THE REAL TRUTH BEHIND RANSOMWARE

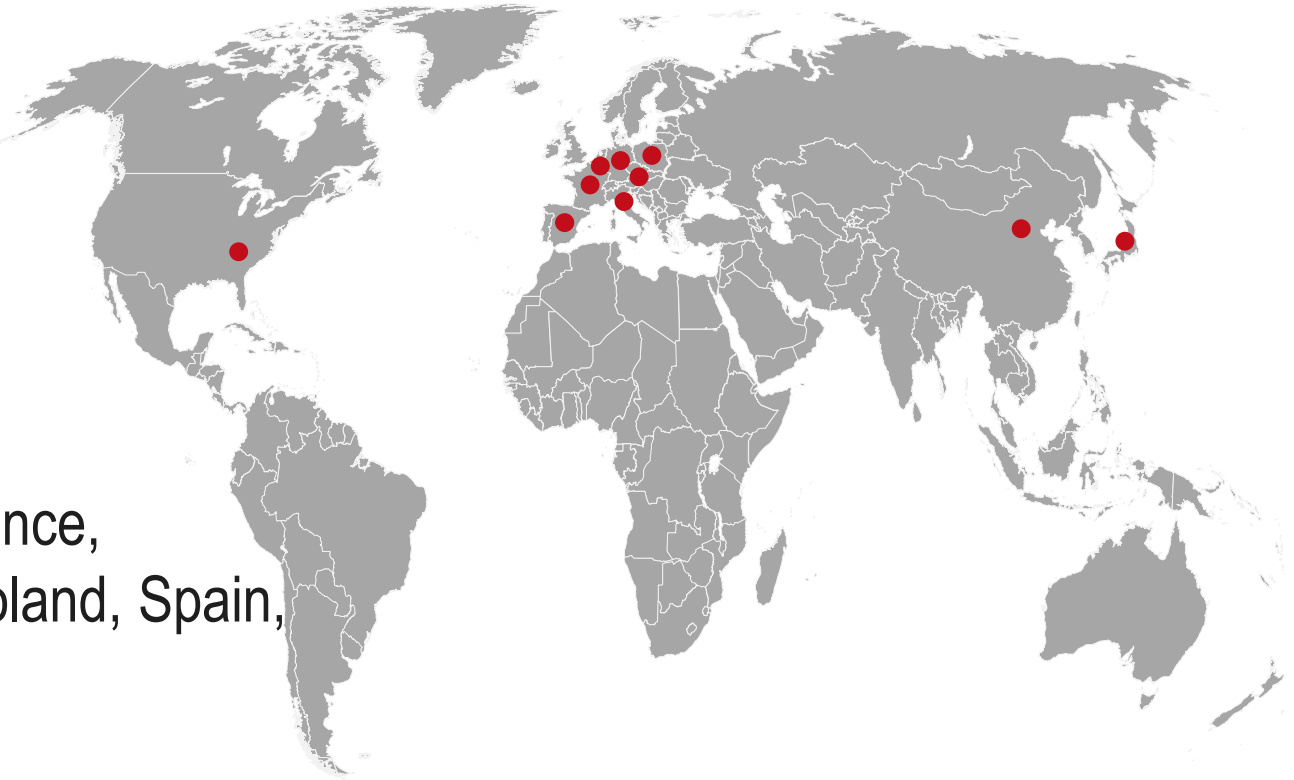
EDDY WILLEMS – SECURITY EVANGELIST

TWITTER: @EDDYWILLEMS

G DATA SIMPLY SECURE

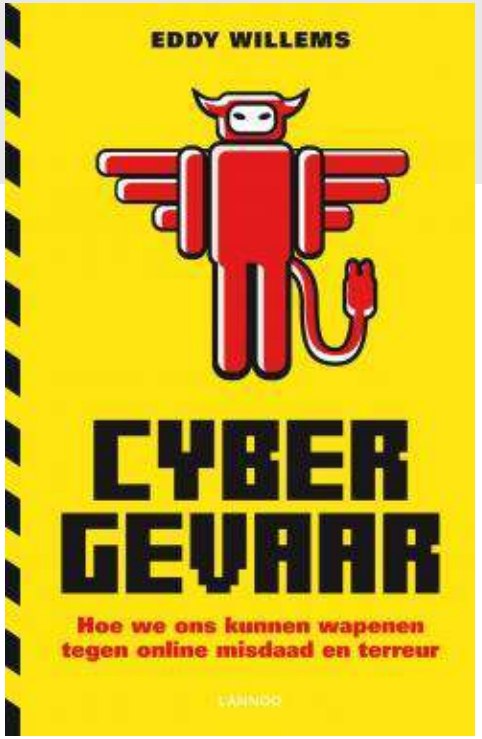
OFFERING SECURITY SOLUTIONS WORLDWIDE

- 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 Sofware 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

RANSOMWARE money

SF metro rail system: Criminal asking 100 Bitcoins … 4 year old Java vulnerability

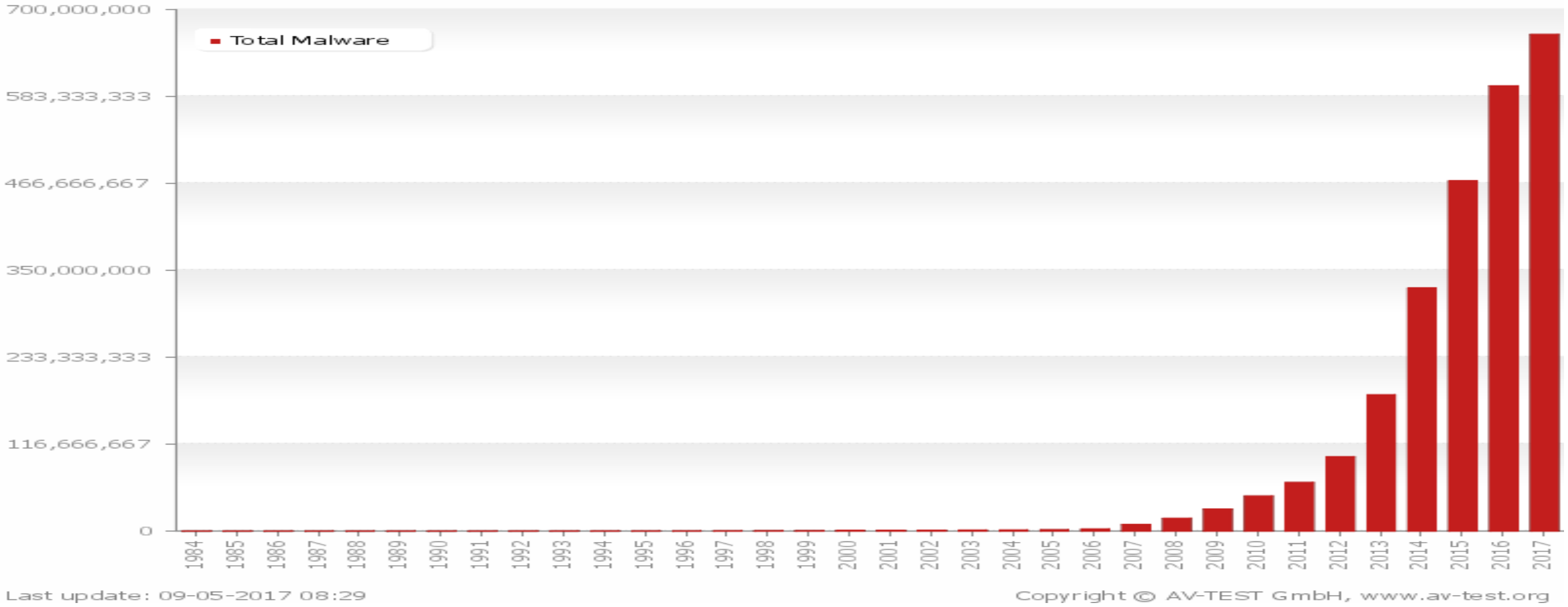
Hosting company Nayana (South Korea) … over 1 million US $ paid

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



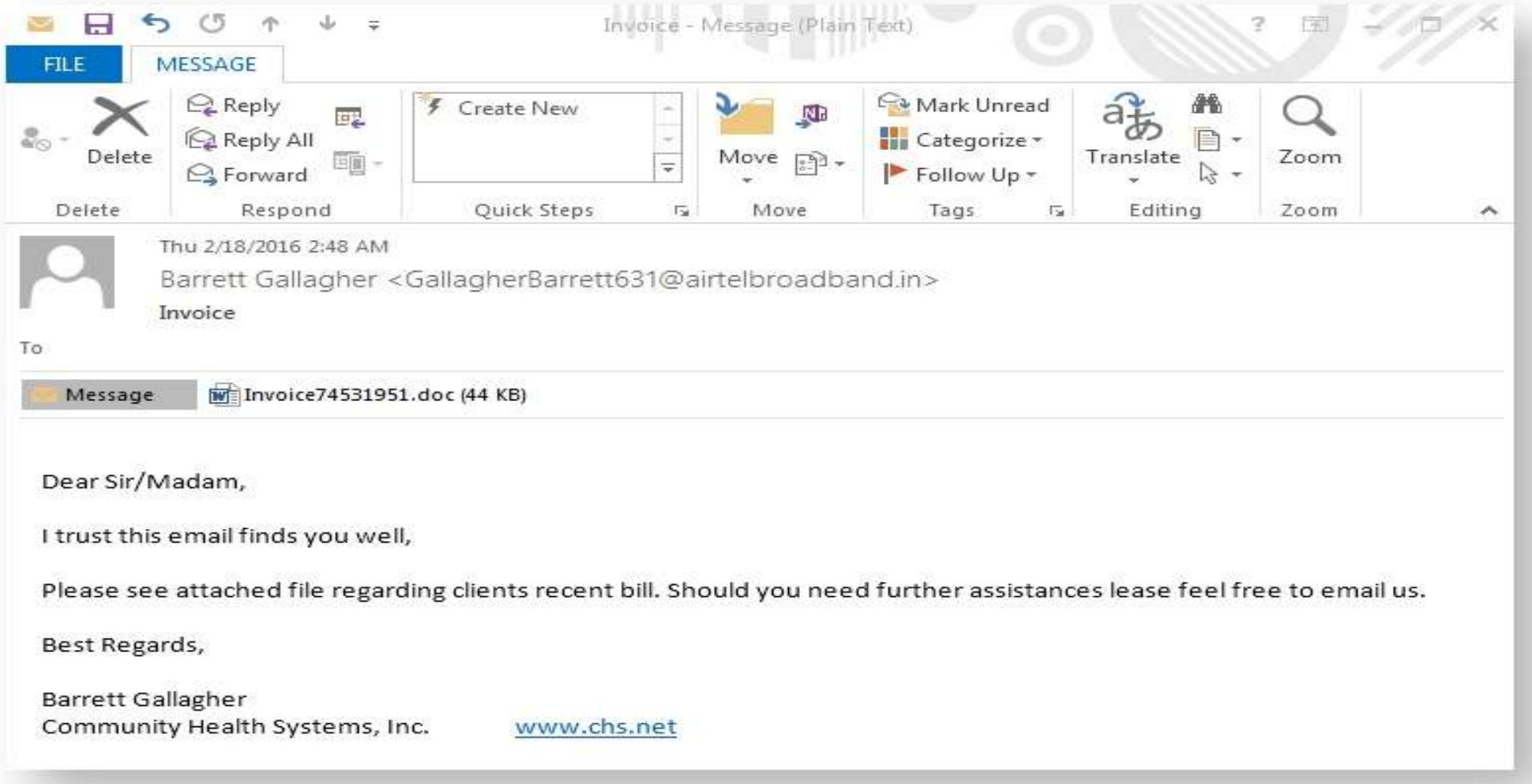
400.000 new samples a day

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

HOW TO GET INFECTED

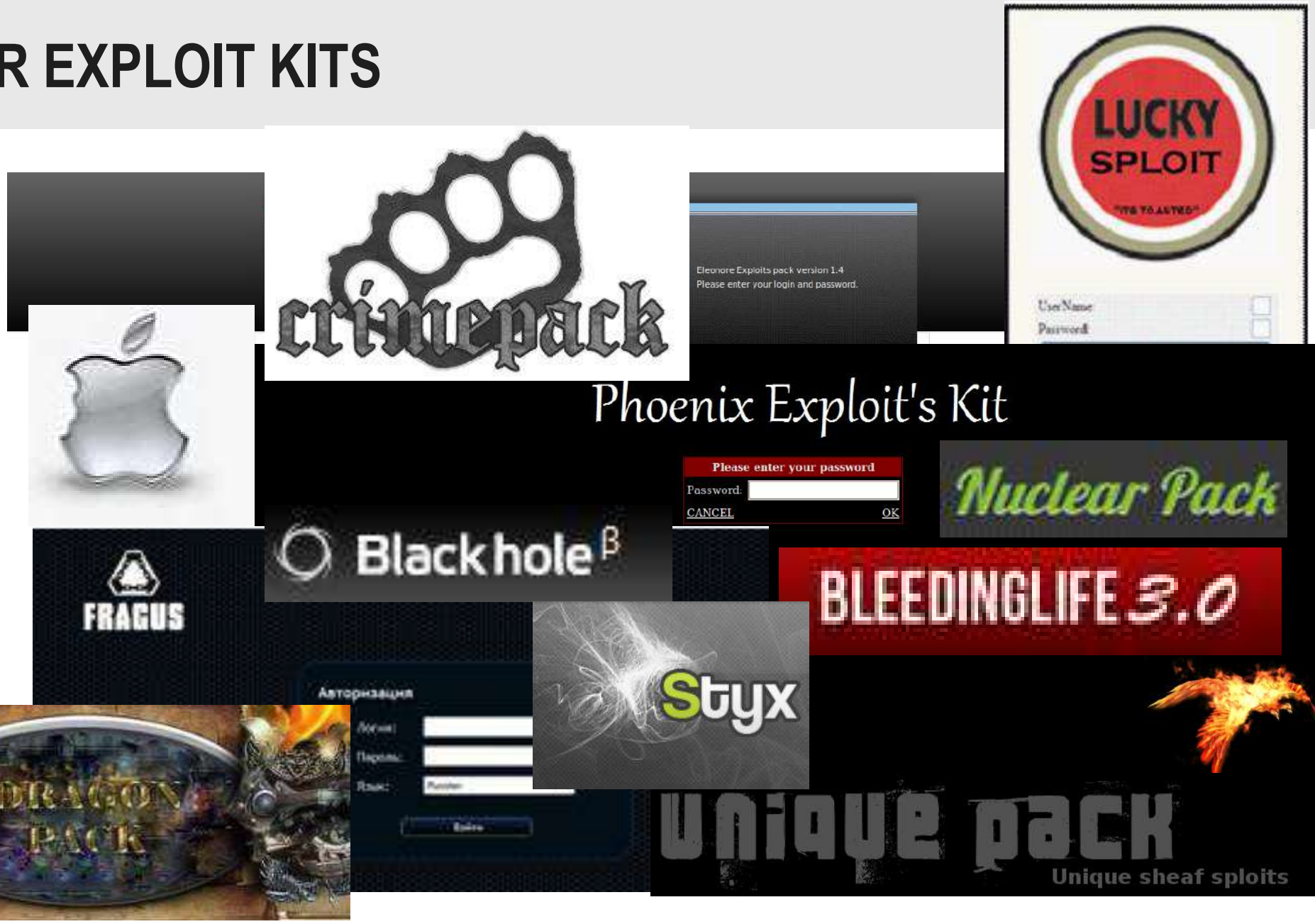
most known modus operandi

SPAMMING MAILS WITH DOCS, ZIP, JAVACRIPT, ETC…



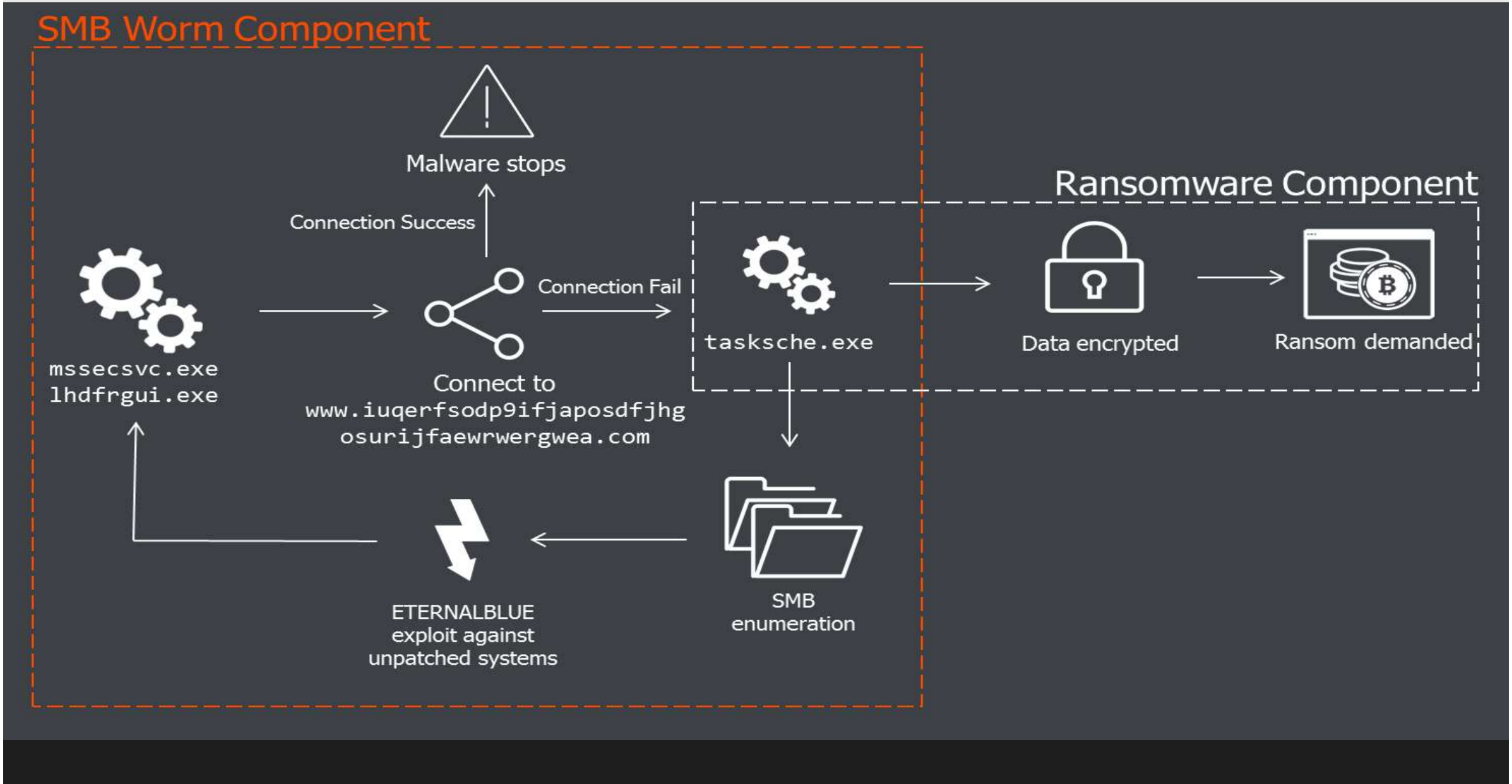
VISITING INFECTED WEBSITES

OTHER EXPLOIT KITS



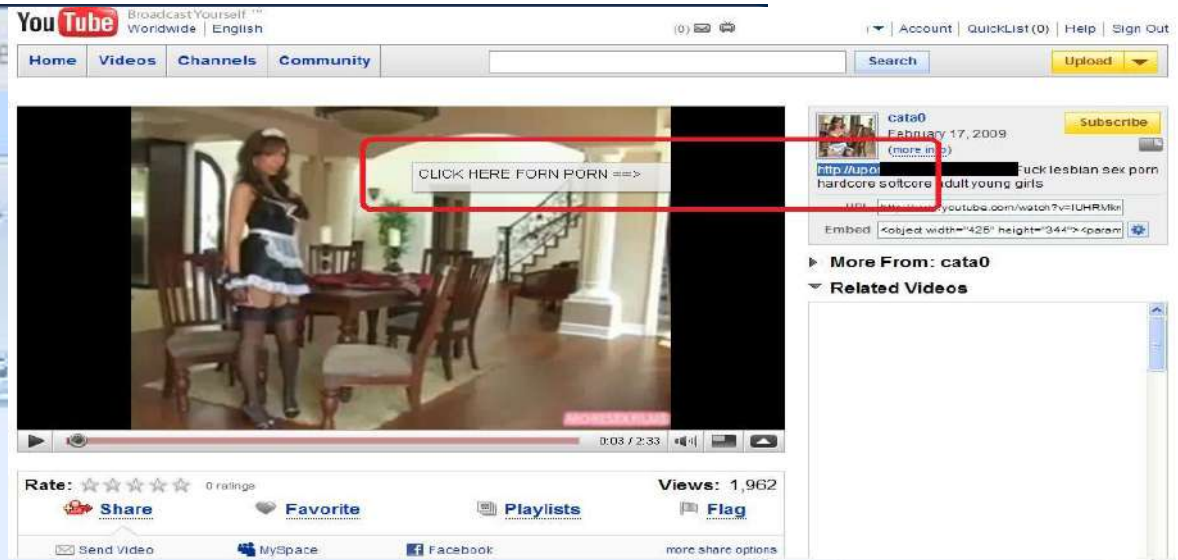
Other:
Malvertising, Downloads, Botnet use
And …

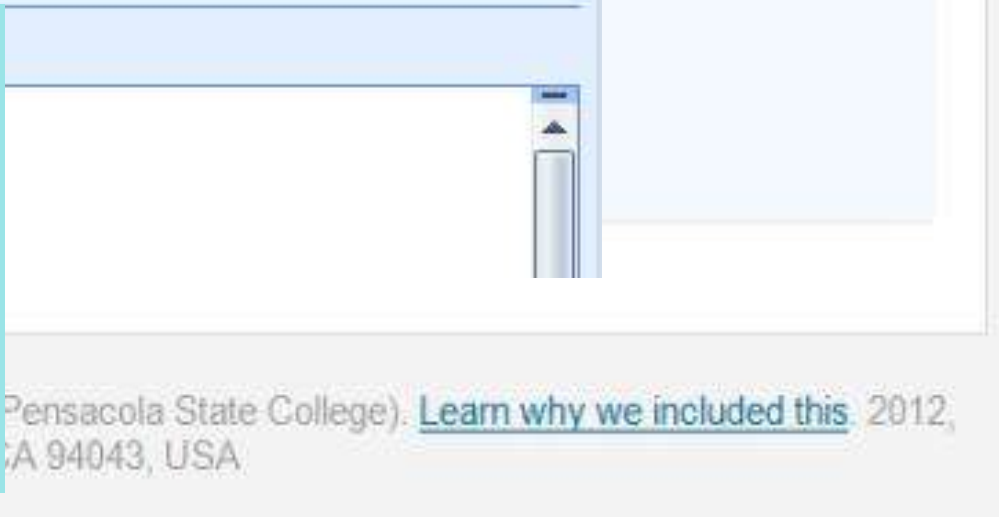
SMB WORM CAPABILITIES



TRIGGER
Why ransomware works?

THE HUMAN FACTOR





have a relaxing
WEEKEND

BIT LAUNDER

TOR URL: **http://yxku52sygpn7oubv.onion/**

TOR Wallet | Bitcoin Tumbler | Emergency Support |

ANONYMIZE BITCOIN

BITCOIN MIXER

... the perfect bitcoin mixing service...

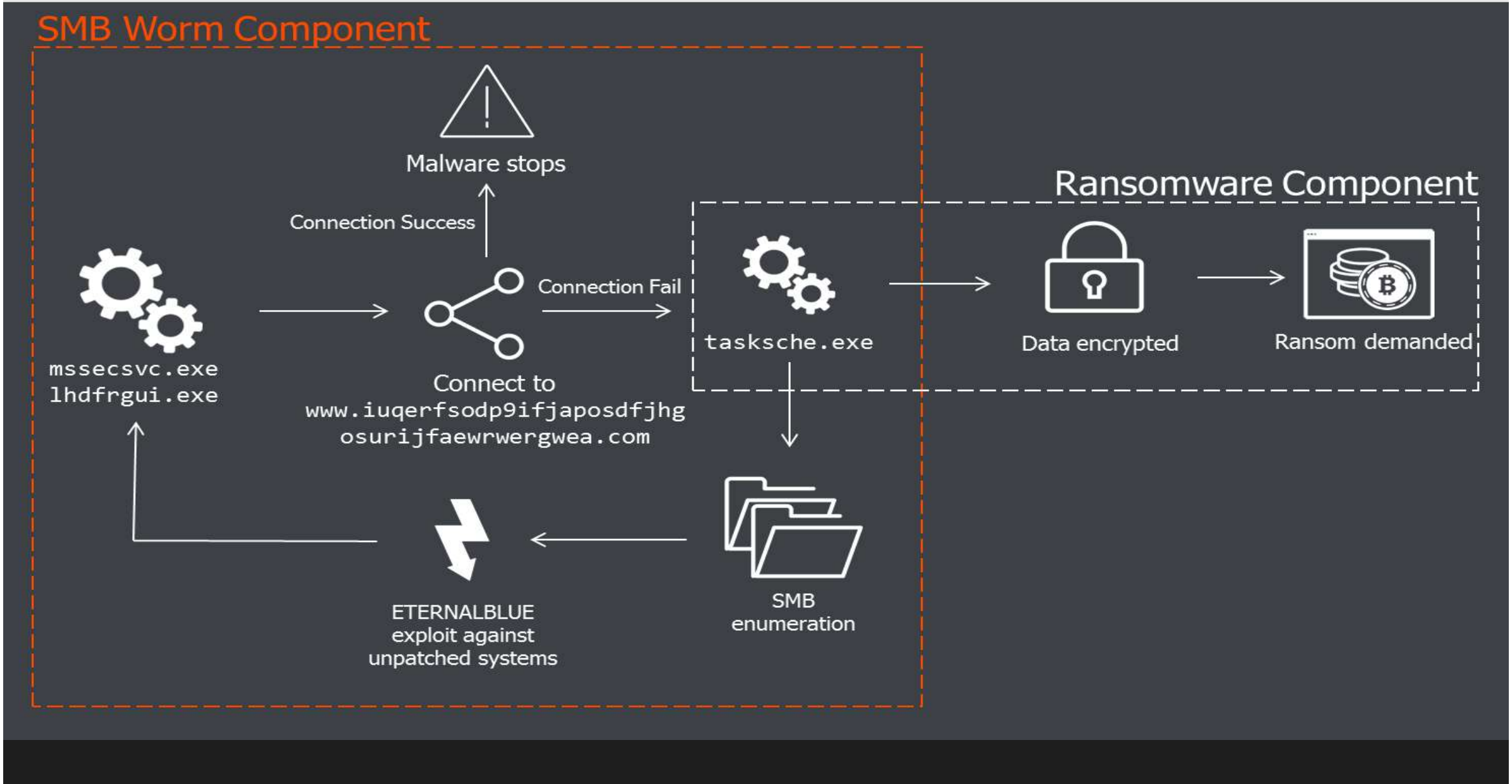
Powerful tools to launder your bitcoins.

Our bitcoin mixing service will fully anonymize bitcoin.

WHY IS RANSOMWARE SO DIFFICULT TO DETECT?

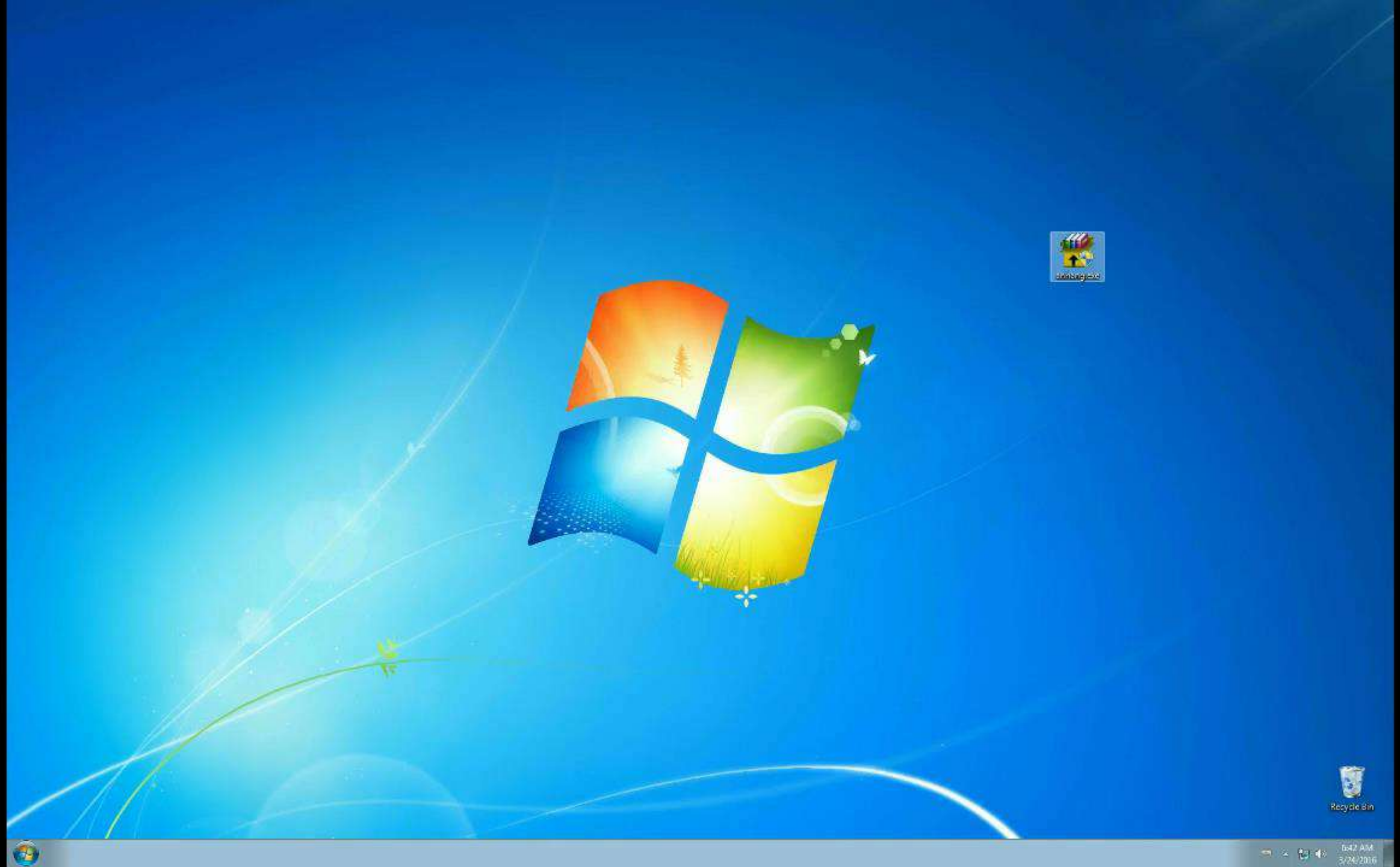
- It features built-in traffic anonymizers, like **TOR** and **Bitcoin**, to avoid tracking by law enforcement agencies and to receive ransom payments
- **Communication** with CC servers is **encrypted** and difficult to detect in network traffic
- It uses **anti-sandboxing mechanisms** so that antivirus 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?



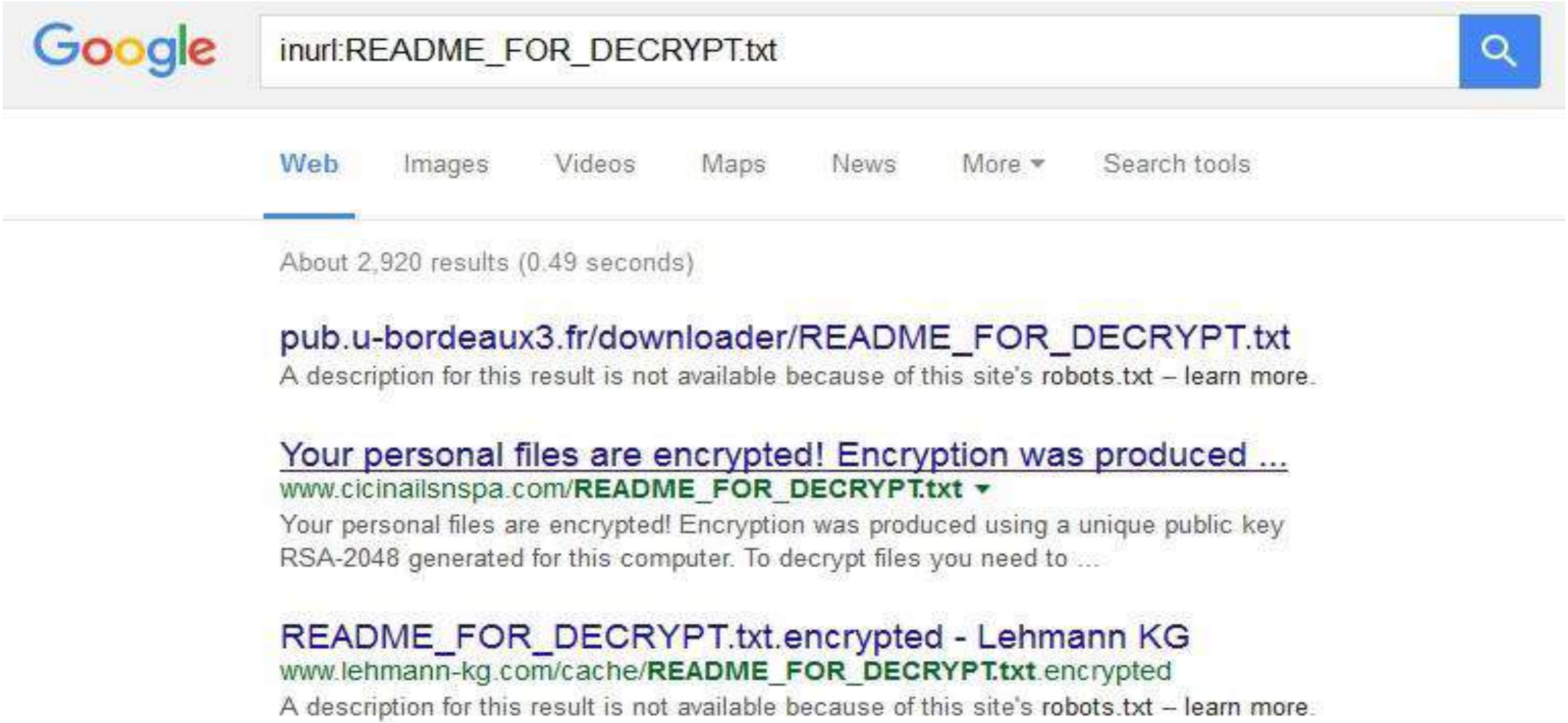
RANSOMWARE EXAMPLES

CRYPTO RANSOMWARE EXAMPLES


Recycle Bin
6:42 AM
3/24/2016

KERANGER RANSOMWARE

LINUX.ENCODER RANSOMWARE (FOR WEBSERVERS)



Logout

SynoLocker™

Automated Decryption Service

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.

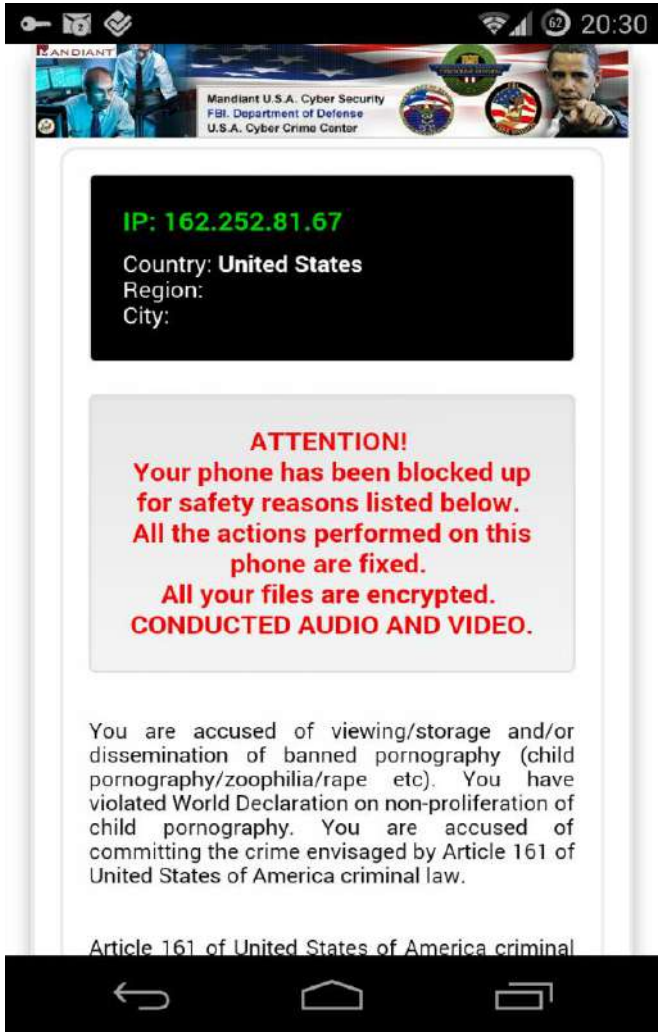
The only accepted payment method is Bitcoin.

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
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
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

I AM
RANSOMWARE
(not really)

NOT PETYA

Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa
If you already purchased your key, please enter it below.
Key: _

REMEDIATION

TO PAY
OR
NOT TO PAY?

REMEDIATION = KNOWN TECHNIQUES

- 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

powered by amazon web services
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL
POLITIE
KASPERSKY lab
Barracuda
GDATA
WWW.NOMORERANSOM.ORG

SC Awards Winner EDITOR'S CHOICE AWARD

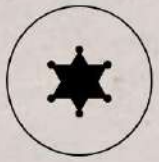
For more information on prevention advice for WannaCry, please click **here.**

NEED HELP unlocking your digital life without paying your attackers*?

YES

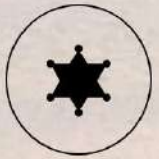
NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!



GOOD NEWS

BAD NEWS



GOOD NEWS

G DATA

THANK YOU!

TWITTER: @EDDYWILLEMS

A secure solution for mobile threats …