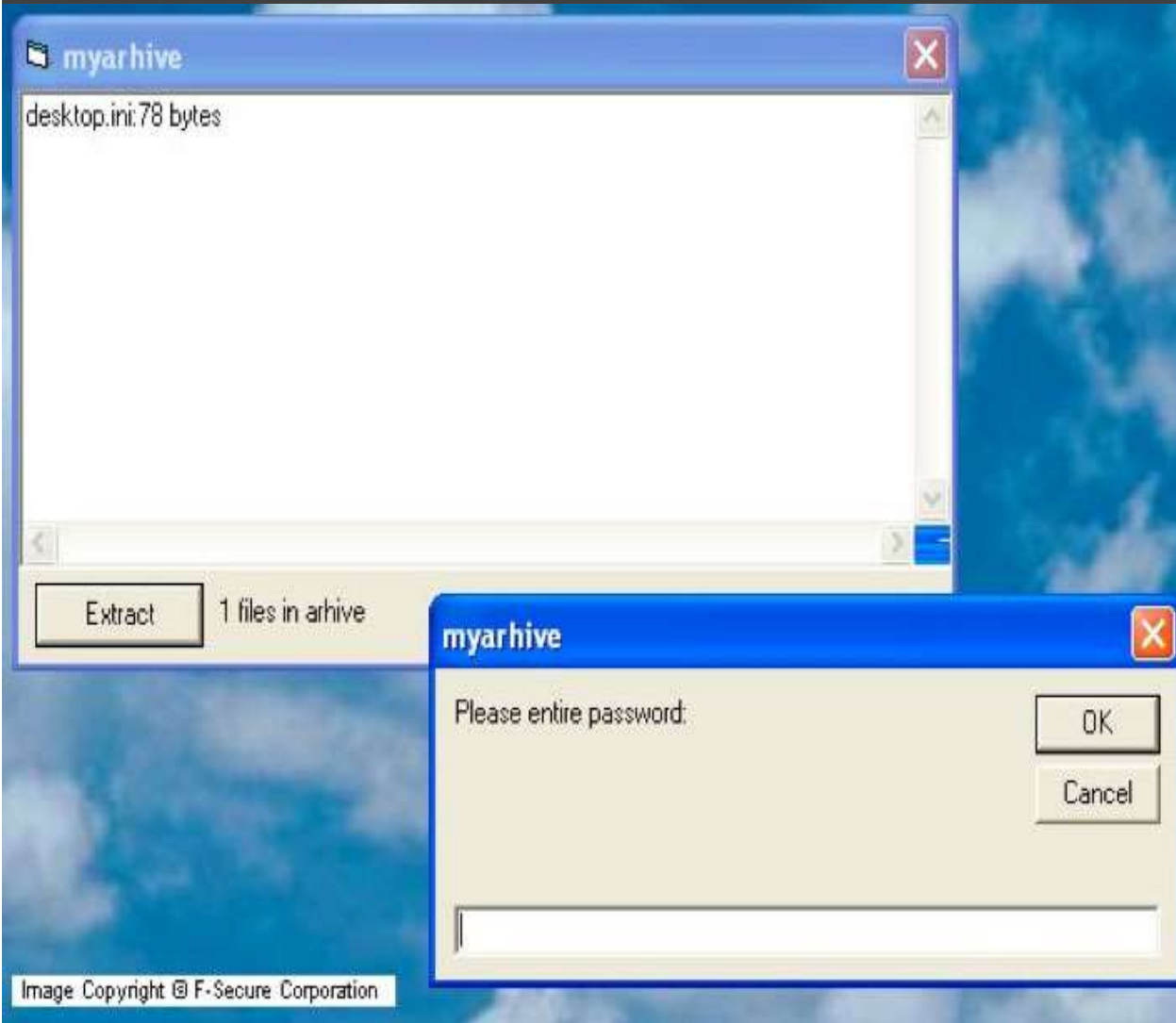
2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



Archiveus and GPCode

- Archiveus (MayAlert)
 - The password was only available after the victim purchased from one of three online drug stores
 - Ransomware that encrypted files on the disk, by “archiving” them.
 - Someone cracked the password -
mf2lro8sw03ufvnsq034jf
owr18f3cszc20vmw
- GPCode
 - Also called PGPCode, it utilized Symmetric Encryption, making it fairly easy to hack

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us

GPCode.AK

- Changed encryption routine to RSA-1024 and AES-256
- Encrypted more files
- Renames them with a ._CRYPT extension and deletes the original files

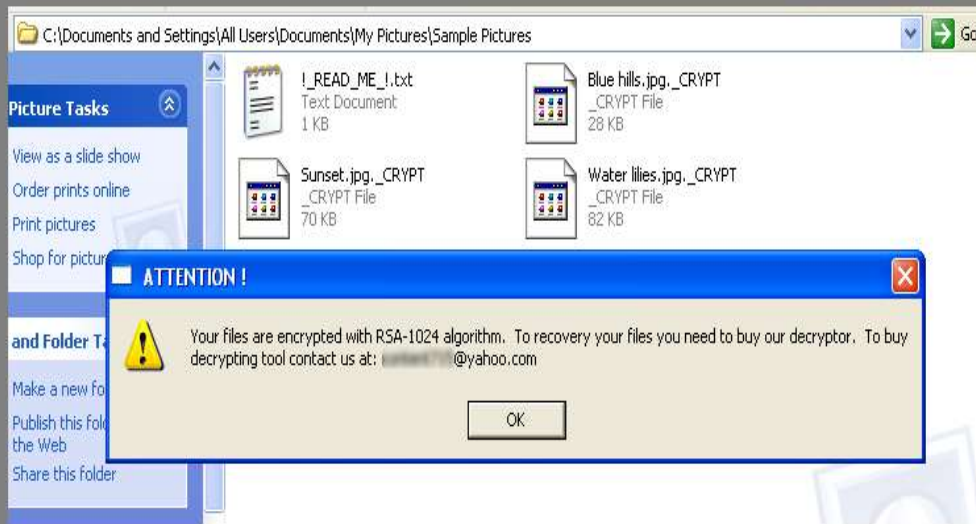


Image by tau.ac.il

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



WinLockers

Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.

Technical details:

Involved IP address: [REDACTED]

Involved host name: [REDACTED]







Source or intermediary sites: <http://pornerbros.com>

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.

HOW TO UNLOCK YOUR COMPUTER:

-  Take your cash to one of this retail locations:
   
-  Get a MoneyPak and purchase it with cash at the register
-  Come back and enter your MoneyPak code to unlock your computer (5 attempts available)
Code:

1	2	3
4	5	6
7	8	9
Delete	0	Enter

- Non Encrypting WinLockers
- Effectively locks Windows, preventing the computer user from accessing their desktop, files, or applications

Permanent lock on 05/01/2013 5:20 p.m. EST

Image by securitystronghold.com

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



Cashing In

- The money starts flowing, hackers realize people are “willing” to pay
- Adds more fuel to the fire, allowing next-gen malware to be created

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us

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 I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, 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 Porno/Zoophilia 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 unblock 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)

Reveton and Urausy

- Reveton
 - Fraudulently claims to be from a legitimate law enforcement authority and that the victim has been downloading pornographic images
 - MoneyPak was commonly used for payment
 - Delivered via Citadel platform
- Urausy
 - Another ransomware that mimics Reveton actions

Image by krebsonsecurity.com

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



CryptoLocker

- CryptoLocker
 - Believed to have been first posted on the Internet in early September 2013
 - CryptoLocker was targeted in late-May 2014 via Operation Tovar, which allowed Fox-IT, a security firm, to obtain the database of private keys, to decrypt encrypted files for free

Image by forbes.com

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



Not Just Windows

Mac Ransomware

- JavaScript type ransomware that would persist even after closing the browser, due to the "restore from crash" feature
- Clicking on "Reset Safari" would allow you to recover from the ransomware and avoid paying \$300 USD

Android Ransomware

- Svpeng, discovered by Kaspersky Labs, infected Android devices
- 25 year old Russian actor was arrested, along with 4 others, however, reports state that Svpeng infected 350,000 Google devices and stole as much as \$930,000

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



Crypto*

- CryptoWall
 - Typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware
 - Deletes Volume Shadow Copies and disabled System Restore
- CryptorBit
 - Also called HowDecrypt, was released in the beginning of December 2013, and into 2014
 - Payment was to be made with BitCoins, located on a TOR server
 - Because it didn't delete shadow copies, you could typically recover encrypted files
 - DecrypterFixer, by Nathan Scott, was written to attempt to decrypt the locked files

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us

Cryptolocker 2.0

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files

<< Back

Proceed to payment >>

CryptoLocker 2.0

- Seen in late 2013, early 2014)
- Encryption level changed
- Only accepts BitCoins
- Cryptolocker 2.0 was written in C#, instead of C++ like CryptoLocker
- Deloitte's Cyber Risk Services assisted in disrupting the CryptoLocker ransomware

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us

More Crypto*

- CryptoDefense
 - CryptoLocker imitator
 - Made over \$34,000 in one month, per Symantec
 - Distributed via spammed emails
 - Uses Tor and Bitcoins for anonymity; public-key cryptography using strong RSA 2048 encryption
- Cryptoblocker
 - Uses AES instead of RSA encryption
 - Will not encrypt any file over 100MB
 - Count down timer to encourage victims to pay

CryptoWall "4" (First seen November 2015)

CryptoWall 3.0 (First seen January 2015)

CryptoWall 2.0 (First seen October 2014)

CryptoWall 1.0 (First seen March 2014)

CryptoDefense (First seen February 2014)

Cryptolocker clone (First seen November 2013)

Source <https://www.cryptowalltracker.org>

1986

1989

2006

2008

2010

2011

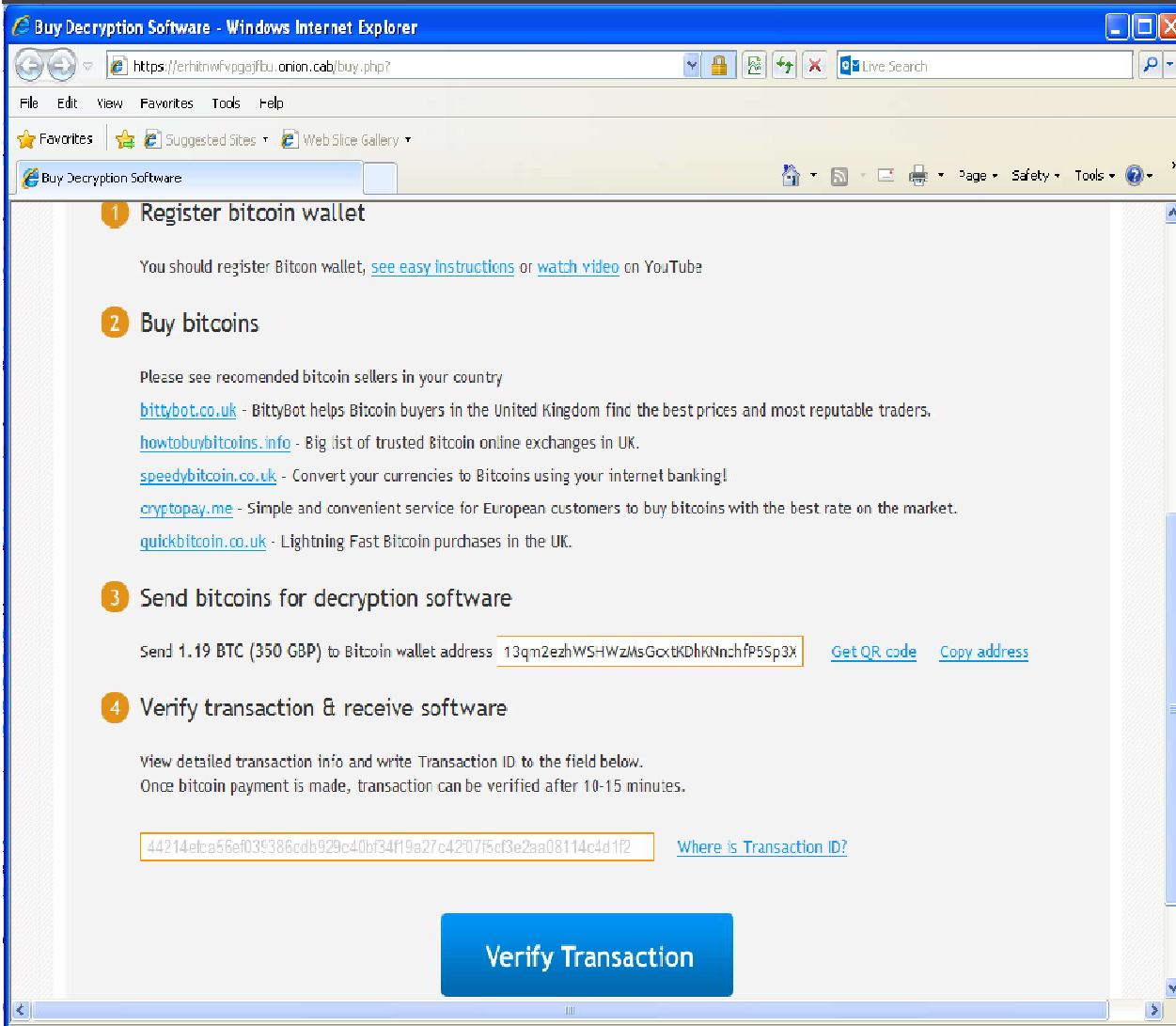
2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



TorrentLocker

- Email campaigns targeted specific countries
 - Australia, Austria, Canada, Czech Republic, Italy, Ireland, France, Germany, Netherlands, New Zealand, Spain, Turkey, and the United Kingdom
- 1.45% of victims are paying the ransom (570 of 39,670 infected systems) that made the criminals between \$292,700 and \$585,401 in Bitcoin (ESET)
- Initially, a tool was created to decrypt the files, however, the Torrent Locker authors modified the encryption scheme to use a different encryption method, which resulted in breaking the decryption tool

1986

1989

2006

2008

2010

2011

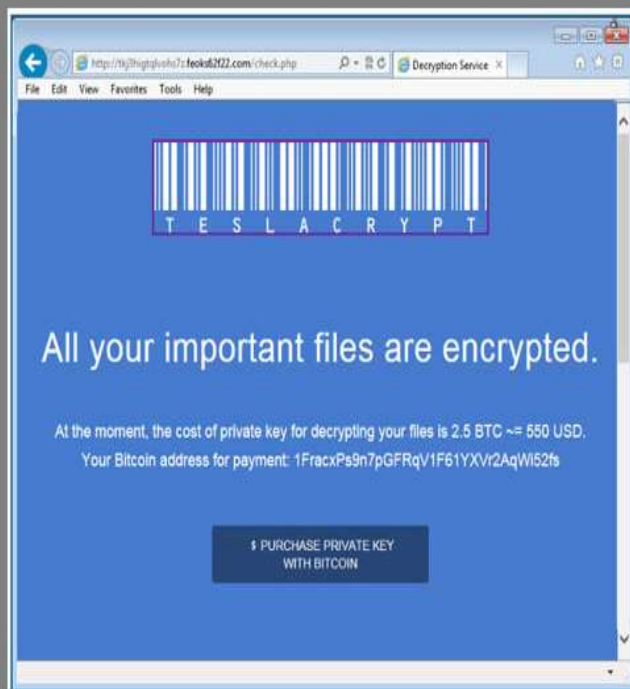
2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



TeslaCrypt and CryptoWall 4.0

- TeslaCrypt,
 - Also called AlphaCrypt uses AES256 encryption
 - Executes "vssadmin delete shadows /all" to delete Volume Shadow Copies
 - Uses BitCoins as the payment method
 - A tool, called TeslaDecrypt, was released to decrypt files encrypted by TeslaCrypt
- CryptoWall 4.0
 - PowerShell and VBScript "variant" was discovered
 - CryptoWall 4.0 utilizes new filenames, and now encrypts a file's name along with its data
 - The HTML page showing how to pay was redesigned
 - Same installation characteristics and communication methods as previous versions of CryptoWall

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

1. <http://6dtxgqam4crv6rr6.tor2web.org/728EF3F4A1802521>

2. <http://6dtxgqam4crv6rr6.onion.to/728EF3F4A1802521>

3. <http://6dtxgqam4crv6rr6.onion.cab/728EF3F4A1802521>

4. <http://6dtxgqam4crv6rr6.onion.link/728EF3F4A1802521>

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>

2. After a successful installation, run the browser and wait for initialization.

3. Type in the address bar: 6dtxgqam4crv6rr6.onion/728EF3F4A1802521

4. Follow the instructions on the site.

!!! Your personal identification ID: 728EF3F4A1802521 !!!

Locky

- The actors behind Dridex, originally a banking Trojan distributor, have switched tactics, now using ransomware
- One method of distribution is via a Word document and Macro
- Another method is via the Neutrino Exploit Kit
- Opening the macro will start the download of Locky, causing the files on the machine to be encrypted
- Targets valuable files, such as .doc, .csv, .pdf, .jpg
- Costs .5 BitCoins (BTC) to decrypt the files, roughly \$200 USD

1986

1989

2006

2008

2010

2011

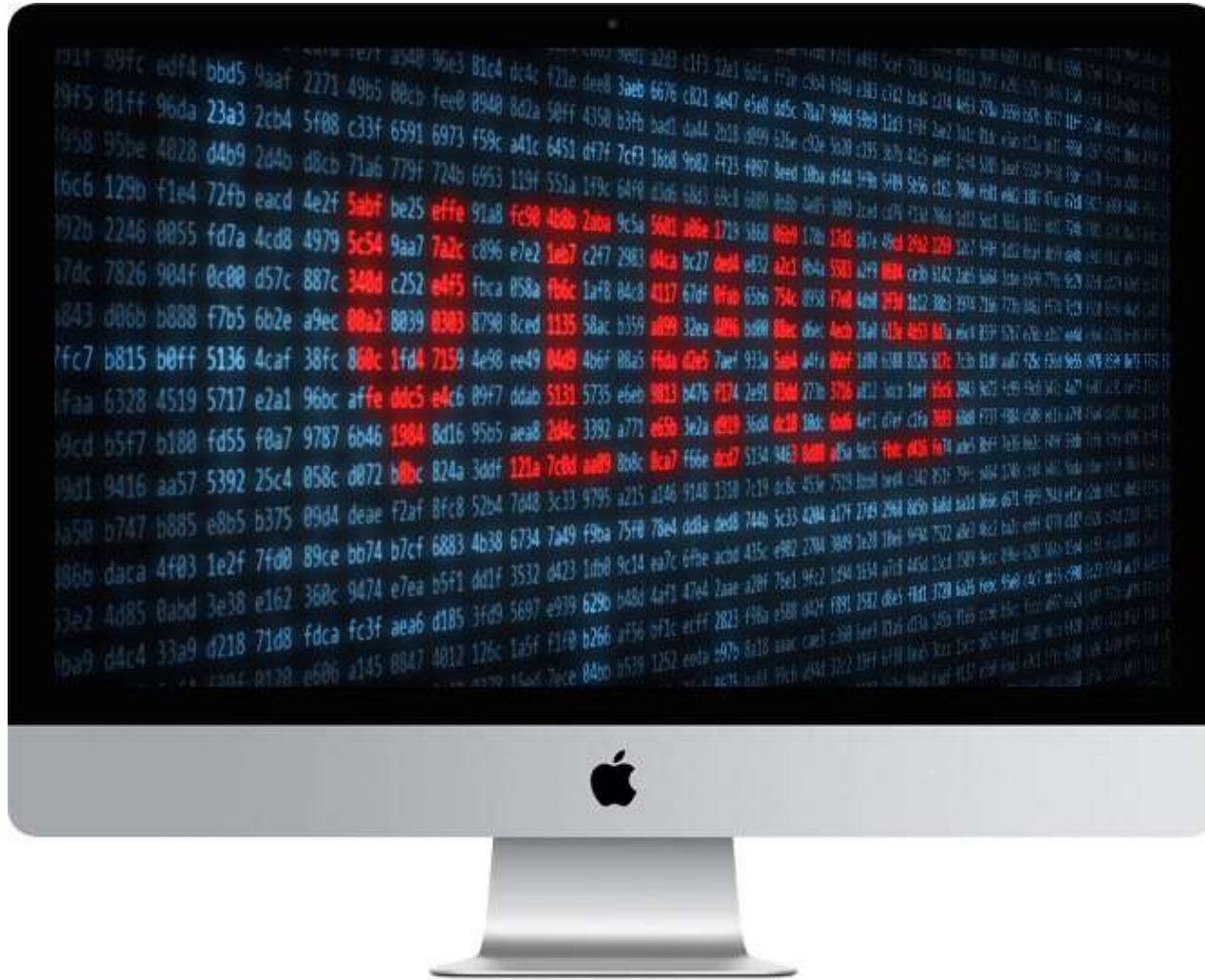
2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us



KeRanger

- First complete version of an OS X Ransomware, discovered by Palo Alto Networks on 3/4/2016
- Attackers infected two installers of Transmission version 2.90
- Version 2.92 looks for KeRanger and removes it
- Approximately 6,500 copies of the infected Transmission
- Recovery costs are about 1BTC or \$400
- KeRanger infected Transmission installers include an extra file named General.rtf

1986

1989

2006

2008

2010

2011

2012

2013

2014

2015+

Ransomware - All Your Data Are Belong To Us

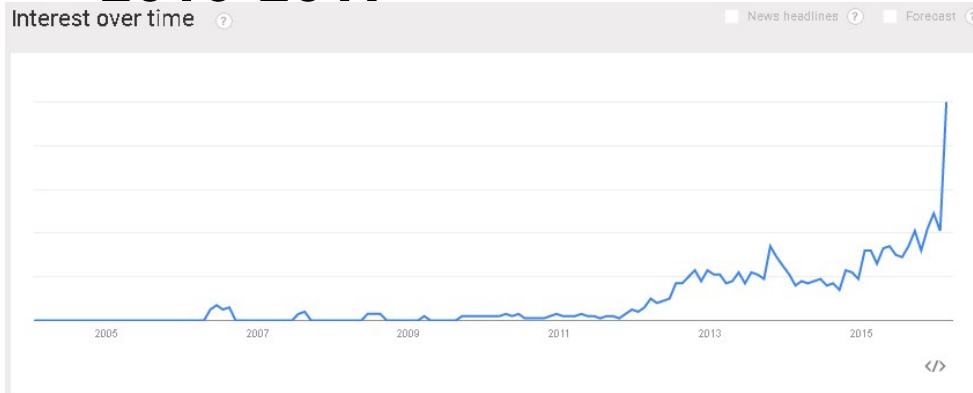
Best Practices



- Back Up and Verify Data
 - Use tools such as Carbonite, Google Drive, or DropBox
- Updates
 - Windows
 - 3rd party software
 - Antivirus signatures
- Education
 - Training
 - Best practices
 - Social engineering
 - Avoid questionable websites
- Enterprise Practices
 - SNORT/IDS
 - YARA Rules
 - Perimeter protection with UTM devices
 - Windows Group or Local Policy Editor to create Software Restriction Policies that block executables from running when they are located in specific paths
 - Monitor other IOCs
- Whitelisting applications
 - PC Matic, Pro, or MSP

Ransomware - All Your Data Are Belong To Us

Ransomware Predictions for 2016-2017



- More expensive to decrypt files
- More persistent, difficult to remove
- Continued use of Office macros
- More exploits being utilized
- More underground "services", providing one-stop shops
- Take down of one or more infrastructures, but not people/gangs
- More domain generating algorithms used to generate random domains
- More use of TOR/Onion Sites

Ransomware - All Your Data Are Belong To Us

Collaborative Efforts



- Community Response
 - Law enforcement
 - Private sectors
 - Independent researchers
- Competitors sharing intelligence
 - DGA cracking
 - URL feeds
 - IOCs, IDS rules, etc.
- CryptoLocker Working Group
 - Rebranded to be more ransomware related, broad coverage

"We're making a lot of progress, but like many other types of crimes... we're not there yet. It is still a problem. We clean up one, and another one shows up on the market."

Richard Jacobs / FBI Cyber Branch