



SIMPLY
SECURE

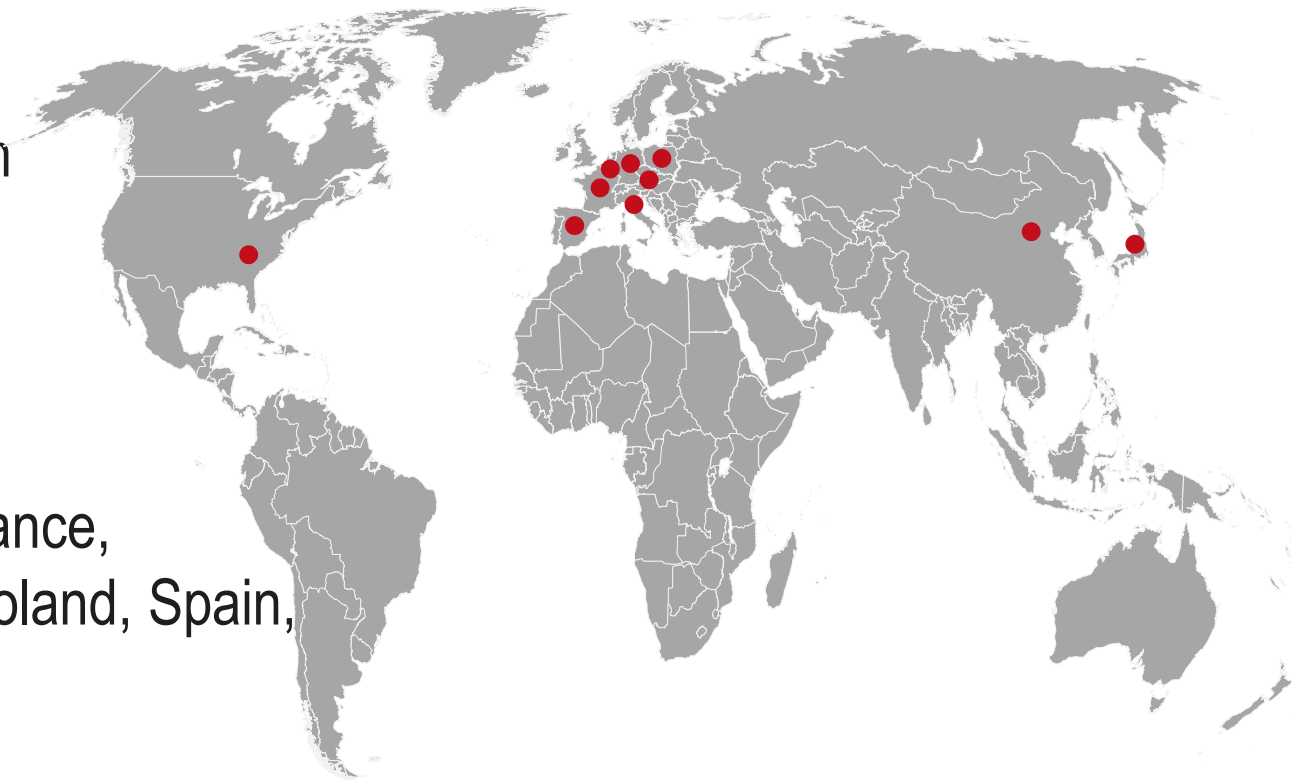
THE REAL TRUTH BEHIND RANSOMWARE

EDDY WILLEMS – SECURITY EVANGELIST

TWITTER: @EDDYWILLEMS

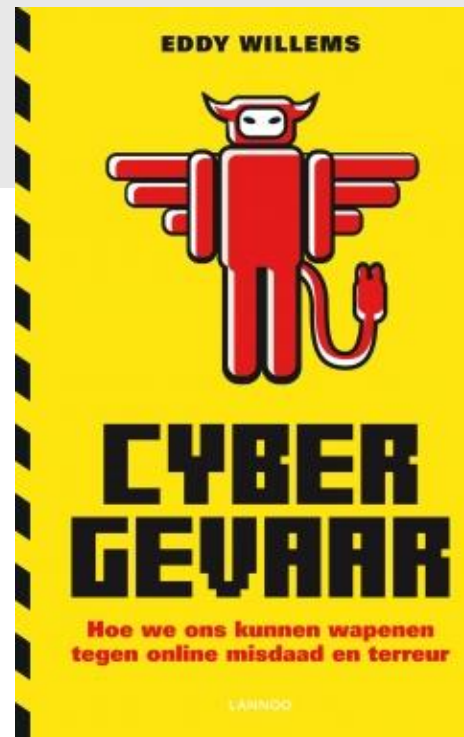
OFFERING SECURITY SOLUTIONS WORLDWIDE

- Founded in Bochum, Germany in 1985
- First AV solution in 1987
- Global head office & development: Bochum
- Security solutions for home and business
- Solutions available in 90+ countries
- ~ 500 employees worldwide
- Subsidiaries in Austria, Belgium, China, France, Germany, Italy, Japan, The Netherlands, Poland, Spain, Switzerland and the United States



● Subsidiaries

INTRODUCTION



- **Security Evangelist at G Data Software AG:**
- Personally Involved in the security industry since 1989
- Worked as **Cyber Security Expert** for CERT-organisations and security companies like Kaspersky Lab, Westcon(Noxs), etc...
- **Director** of **EICAR**(+Co-founder), **AMTSO** and **LSEC** (3 international security industry org.)
- **Researcher/Technical Spokesperson**, interviewed/cited in 1000's publications/media (CNN,..)
- **Author** of the book ,Cybergevaar' (BE/NL Dutch 2013) ,Cybergefahr' (DE German 2016)

RANSOMWARE

1. Screen Lockers – 2. Crypto

Blocking device/work

Unusable + encryption

Pay Ransom or loose data/time

=> Time and data critical!

THE MONEY PROBLEM

The global impact of ransomware



RANSOMWARE money

EREBUS

Data crypted

Every important file (documents, photos, videos etc) on this computer has been encrypted using an unique key for this computer. It is impossible to recover your files without this key. You can try to open them they won't work and will stay that way.

That is, unless you buy a decryption key and decrypt your files.

Click 'recover my files' below to go to the website allowing you to buy the key.

From now on you have 96 hours to recover the key after this time it will be deleted and your files will stay unusable forever

Your id is : " you can find this page on your desktop and document folder Use it to

if the button below doesn't work you need to download a web browser called 'tor browser'

download by clicking [here](#) then install the browser, it's like chrome, firefox or internet explorer except it allows you to browse to special websites. once it's launched browse to <http://erebus5743lnq6db.onion>

Recover my files

Crypted Files :

**SF metro rail system: Criminal asking 100 Bitcoins ... 4 year old Java vulnerability
Hosting company Nayana (South Korea) ... over 1 million US \$ paid**

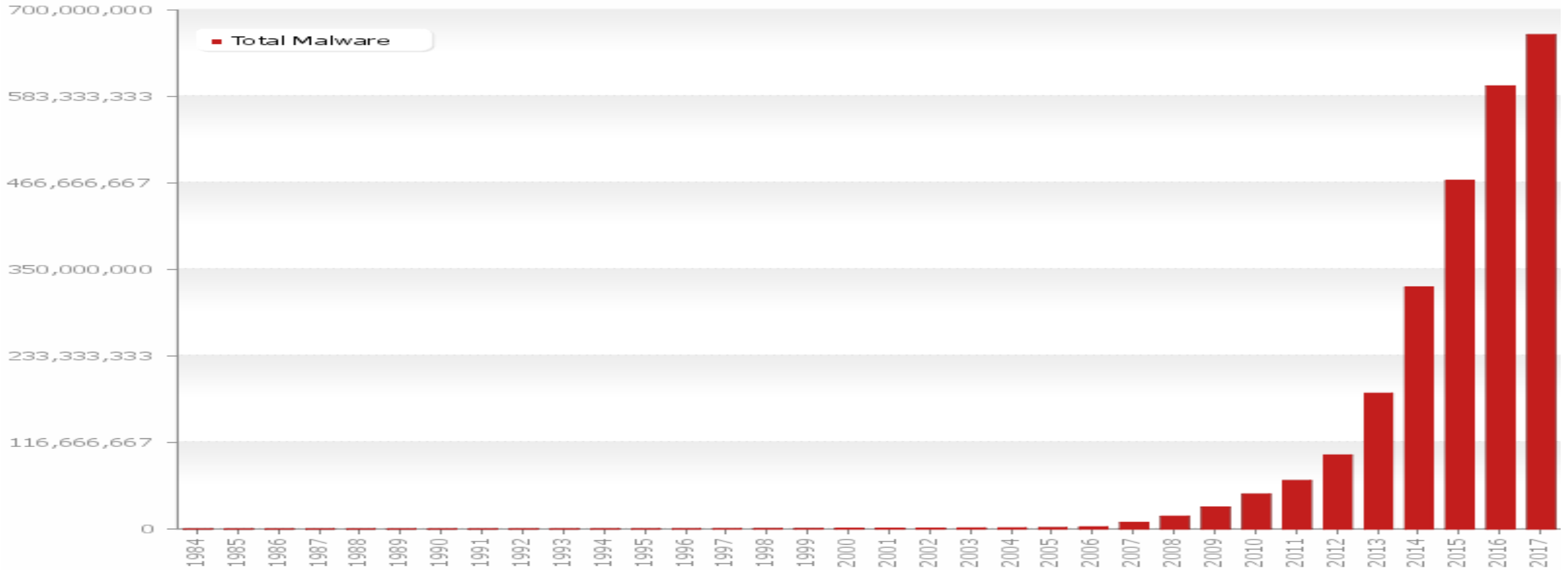
MEMORIES

AIDS INFORMATION DISKETTE

- 1989 PC Cyborg Corporation, Joseph L. Popp
- Diskette with AIDS Information given at WHO-Conference
- Over 20.000 copies via PC World magazine
- Encrypts HD after some reboots
- Asked \$189 ransom to pay to P.O.Box in Panama
- One of the first to decrypt/solution



TODAY'S MALWARE THREATS



Last update: 09-05-2017 08:29

Copyright © AV-TEST GmbH, www.av-test.org

400.000 new samples a day

Over 600 million samples => 99,9% not visible!

HOW TO GET INFECTED

most known modus

operandi

SPAMMING MAILS WITH DOCS, ZIP, JAVACRIPT, ETC...

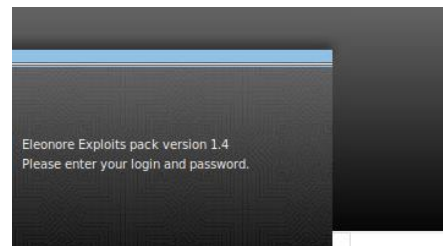
The screenshot shows a Microsoft Outlook window titled "Invoice - Message (Plain Text)". The ribbon is set to "MESSAGE" and includes tabs for "FILE" and "MESSAGE". The "MESSAGE" tab contains several groups of actions: "Delete" (with a trash can icon), "Respond" (with Reply, Reply All, and Forward icons), "Quick Steps" (with a "Create New" button), "Move" (with folder and document icons), "Tags" (with Mark Unread, Categorize, and Follow Up icons), "Editing" (with Translate and Zoom icons), and another "Zoom" group (with a magnifying glass icon). The email header shows a sender profile picture, the date and time "Thu 2/18/2016 2:48 AM", the name "Barrett Gallagher", and the email address "<GallagherBarrett631@airtelbroadband.in>". The subject is "Invoice". The "To" field is empty. Below the header, there is a message bar with a "Message" tab and an attachment icon, followed by the text "Invoice74531951.doc (44 KB)". The main body of the email contains the following text: "Dear Sir/Madam,", "I trust this email finds you well,", "Please see attached file regarding clients recent bill. Should you need further assistances lease feel free to email us.", "Best Regards,", "Barrett Gallagher", "Community Health Systems, Inc. www.chs.net".

ige (Plain Text)

VISITING INFECTED WEBSITES



OTHER EXPLOIT KITS



Phoenix Exploit's Kit



Other:

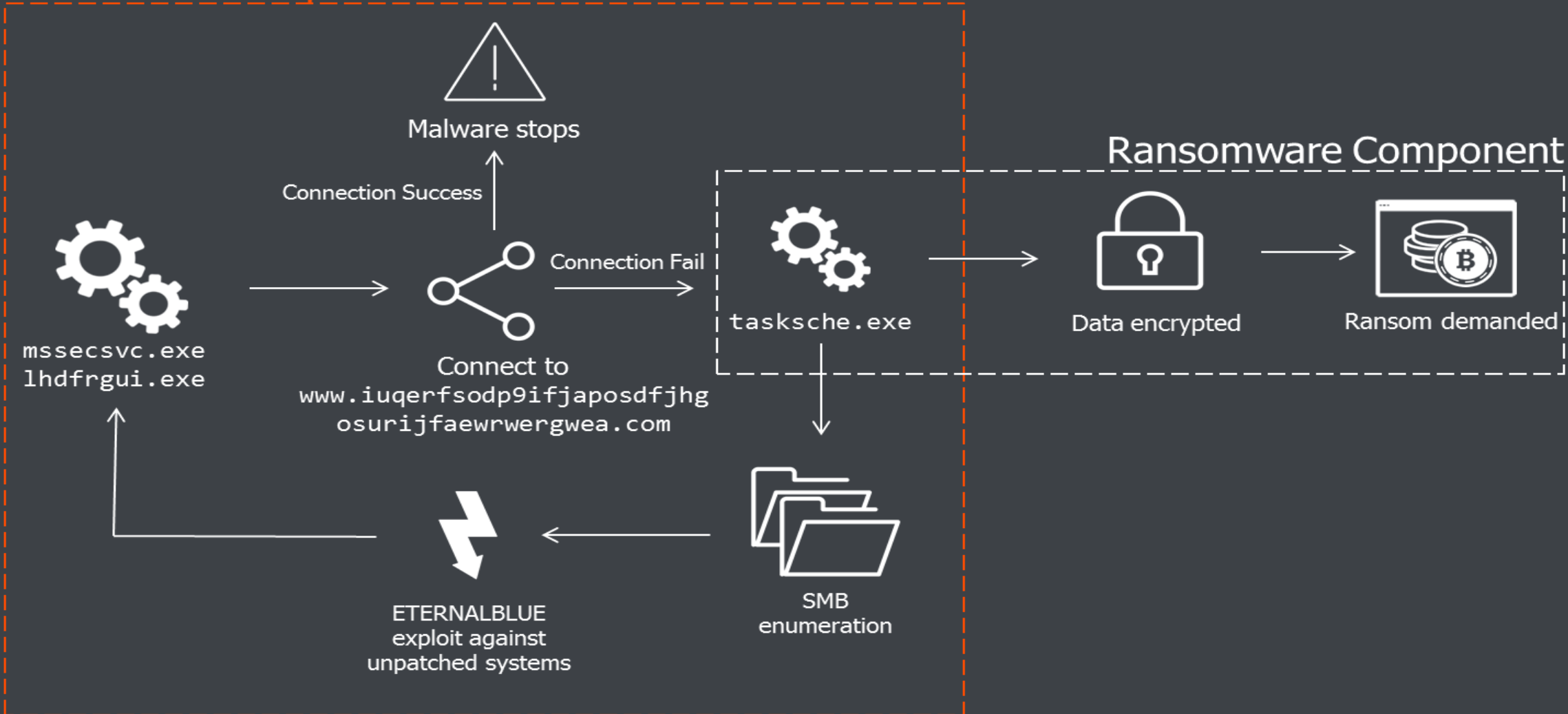
Malvertising, Downloads,

Botnet use

And ...

SMB WORM CAPABILITIES

SMB Worm Component



TRIGGER

**Why ransomware
works?**

THE HUMAN FACTOR

2011 Recruitment plan - Message

Message

Reply Reply Forward
to All

Delete Move to Other
Folder Actions

Block Sender Not Junk
Sender

Safe Lists

Junk E-mail

From: web master [webmaster@beyond.com]
To: [redacted]@emc.com
Cc: [redacted]
Subject: 2011 Recruitment plan

YouTube Broadcast Yourself™ Worldwide | English

Home Videos Channels Community

CLICK HERE FORN PORN ==>

Rate: ☆☆☆☆☆ 0 ratings Views: 1,962

Share Favorite Playlists Flag

Send Video MySpace Facebook more share options

twitter

Name or location search Home Find & Follow Settings Help Sign out

o_o michelle1 [redacted]

Follow

Check out my new website
[http://\[redacted\].m/g...](http://[redacted].m/g...)
2 days ago from web

RSS Older >

About

Name michelle1 [redacted]
Web [http://\[redacted\]](http://[redacted])

Stats

Following 2,049
Followers 52
Favorites 0
Updates 1

Following

Rob [redacted]

© 2008 Twitter About Us Contact Blog Status Downloads API Help Jobs TOS Privacy

Pensacola State College). [Learn why we included this.](#) 2012,
CA 94043, USA

have a relaxing



WEEKEND

M

BIT  **LAUNDER**

TOR URL: <http://yxku52sygpn7oubv.onion/>

[TOR Wallet](#) | [Bitcoin Tumbler](#) |

[Emergency Support](#) |



ANONYMIZE
BITCOIN

BITCOIN MIXER

... the perfect bitcoin mixing service...

Powerful tools to launder your bitcoins.

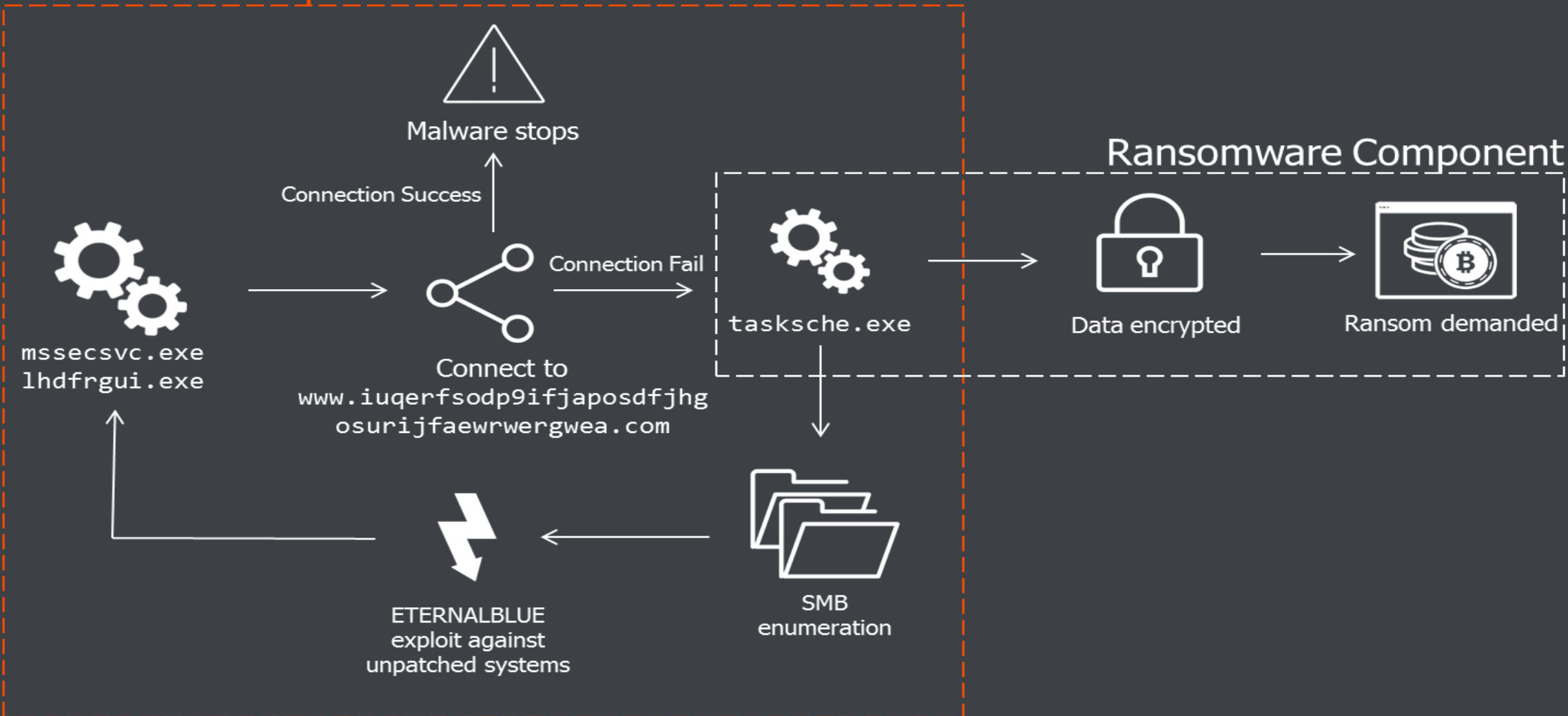
Our bitcoin mixing service will fully anonymize bitcoin.

WHY IS RANSOMWARE SO DIFFICULT TO DETECT?

- It features built-in traffic anonymizers, like **TOR** and **Bitcoin**, to avoid tracking by law enforcement agencies and to receive ransom payments
- **Communication** with CC servers is **encrypted** and difficult to detect in network traffic
- It uses **anti-sandboxing mechanisms** so that antivirus analyzing techniques won't pick it up
- It employs **domain shadowing** to conceal exploits and hide the communication between the downloader (payload) and the servers controlled by cyber criminals (where the ransomware is stored)
- It features **Fast Flux**, another technique used to keep the source of the infection anonymous (swap the IP addresses constantly and with high frequency by changing DNS records, so that automated analysis mechanisms cannot detect the real source of the infection)
- It deploys **encrypted payloads** which can make it more difficult for antivirus to see that they include malware
- It has **polymorphic behavior** that endows the ransomware with the ability to mutate
- It has **the ability to remain dormant**

WANNACRY ... KillSwitch OR NOT?

SMB Worm Component



RANSOMWARE EXAMPLES

CRYPTO RANSOMWARE EXAMPLES

!!! 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, V
To receive your private key for
1. <http://6dbxgqam4crv6rr6.onion>
2. <http://6dbxgqam4crv6rr6.onion>
3. <http://6dbxgqam4crv6rr6.onion>
4. <http://6dbxgqam4crv6rr6.onion>

If all of this addresses are no
1. Download and install To
2. After a successful instal
3. Type in the address bar
4. Follow the instructions c

!!! Your personal identification



The image shows a ransomware message overlaid on a browser window. The message is in red text on a black background. The browser window shows a page titled 'Locky Decrypter Page' with a URL bar containing '6dbxgqam4crv6rr6.onion'. The page content is in white text on a blue background, mentioning 'Locky Decrypter' and 'How to buy Locky decrypter?'. A Bitcoin logo is visible at the bottom of the page. A Notepad window in the top right corner shows the ransomware message in French, including the same instructions and a personal identifier '00B245586'.

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.

 bitcoin

Locky_recover_instructions.txt - Bloc-notes
Fichier Edition Format Affichage ?
!!! INFORMATION IMPORTANTE !!!
Tous vos fichiers ont été chiffrés avec le
Plus d'informations peuvent être trouvées.
<http://fr.wikipedia.org/wiki/Chiffrement>
http://fr.wikipedia.org/wiki/Advanced_E
Déchiffrer vos fichiers est seulement poss
de déchiffrement se trouvant sur notre ser
Pour recevoir votre clé privée suivez l'un
1. <http://6dtxgqam4crv6rr6.tor2web.org>
2. <http://6dtxgqam4crv6rr6.onion.to/00>
3. <http://6dtxgqam4crv6rr6.onion.cab/0>
4. <http://6dtxgqam4crv6rr6.onion.1fnk/>
Si aucune de ces adresses ne fonctionne, s
1. Téléchargez et installez le navigat
2. Après son installation, démarrez-le
3. Tapez dans la barre d'adresse: 6dtx
4. Suivez les instructions du site.
!!! votre identifiant personnel: 00B245586



6:42 AM
3/24/2016

KERANGER RANSOMWARE



The image shows a screenshot of the Transmission website homepage. The browser address bar displays "https://www.transmissionbt.com". The main header features the word "TRANSMISSION" in large white letters on a red background, with the tagline "A Fast, Easy, and Free BitTorrent Client" below it. To the right is a large 3D-style icon of a download button. A navigation menu includes links for MAIN, ABOUT, DOWNLOAD, DEVELOPMENT, ADD-ONS, CONTENT, and SUPPORT. A "Feature Spotlight" section lists several features, and a box highlights "Transmission 2.90" with links for "Download Now", "Release Notes", and "Previous Releases". The footer contains a PayPal donation link, copyright information, and a logo for CocheFly.

← → ↻ <https://www.transmissionbt.com> ☰

TRANSMISSION

A Fast, Easy, and Free BitTorrent Client

MAIN ABOUT DOWNLOAD DEVELOPMENT ADD-ONS CONTENT SUPPORT

Feature Spotlight:

- Uses **fewer resources** than other clients
- Native **Mac**, **GTK+** and **Qt** GUI clients
- **Daemon** ideal for servers, embedded systems, and headless use
- All these can be remote controlled by **Web** and **Terminal** clients
- Local Peer Discovery
- Full **encryption**, **DHT**, **μTP**, **PEX** and **Magnet Link** support

[Learn More...](#)

Transmission 2.90

[Download Now](#)
[Release Notes](#)
[Previous Releases](#)

 [Donate to Transmission](#) © Copyright 2005 - 2016 Transmission Project, All Rights Reserved Bandwidth provided by 
Design by **Stranded Design**, implemented by **Booable**

LINUX.ENCODER RANSOMWARE (FOR WEBSERVERS)



inurl:README_FOR_DECRYPT.txt



Web

Images

Videos

Maps

News

More ▾

Search tools

About 2,920 results (0.49 seconds)

pub.u-bordeaux3.fr/downloader/README_FOR_DECRYPT.txt

A description for this result is not available because of this site's robots.txt – learn more.

[Your personal files are encrypted! Encryption was produced ...](http://www.cicinailsnspa.com/README_FOR_DECRYPT.txt)

www.cicinailsnspa.com/README_FOR_DECRYPT.txt ▾

Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to ...

[README_FOR_DECRYPT.txt.encrypted - Lehmann KG](http://www.lehmann-kg.com/cache/README_FOR_DECRYPT.txt.encrypted)

www.lehmann-kg.com/cache/README_FOR_DECRYPT.txt.encrypted

A description for this result is not available because of this site's robots.txt – learn more.

SynoLocker™

Automated Decryption Service

Logout

7 days, 13 hours, 35 mins, 25 secs

PRICE OF DECRYPTION KEY DOUBLE WHEN COUNTDOWN EXPIRE

To decrypt your files you need to buy a unique decryption key that is linked to your identification code.

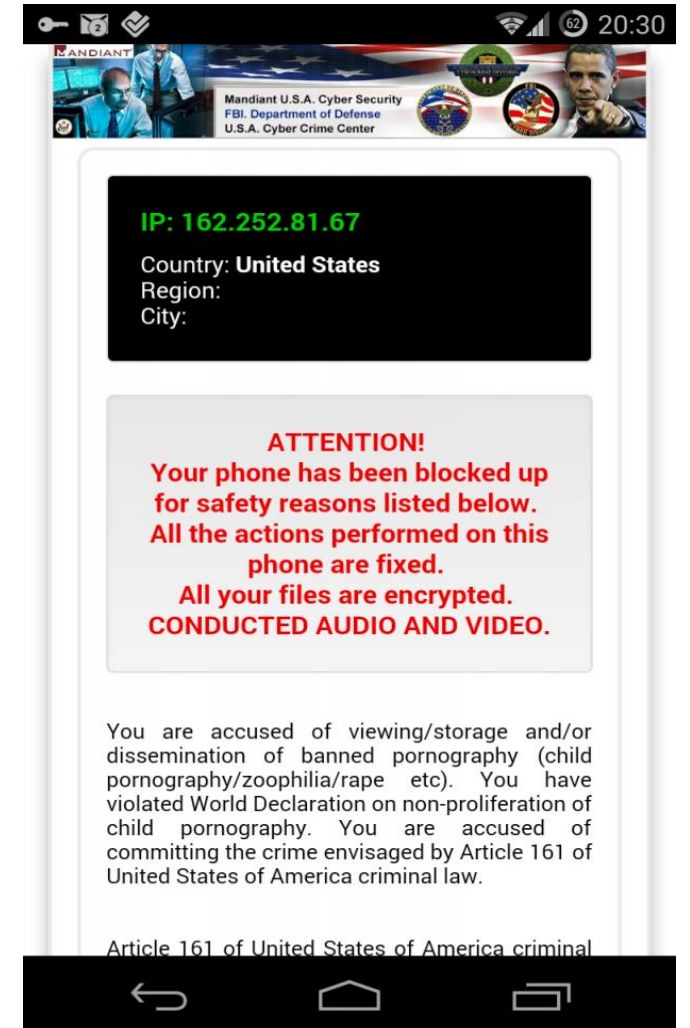
The only accepted payment method is Bitcoin.

Visit the [help](#) page if you need information on how to purchase and send a Bitcoin payment

Follow these simple steps to get your decryption key:

AND ...

Reveton for Android!



WANNACRY

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

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 GMT from Monday to Friday.


Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **Send \$600 worth of bitcoin to this address:**
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

REMEDICATION



**TO PAY
OR
NOT TO PAY?**

REMEDIATION = KNOWN TECHNIQUES => Inside G DATA products

- Security package (Endpoint Protection) installed on every system
- Activate or use behavior protection and exploit protection
- Patch Management (PASAP = Patch ASAP)
- Backups (external and not always connected drives)
- Only admin rights for certain users
- Limit user rights on shares or in-the-cloud
- Disable macro's where not used!
- Mailgateway: filter out all executables (eg. .exe .com .js .htm .scr ...etc)
- Mailgateway: use your own filepassing method (eg. zip with specific password)



**BLOCKING TOOLS:
BEHAVIOUR BLOCKING
ANTI-EXPLOIT
ANTI-RANSOMWARE**

WITHOUT G DATA'S ANTI-RANSOMWARE TECHNOLOGY



Spora Ransomware running on an unprotected system



Search the web and Windows



ENG 3:19 AM
DE 1/19/2017

WITH G DATA'S ANTI-RANSOMWARE TECHNOLOGY

1 Element 1 Element ausgewählt (138 KB)

Name	Änderungsdatum	Typ	Größe
Rechung_234711	18.01.2017 14:30	HTML-Anwendung	139 KB

3 Elemente 1 Element ausgewählt (81,0 KB)

Änderungsdatum	Typ	Größe
18.01.2017 14:30	Dateiordner	
10.08.2016 16:35	Anwendung	237 KB
18.01.2017 14:26	ZIP-komprimierte...	82 KB

G DATA INTERNET SECURITY

14:30
18.01.2017

Spora Ransomware running on a system protected by G DATA

THE FUTURE?

Ransomware (and most other malware) is seen as possible data leakage!
You need to notify this ...

GDPR
IS COMING

You need products you who
can give you lists and
summaries like G DATA's

The real problem is that new Ransomware will arise and ask you a Ransom just below 4% of your annual turnover or below 20 million Euro ... so you don't have to notify if you pay! (at least that's what they say)



GDATA

G

THANK YOU!

TWITTER: @EDDYWILLEMS

A secure solution for mobile threats ...

