# An Exploration of Ransomware

Reese Pearsall, Logan Pappas, Dallas LeGrande, Chris Cooper

# In the news

Erie County Medical Center in Buffalo, NY

Victim of ransomware attack in 2017

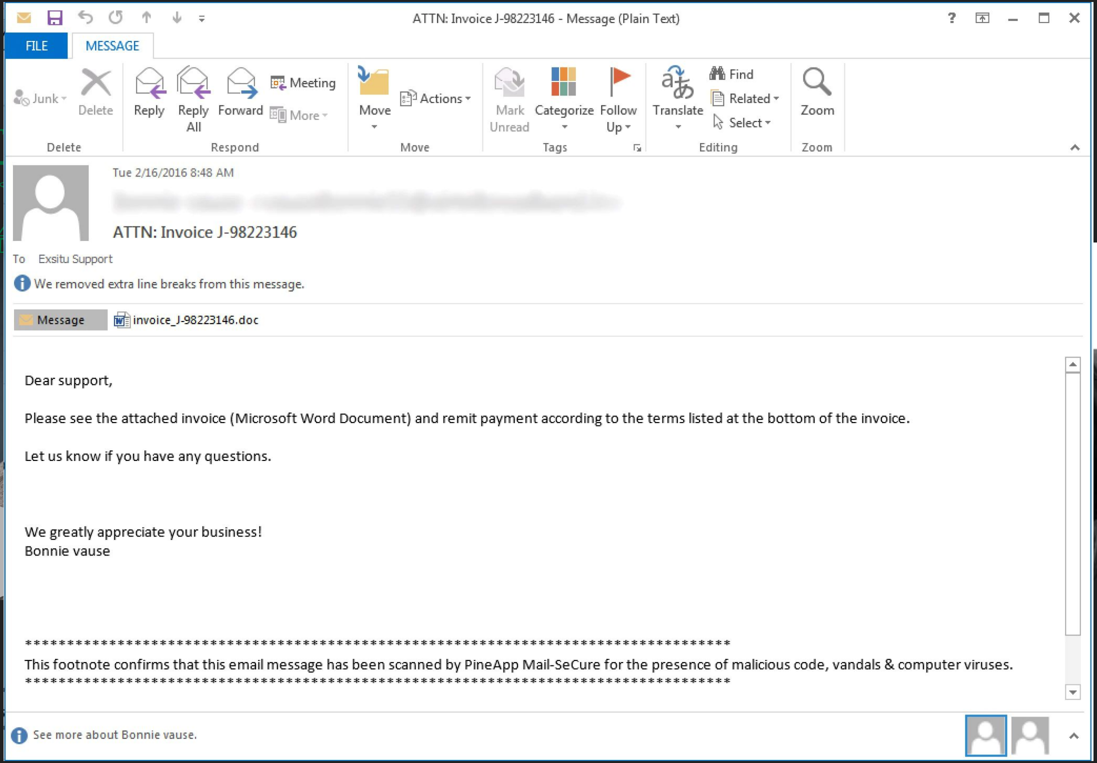
Did not pay the ransom, but ended up paying around **<u>10 million</u>** dollars recovering from the incident

# What is ransomware?

- Malicious software (malware) that infects computers and locks up the computer’s files until some ransom is paid

# How Ransomware works

# How Ransomware works



Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

Message invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

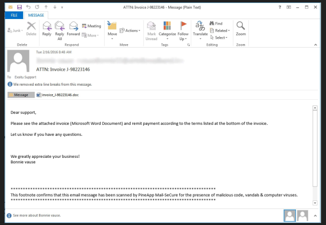
Let us know if you have any questions.

We greatly appreciate your business!
Bonnie vause

```
******************************************************************************
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.
******************************************************************************
```

See more about Bonnie vause.

# How Ransomware works



ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

Message invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!
Bonnie vause

*****************************************************************************

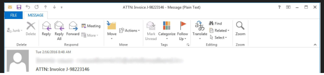
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.

*****************************************************************************

See more about Bonnie vause.

Malicious email

# How Ransomware works

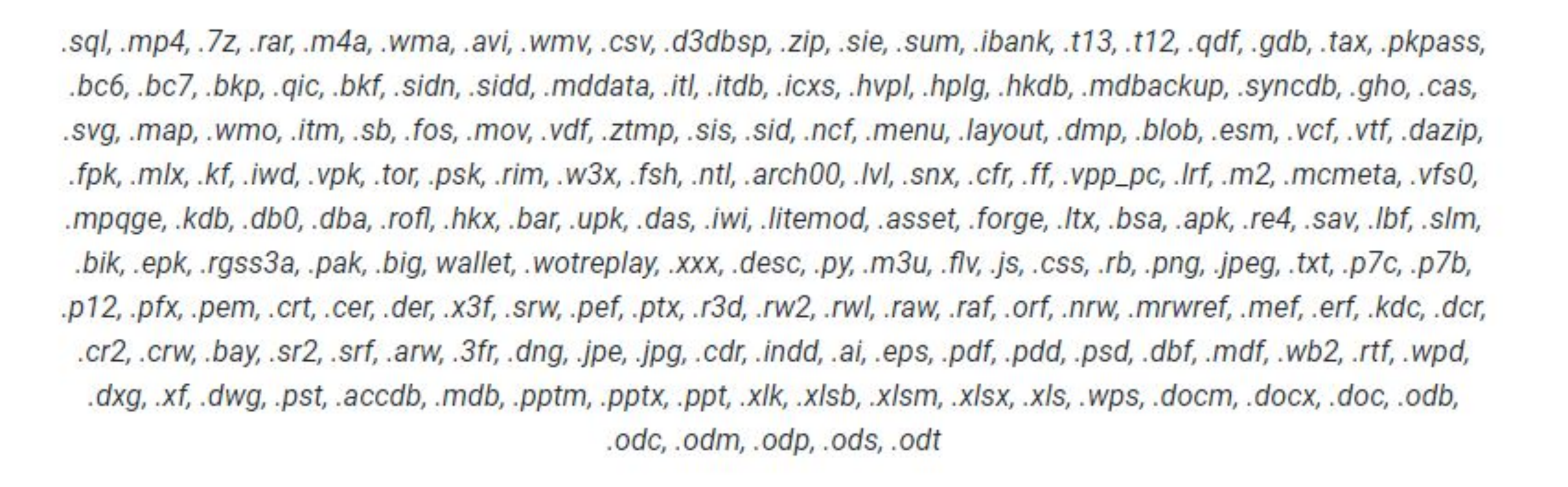


ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

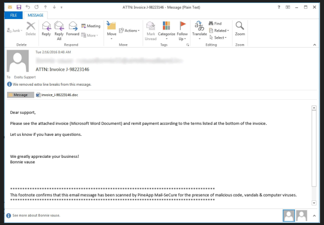
ATTN: Invoice J-98223146



.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

om

# How Ransomware works



ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

Message invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

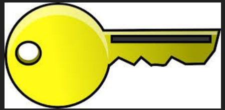
Let us know if you have any questions.

We greatly appreciate your business!
Bonnie vause

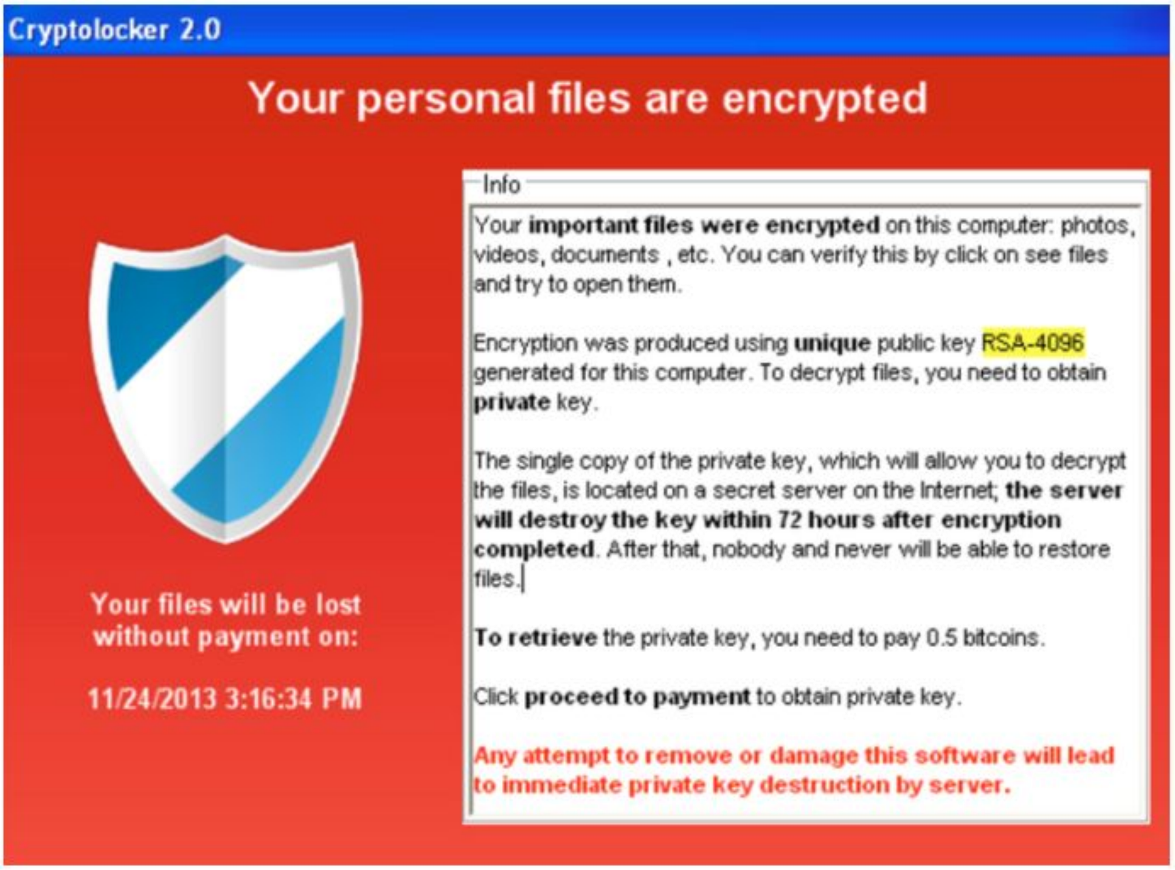
********************************************************************************
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.
********************************************************************************

See more about Bonnie vause.

Malicious email



# How R



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.

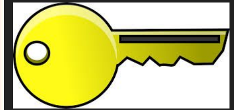
Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

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.

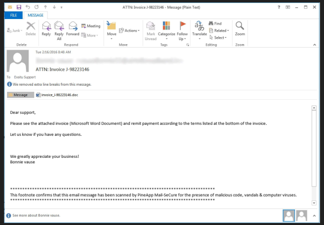
**To retrieve** the private key, you need to pay 0.5 bitcoins.

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.**



# How Ransomware works



ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

Message invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

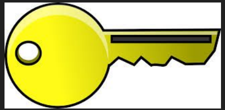
Let us know if you have any questions.

We greatly appreciate your business!
Bonnie vause

```
**********************************************************************************
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.
**********************************************************************************
```

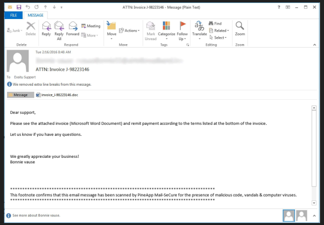
See more about Bonnie vause.

Malicious email



What can Travis do now?

# How Ransomware works



ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!
Bonnie vause

***********************************************************************************

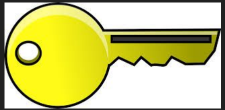
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.

*********************************************************************************

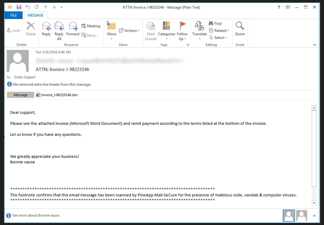
See more about Bonnie vause.

Malicious email

1. Pay the criminal



# How Ransomware works



ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

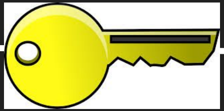
We greatly appreciate your business!
Bonnie vause

***************************************************************************************
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.
***************************************************************************************

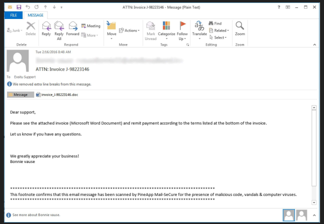
See more about Bonnie vause.

Malicious email

1. Pay the criminal



# How Ransomware works



ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

Message invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

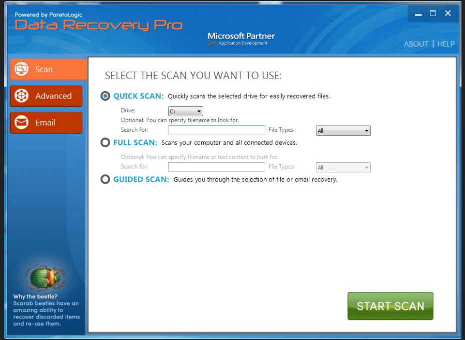
We greatly appreciate your business!
Bonnie vause

****************************************************************************************
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.
****************************************************************************************

See more about Bonnie vause.

Malicious email

2. Find experts / resource to disinfect system without paying the criminal



SELECT THE SCAN YOU WANT TO USE:

● QUICK SCAN: Quickly scans the selected drive for easily recovered files.

Drive: C:

Optional: You can specify filename to look for.

Search for: File Types: All

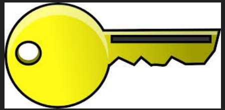
○ FULL SCAN: Scans your computer and all connected devices.

Optional: You can specify filename or text content to look for.

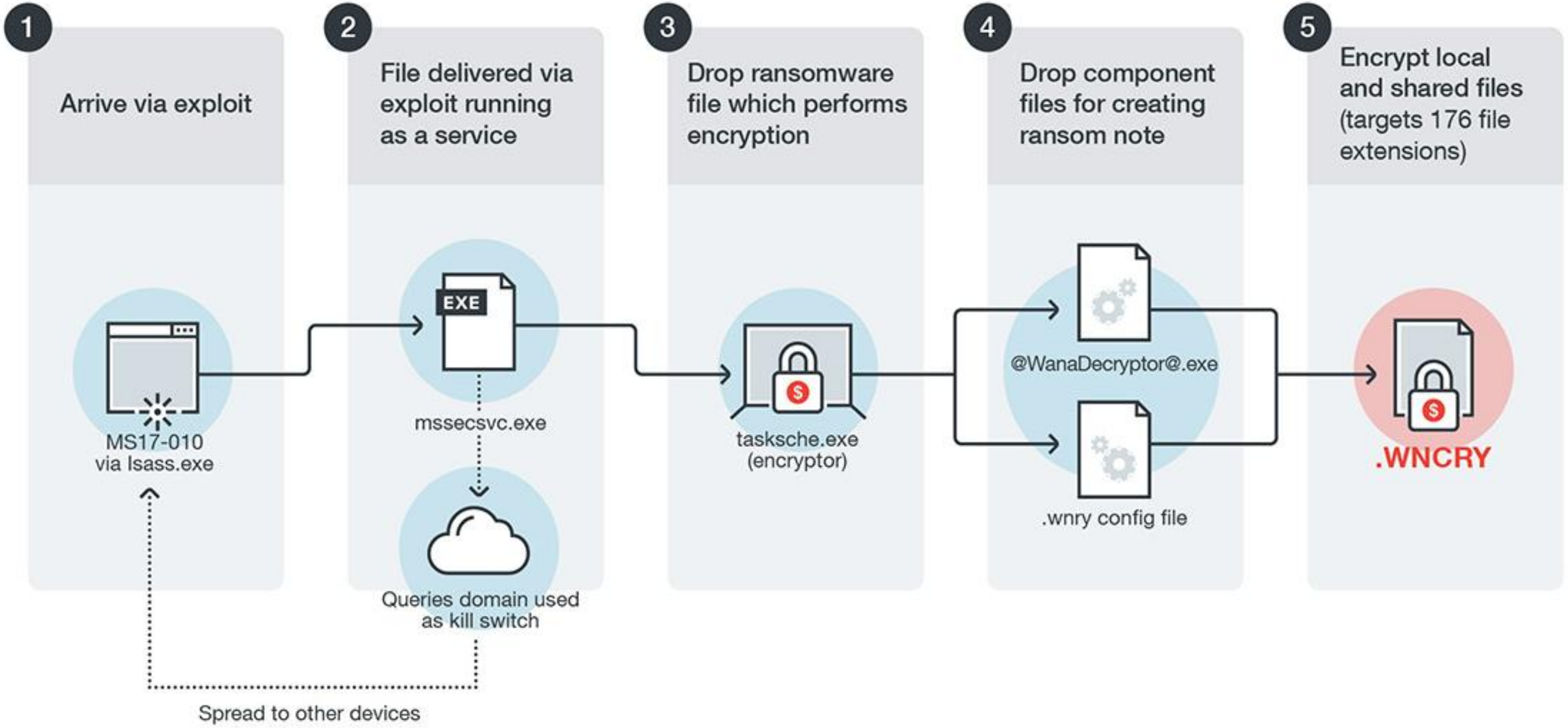
Search for: File Types: All

○ GUIDED SCAN: Guides you through the selection of file or email recovery.

Why the beetle?
Scarab beetles have an amazing ability to recover discarded items and re-use them.



# How Ransomware works: Wannacry



1 Arrive via exploit

2 File delivered via exploit running as a service

3 Drop ransomware file which performs encryption

4 Drop component files for creating ransom note

5 Encrypt local and shared files (targets 176 file extensions)

MS17-010 via lsass.exe

EXE

mssecsvc.exe

Queries domain used as kill switch

Spread to other devices

tasksche.exe (encryptor)

@WanaDecryptor@.exe

.wnry config file

.WNCRY

# History of ransomware

## When was the first instance/attack?

In 1989, Joseph L. Popp created the first ransomware virus, It was called the AIDS Trojan, also known as the PC Cyborg. Popp sent 20,000 infected diskettes labeled “AIDS Information – Introductory Diskettes” to attendees of the World Health Organization’s international AIDS conference. The AIDS Trojan was “generation one” ransomware malware and relatively easy to overcome.

The Trojan used simple symmetric cryptography and tools were soon available to decrypt the file names. But the AIDS Trojan set the scene for what was to come.

# History of ransomware

## When did it become more of a problem?

In 2011 the first large scale ransomware outbreak started.

Ransomware became more successful in extorting money from its victims with new anonymous payment services.

There were about 30,000 new samples detected in each of the first two quarters of 2011 and by late 2011 the number of samples detected doubled to 60,000.

In 2013 ransomware started to evolve and infect android smartphones and OSX devices.

A business will fall victim to a ransomware attack every 14 seconds by 2019, and every 11 seconds by 2021

# History of ransomware

## How much has ransomware made?

- In 2018 ransomware was estimated to cost businesses more than 8 billion dollars, up from just one billion in 2016.
- The average cost of ransomware attacks on businesses is $133,000
- Ransomware has a minimum global revenue of 1 billion dollars.

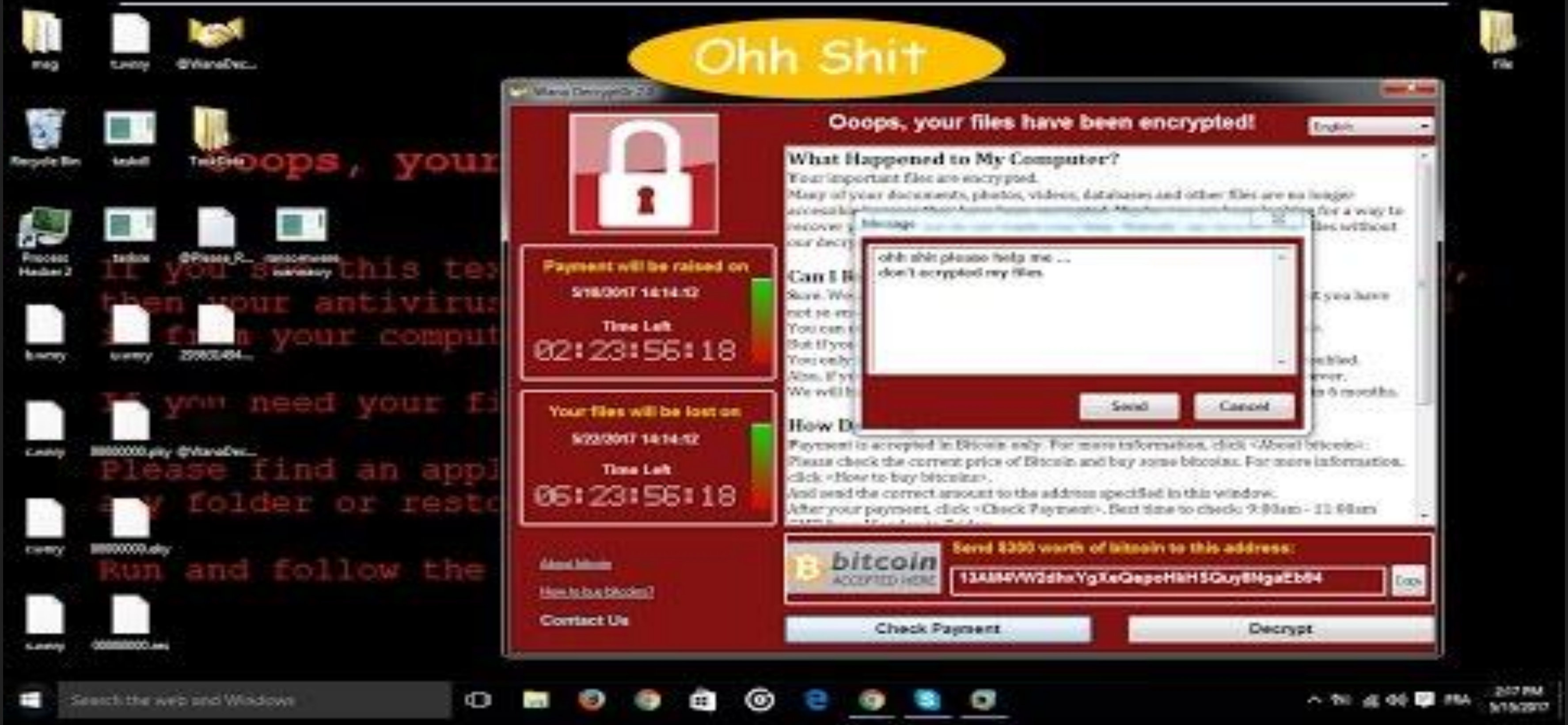
# How ransomware effects operating systems

1) Before encryption begins, the malware makes initializations to create a log file. It also collects information using the g_init function and stores it in GINFO with the following info:work_path, self_path, self_hash, os, os_version, os_arch, nic, locale, timezone, id, seed_sys, seed_hash, password, key_app_rsa_pub, key_rsa_size, cc_server_size, cc_timeout, cc_timeout_conn, url_list_size, url_dn_list_size

2) Now, the encryption can begin. Erebus uses algorithms to randomly generate keys on the local machine, then encrypts the key using a RSA-2048 algorithm with its public key (which thus makes decryption impossible without the RSA-2048 private key).

The file encrypted by EREBUS ransomware contains the following information: Header, Encrypted original file name, Encrypted AES key, Encrypted RC4 key, RC4 encrypted file data

3) Finally, it asks for payment. After encrypting files, Erebus deletes itself from the infected server.  The _DECRYPT_FILE then provides instructions for installing the TOR browser and lists several URLs for submitting payment to decrypt the files.



Ooops, your files have been encrypted!

**What Happened to My Computer?**
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessib … for a way to recover y … files without our decry…

**Can I R…**
Sure. We … if you have not so en…
You can …
But if you…
You only … scheduled.
Also, if y… server.
We will h… in 6 months.

**How D…**
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Message

ohh shit please help me ...
don't ecrypted my files

Send | Cancel

Payment will be raised on
5/18/2017 14:14:12
Time Left
02:23:56:18

Your files will be lost on
5/22/2017 14:14:12
Time Left
06:23:56:18

About bitcoin
How to buy bitcoins?
Contact Us

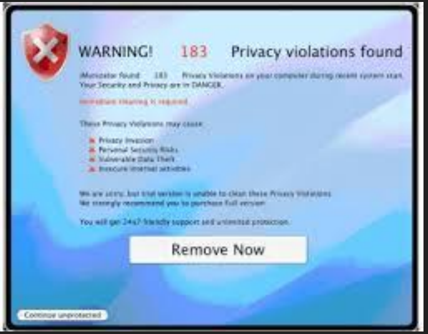
bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

Check Payment | Decrypt

# Main Types of Ransomware



WARNING! 183 Privacy violations found

iMonitor found 183 Privacy Violations on your computer during recent system start.
Your Security and Privacy are in DANGER.

Immediate cleaning is required.

These Privacy Violations may cause:

- Privacy Invasion
- Personal Security Risks
- Vulnerable Data Theft
- Insecure internet activities

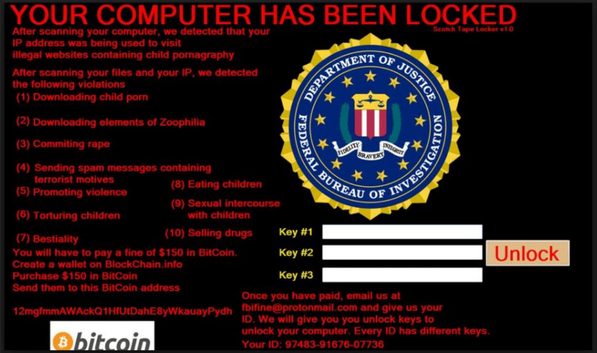
We are sorry, but trial version is unable to clean these Privacy Violations.
We strongly recommend you to purchase Full version.

You will get 24x7 friendly support and unlimited protection.

Scareware

(pop-ups)

Screen lockers (Fake FBI scams)



YOUR COMPUTER HAS BEEN LOCKED

Scotch Tape Locker v1.0

After scanning your computer, we detected that your
IP address was being used to visit
illegal websites containing child pornagraphy

After scanning your files and your IP, we detected
the following violations

(1) Downloading child porn

(2) Downloading elements of Zoophilia

(3) Commiting rape

(4) Sending spam messages containing terrorist motives

(5) Promoting violence

(6) Torturing children

(7) Bestiality

(8) Eating children

(9) Sexual intercourse with children

(10) Selling drugs

You will have to pay a fine of $150 in BitCoin.
Create a wallet on BlockChain.info
Purchase $150 in BitCoin
Send them to this BitCoin address

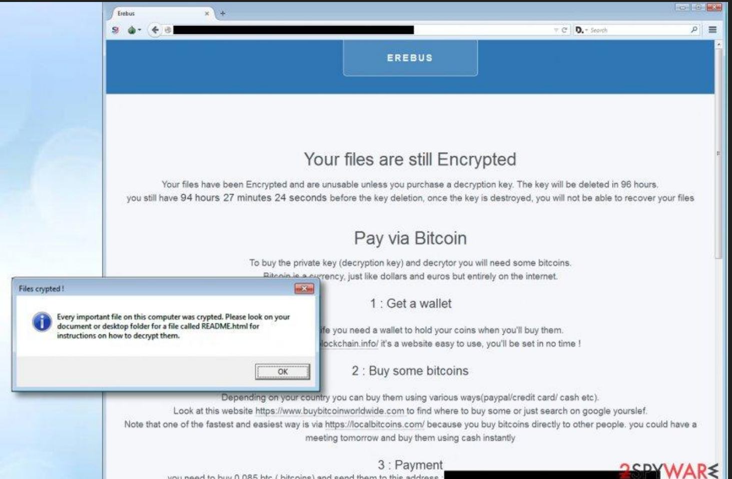
12mgfmmAWAckQ1HfUtDahE8yWkauayPydh

Key #1

Key #2

Key #3

Once you have paid, email us at
fbifine@protonmail.com and give us your
ID. We will give you you unlock keys to
unlock your computer. Every ID has different keys.
Your ID: 97483-91676-07736



Erebus

[redacted]

EREBUS

Your files are still Encrypted

Your files have been Encrypted and are unusable unless you purchase a decryption key. The key will be deleted in 96 hours.
you still have 94 hours 27 minutes 24 seconds before the key deletion, once the key is destroyed, you will not be able to recover your files

Pay via Bitcoin

To buy the private key (decryption key) and decrytor you will need some bitcoins.
Bitcoin is a currency, just like dollars and euros but entirely on the internet.

1 : Get a wallet

...fe you need a wallet to hold your coins when you'll buy them.
...lockchain.info/ it's a website easy to use, you'll be set in no time !

2 : Buy some bitcoins

Depending on your country you can buy them using various ways(paypal/credit card/ cash etc).
Look at this website https://www.buybitcoinworldwide.com to find where to buy some or just search on google yourslef.
Note that one of the fastest and easiest way is via https://localbitcoins.com/ because you buy bitcoins directly to other people. you could have a meeting tomorrow and buy them using cash instantly

3 : Payment

you need to buy 0.085 btc ( bitcoins) and send them to this address : [redacted]

Files crypted !

Every important file on this computer was crypted. Please look on your document or desktop folder for a file called README.html for instructions on how to decrypt them.

Encrypting Ransomware

# Solutions?

CryptoDrop is protecting your files from ransomware.

Thanks for purchasing the CryptoDrop Fast Recovery Edition!

Your license is valid until 4/24/2018.

Copyright © 2017 CryptoDrop, LLC

Version 1.0.38.1459

Cybersecurity programs
Backups
Decryptors
Patch and Update software
Educate users

nomoreransom.org

# Local Backups

Local backup solutions

Pros:

Accessibility

Reliability

Privacy

Cons:

Vulnerable to ransomware

Maintenance

# Cloud Backups

Cloud backup solutions

Pros:

Security

Scalability

Cons:

Restricted to bandwidth

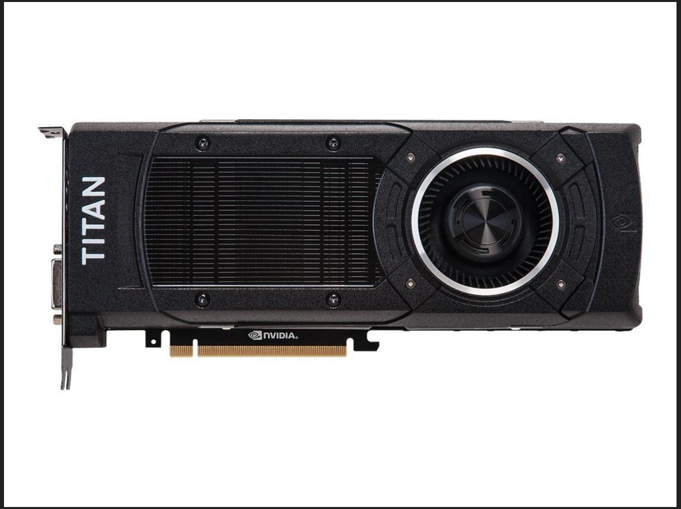
Trusting a 3rd party

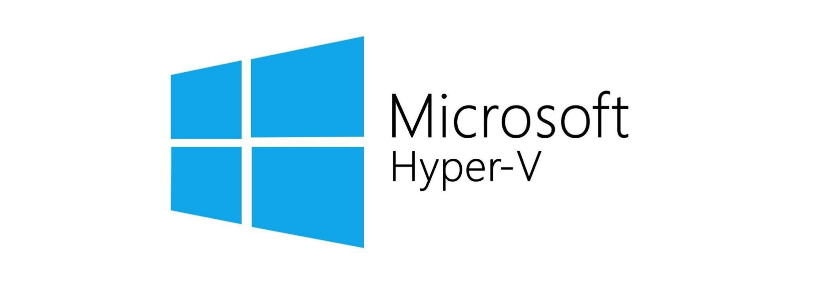
# Decryption Methods

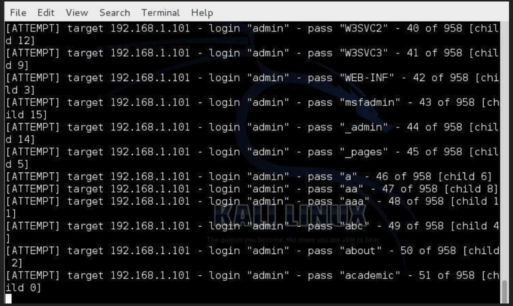
[nomoreransom.org](nomoreransom.org)

Brute force

Sandboxing analysis







```
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC2" - 40 of 958 [chil
d 12]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC3" - 41 of 958 [chil
d 9]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "WEB-INF" - 42 of 958 [chi
ld 3]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "msfadmin" - 43 of 958 [ch
ild 15]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_admin" - 44 of 958 [chil
d 14]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_pages" - 45 of 958 [chil
d 5]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "a" - 46 of 958 [child 6]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aa" - 47 of 958 [child 8]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aaa" - 48 of 958 [child 1
1]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "abc" - 49 of 958 [child 4
]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "about" - 50 of 958 [child
 2]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "academic" - 51 of 958 [ch
ild 0]
```

# Future of ransomware

- Artificial Intelligence
- IoT
- Targeted attacks

Mac ransomware (KeRanger, 2016)

# References

https://invenioit.com/security/linux-ransomware-attacks-rise/

https://www.knowbe4.com/ransomware

https://safeatlast.co/blog/ransomware-statistics/