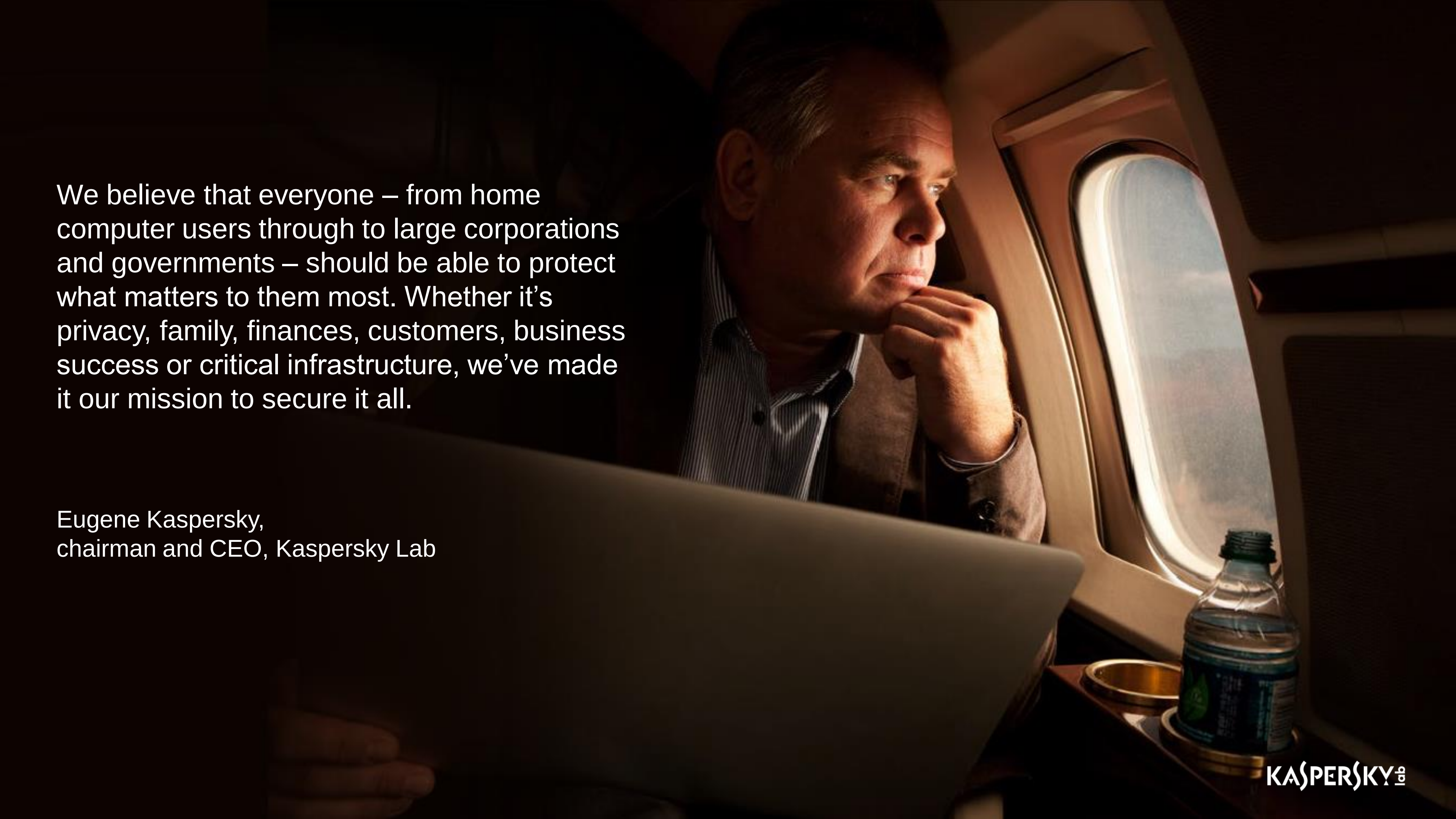
RANSOMWARE IN ANZ

Noushin Shabab

Senior Security Researcher at Global Research and Analysis Team ANZ

KASPERSKY lab



We believe that everyone – from home computer users through to large corporations and governments – should be able to protect what matters to them most. Whether it’s privacy, family, finances, customers, business success or critical infrastructure, we’ve made it our mission to secure it all.

Eugene Kaspersky,
chairman and CEO, Kaspersky Lab

EXPERTISE

1/3 of our employees are R&D specialists

325,000 new malicious files detected by Kaspersky Lab every day

40 world-leading security experts – our elite group

Our Global Research and Analysis Team of security experts constantly explore and fight the most advanced cyberthreats.

OUR ROLE IN THE GLOBAL IT SECURITY COMMUNITY

INTERPOL | STRATEGIC PARTNER

We participate in joint operations and cyberthreat investigations with the Global IT security community, international organisations such as INTERPOL and Europol, law enforcement agencies and CERTs worldwide

We hold regular training courses for INTERPOL and Europol officers and the police forces of many countries, e.g. City of London Police

We provide expert speakers at conferences around the globe, e.g. World Economic Forum in Davos

We host the annual Kaspersky Lab Security Analyst Summit which brings together the world’s best IT security experts

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

AGENDA

- What is ransomware?
- History
- Classifications of ransomware
- Propagation and Acceleration
- Ransomware in ANZ
- How to prevent ransomware?
- No more ransom!

WHAT IS RANSOMWARE?

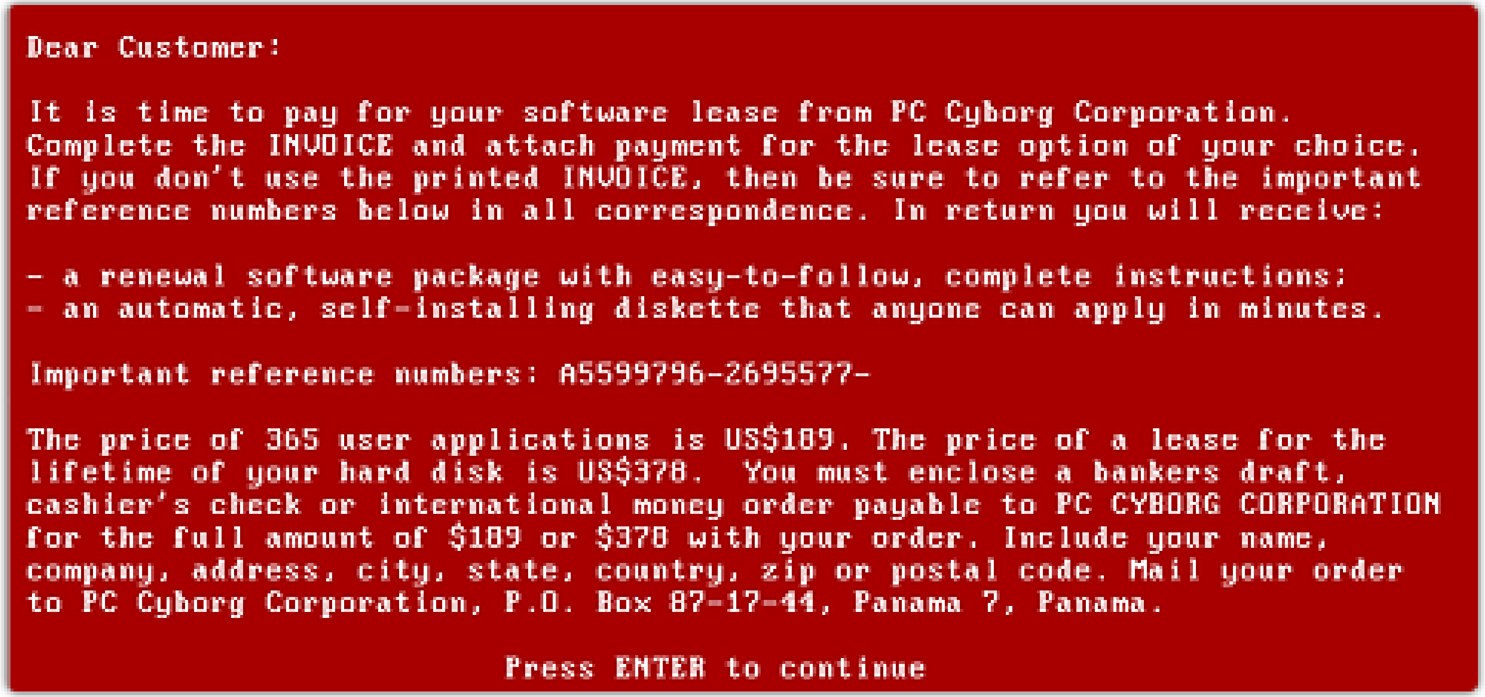
WHAT IS RANSOMWARE?

Ransomware is a type of malware that attempts to extort money from a user by infecting and taking control of the victim's machine or the files or documents stored on it.

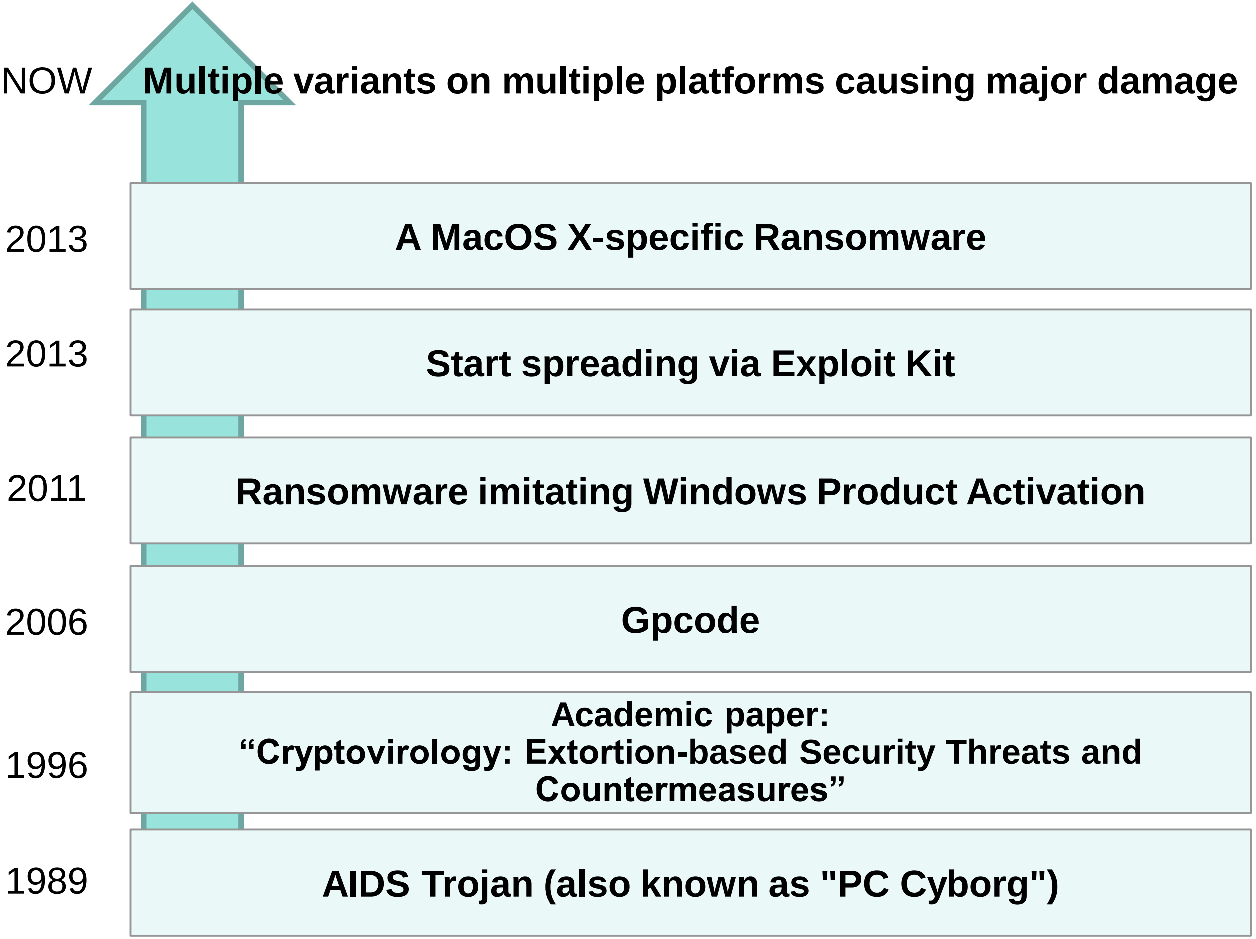
Typically, ransomware will either lock the computer to prevent normal usage or encrypt the documents and files on it to prevent access to saved data

HISTORY OF RANSOMWARE.

FIRST RANSOMWARE



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```



NOW	**Multiple variants on multiple platforms causing major damage**
2013	**A MacOS X-specific Ransomware**
2013	**Start spreading via Exploit Kit**
2011	**Ransomware imitating Windows Product Activation**
2006	**Gpcode**
1996	**Academic paper: “Cryptovirology: Extortion-based Security Threats and Countermeasures”**
1989	**AIDS Trojan (also known as "PC Cyborg")**

TYPES OF RANSOMWARE

- ➢ Screen Locker

- ➢ Mobile device Ransomware(Android)

- ➢ Ransomware encrypting web servers

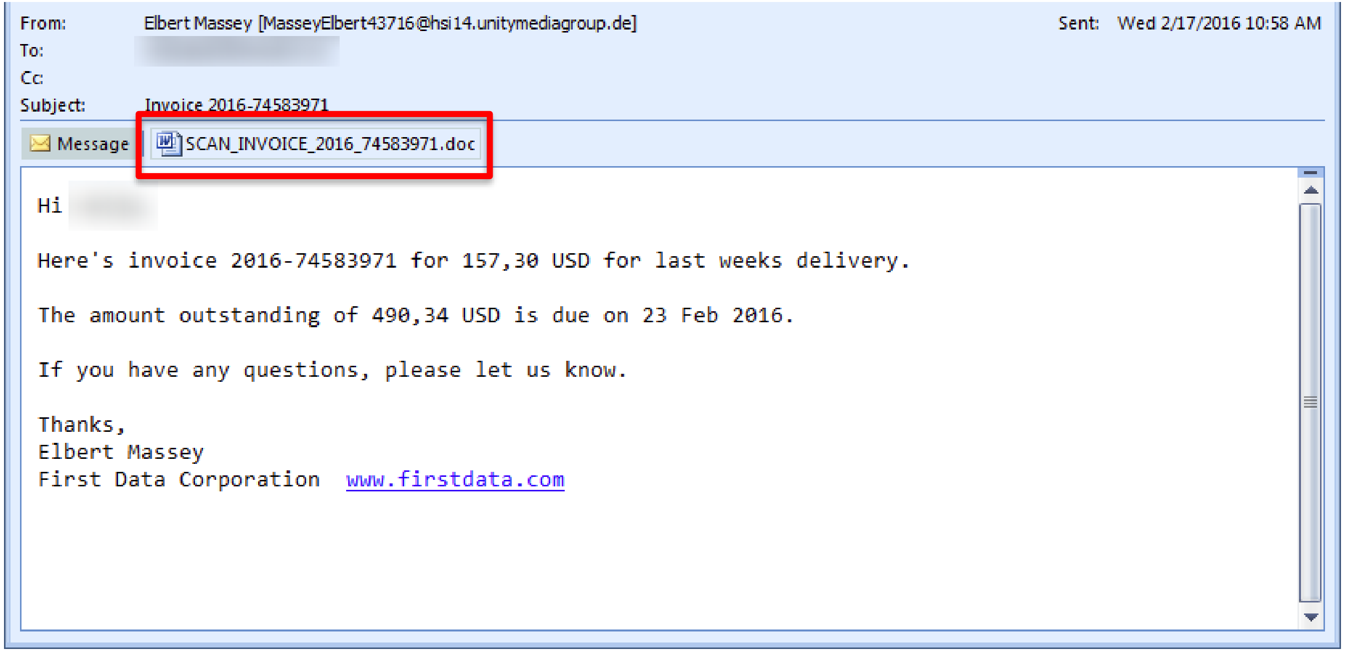
- ➢ Encryption Ransomware

PROPERGATION AND ACCELERATION

PROPERGATION METHODS

- Infected websites
- Malvertising
- Emails
- Instant Message
- Social Networks

EMAIL WITH MS OFFICE DOCUMENT ATTACHMENT



From: Elbert Massey [MasseyElbert43716@hsi14.unitymediagroup.de]

Sent: Wed 2/17/2016 10:58 AM

To: [redacted]

Cc:

Subject: Invoice 2016-74583971

Hi [redacted]

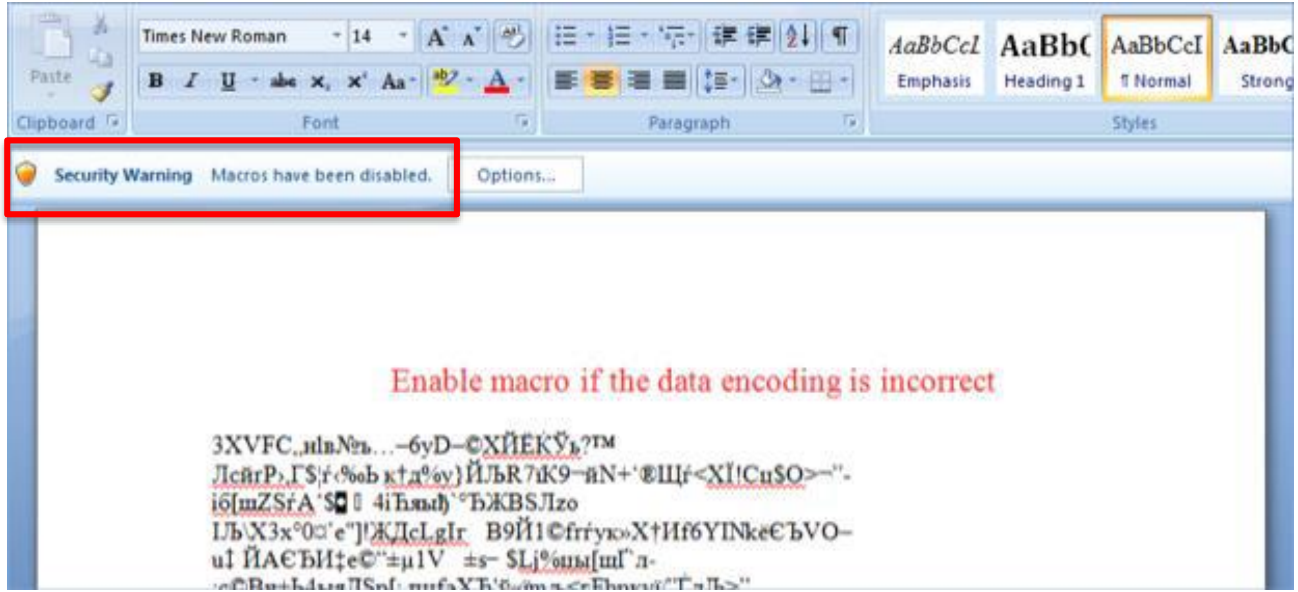
Here's invoice 2016-74583971 for 157,30 USD for last weeks delivery.

The amount outstanding of 490,34 USD is due on 23 Feb 2016.

If you have any questions, please let us know.

Thanks,
Elbert Massey
First Data Corporation www.firstdata.com

TRICKS TO MAKE USERS ENABLE DOCUMENT MACROS

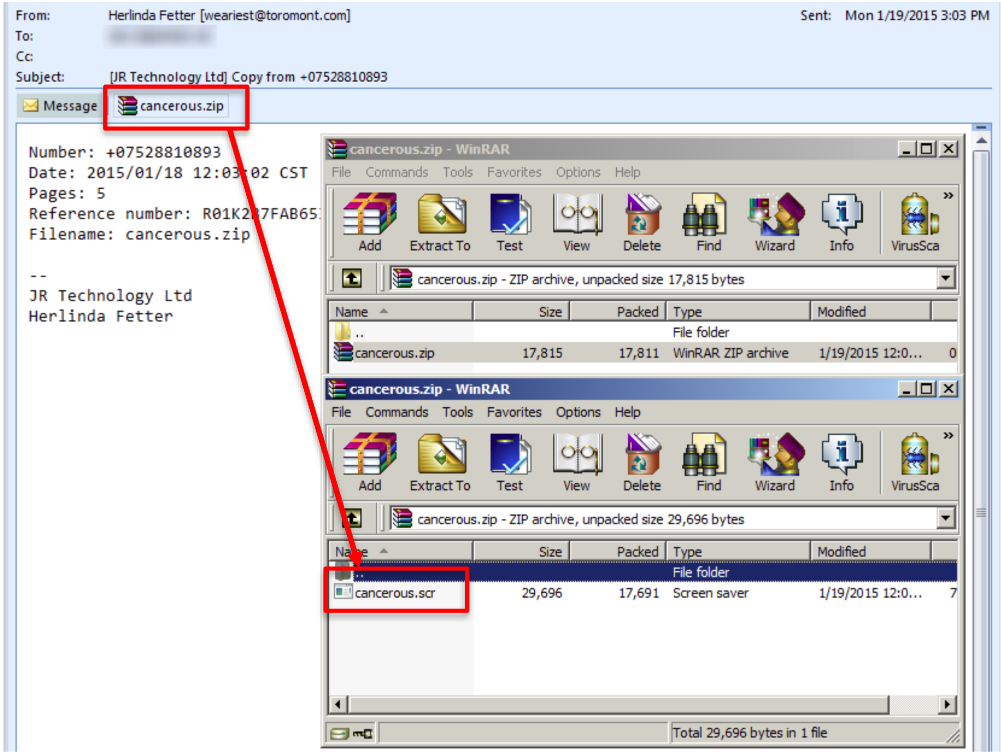


Security Warning Macros have been disabled.

Enable macro if the data encoding is incorrect

```
3XVFC„нlвN℗ъ…–6yD–©XЙЁКЎъ?™
ЛсйrР›‚Г$¦ѓ‹%ъЬ к†д°⁄у}ЙЉЬR7іК9¬йN+'®Щѓ<XЇ!Cu$O>¬"-
і6[шZSѓA`$◘ ▯ 4iЋяыђ`°ЂЖBSЛzo
1Љ\X3x°0¤'e"]!ЖДсLgIr  B9Й1©frѓук»X†Иf6YINkeЄЪVO–
u‡ ЙАЄЪИ‡e©"±µ1V  ±s– $Lj%шы[шГл-
```

EMAIL WITH ARCHIVED EXECUTABLE



From: Herlinda Fetter [weariest@toromont.com] Sent: Mon 1/19/2015 3:03 PM
To: [redacted]
Cc:
Subject: [JR Technology Ltd] Copy from +07528810893

Message | cancerous.zip

```
Number: +07528810893
Date: 2015/01/18 12:03:02 CST
Pages: 5
Reference number: R01K2B7FAB65
Filename: cancerous.zip

--
JR Technology Ltd
Herlinda Fetter
```

cancerous.zip - WinRAR

File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusSca

cancerous.zip - ZIP archive, unpacked size 17,815 bytes

Name	Size	Packed	Type	Modified
..			File folder	
cancerous.zip	17,815	17,811	WinRAR ZIP archive	1/19/2015 12:0...

cancerous.zip - WinRAR

File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusSca

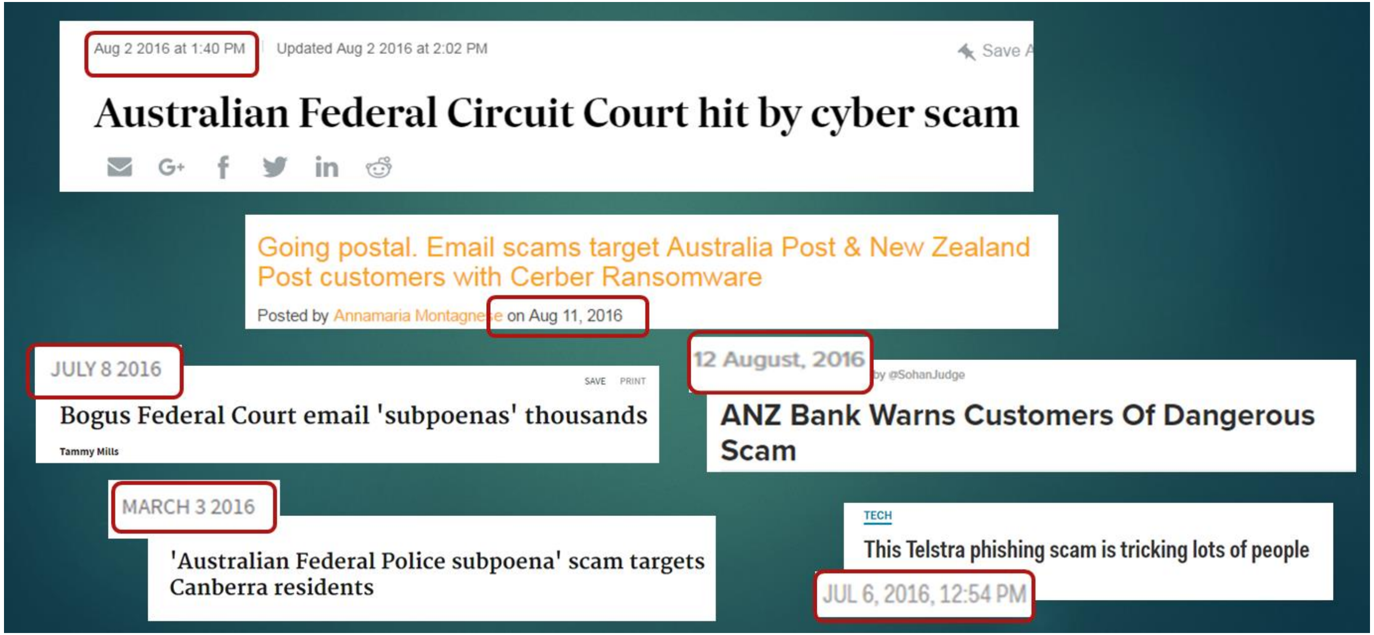
cancerous.zip - ZIP archive, unpacked size 29,696 bytes

Name	Size	Packed	Type	Modified
..			File folder	
cancerous.scr	29,696	17,691	Screen saver	1/19/2015 12:0...

Total 29,696 bytes in 1 file

EXAMPLES IN AUSTRALIA AND NEW ZEALAND

SCAM EMAIL HEADLINES IN AUSTRALIA



Aug 2 2016 at 1:40 PM | Updated Aug 2 2016 at 2:02 PM

Australian Federal Circuit Court hit by cyber scam

Going postal. Email scams target Australia Post & New Zealand Post customers with Cerber Ransomware

Posted by Annamaria Montagnese on Aug 11, 2016

JULY 8 2016

Bogus Federal Court email 'subpoenas' thousands

Tammy Mills

12 August, 2016

by @SohanJudge

ANZ Bank Warns Customers Of Dangerous Scam

MARCH 3 2016

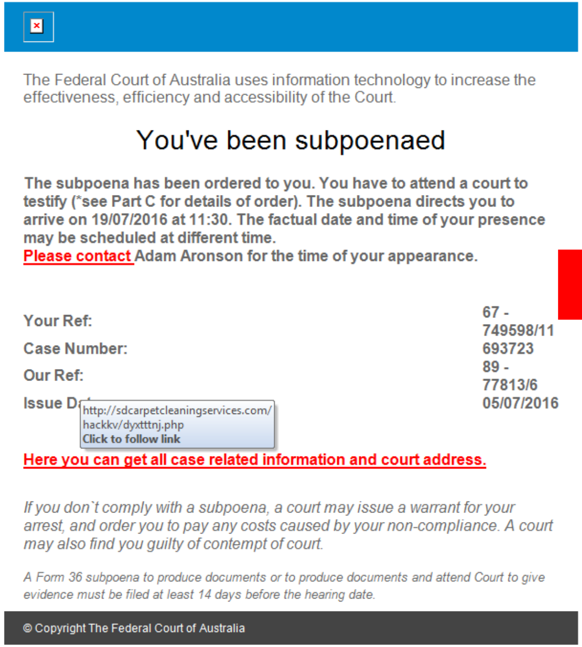
'Australian Federal Police subpoena' scam targets Canberra residents

TECH

This Telstra phishing scam is tricking lots of people

JUL 6, 2016, 12:54 PM

SCAM EMAILS ON THE FEDERAL COURT



The Federal Court of Australia uses information technology to increase the effectiveness, efficiency and accessibility of the Court.

You've been subpoenaed

The subpoena has been ordered to you. You have to attend a court to testify (*see Part C for details of order). The subpoena directs you to arrive on 19/07/2016 at 11:30. The factual date and time of your presence may be scheduled at different time.
Please contact Adam Aronson for the time of your appearance.

Your Ref:	**67 - 749598/11**
Case Number:	**693723**
Our Ref:	**89 - 77813/6**
Issue D	**05/07/2016**

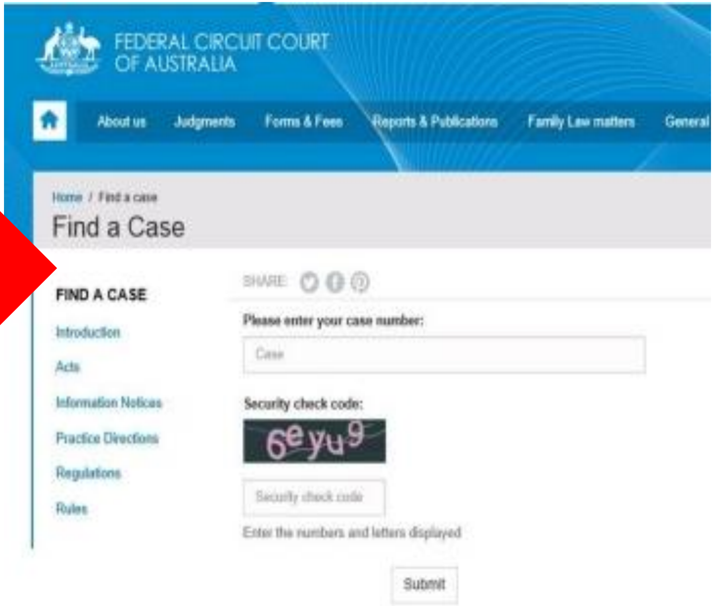
http://sdcarpetcleaningservices.com/hackkv/dyxtttnj.php
Click to follow link

Here you can get all case related information and court address.

If you don`t comply with a subpoena, a court may issue a warrant for your arrest, and order you to pay any costs caused by your non-compliance. A court may also find you guilty of contempt of court.

A Form 36 subpoena to produce documents or to produce documents and attend Court to give evidence must be filed at least 14 days before the hearing date.

© Copyright The Federal Court of Australia



Find a Case

Please enter your case number:

Case

Security check code:

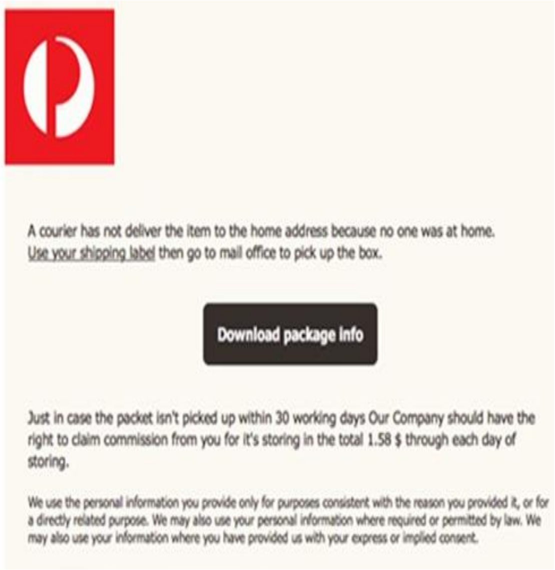
6eyu9

Security check code

Enter the numbers and letters displayed

Submit

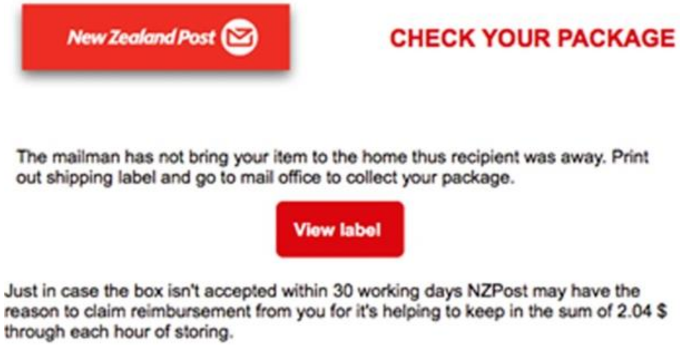
SCAM EMAILS ON THE ANZ POST



A courier has not deliver the item to the home address because no one was at home.
Use your shipping label then go to mail office to pick up the box.

Just in case the packet isn't picked up within 30 working days Our Company should have the right to claim commission from you for it's storing in the total 1.58 $ through each day of storing.

We use the personal information you provide only for purposes consistent with the reason you provided it, or for a directly related purpose. We may also use your personal information where required or permitted by law. We may also use your information where you have provided us with your express or implied consent.

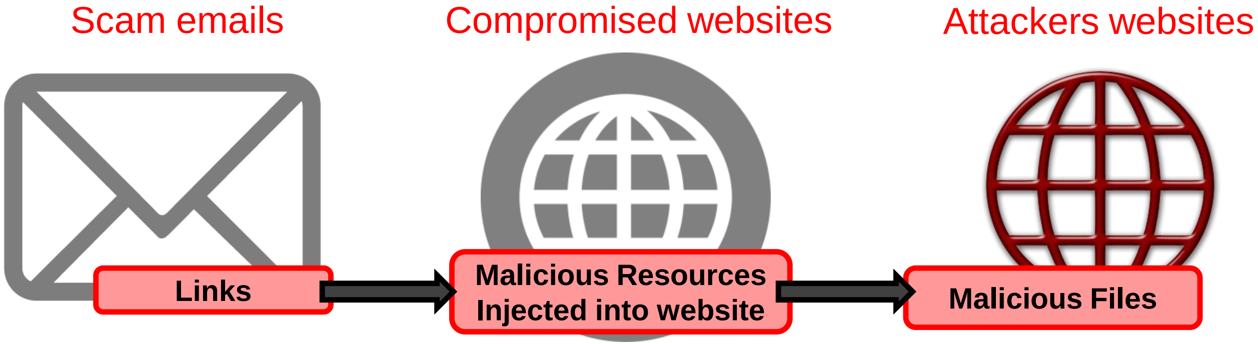


CHECK YOUR PACKAGE

The mailman has not bring your item to the home thus recipient was away. Print out shipping label and go to mail office to collect your package.

Just in case the box isn't accepted within 30 working days NZPost may have the reason to claim reimbursement from you for it's helping to keep in the sum of 2.04 $ through each hour of storing.

INFECTION VECTOR



Scam emails

Compromised websites

Attackers websites

Links

Malicious Resources Injected into website

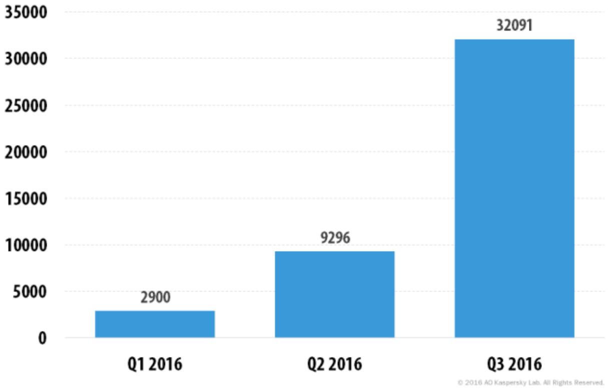
Malicious Files

STATISTICS ON RANSOMWARE

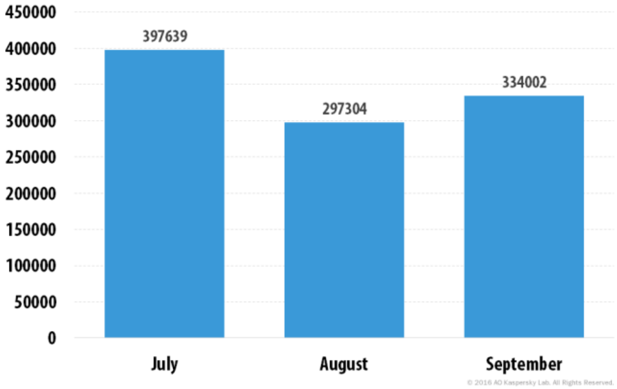
RANSOMWARE IN Q3

- The overall number of cryptor modifications in our malware collection to-date is at least 26,000. 21 new cryptor families and 32.091 new modifications were detected in Q3 2016.

- In Q3 2016, **821,865** unique users were attacked by cryptors – **2.6** times more than in the previous quarter.

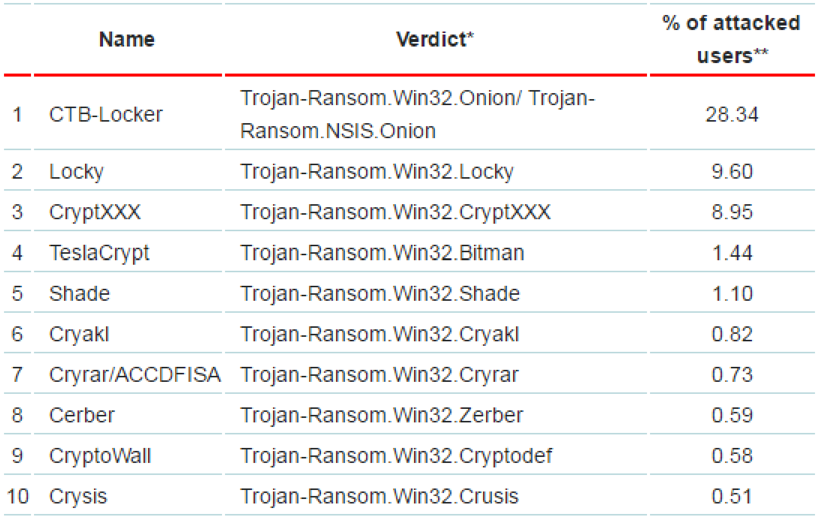


Number of new cryptor samples in our collection



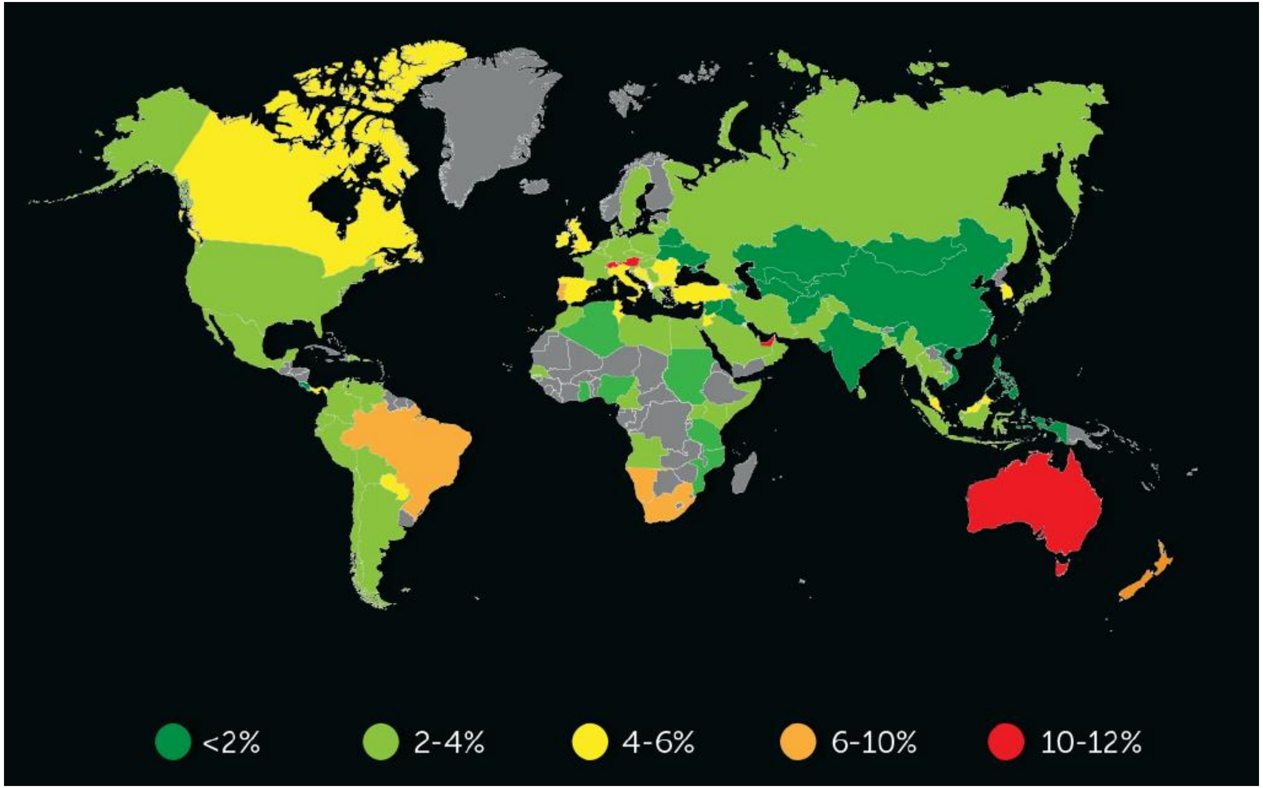
Number of users attacked by ransomware

TOP 10 CRYPTORS Q3



	Name	Verdict*	% of attacked users**
1	CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	28.34
2	Locky	Trojan-Ransom.Win32.Locky	9.60
3	CryptXXX	Trojan-Ransom.Win32.CryptXXX	8.95
4	TeslaCrypt	Trojan-Ransom.Win32.Bitman	1.44
5	Shade	Trojan-Ransom.Win32.Shade	1.10
6	Cryakl	Trojan-Ransom.Win32.Cryakl	0.82
7	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0.73
8	Cerber	Trojan-Ransom.Win32.Zerber	0.59
9	CryptoWall	Trojan-Ransom.Win32.Cryptodef	0.58
10	Crysis	Trojan-Ransom.Win32.Crusis	0.51

MAP OF AUSTRALIA AND NEW ZEALAND

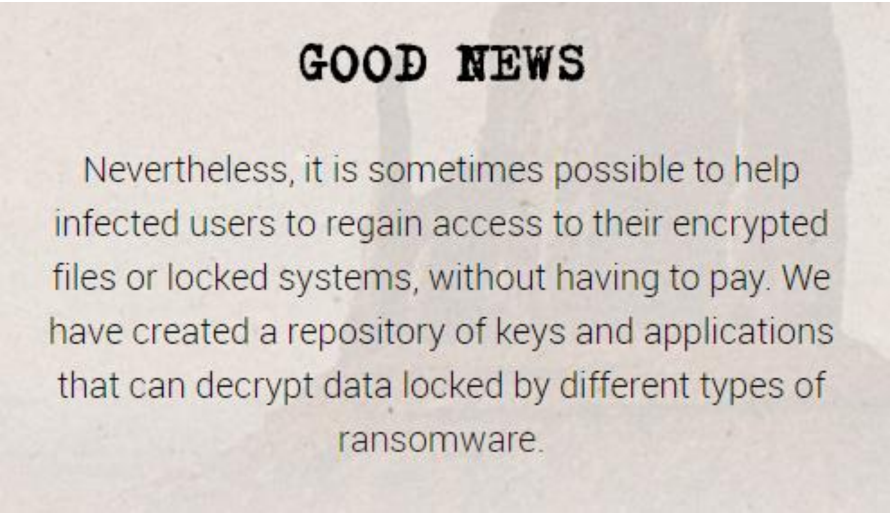


HOW TO PREVENT RANSOMWARE?

- Always Make Backups
- Keep all software updated
- Improve User Awareness
- Use Reliable Antivirus solution
- DON’T PAY THE RANSOM!

NO MORE RANSOM

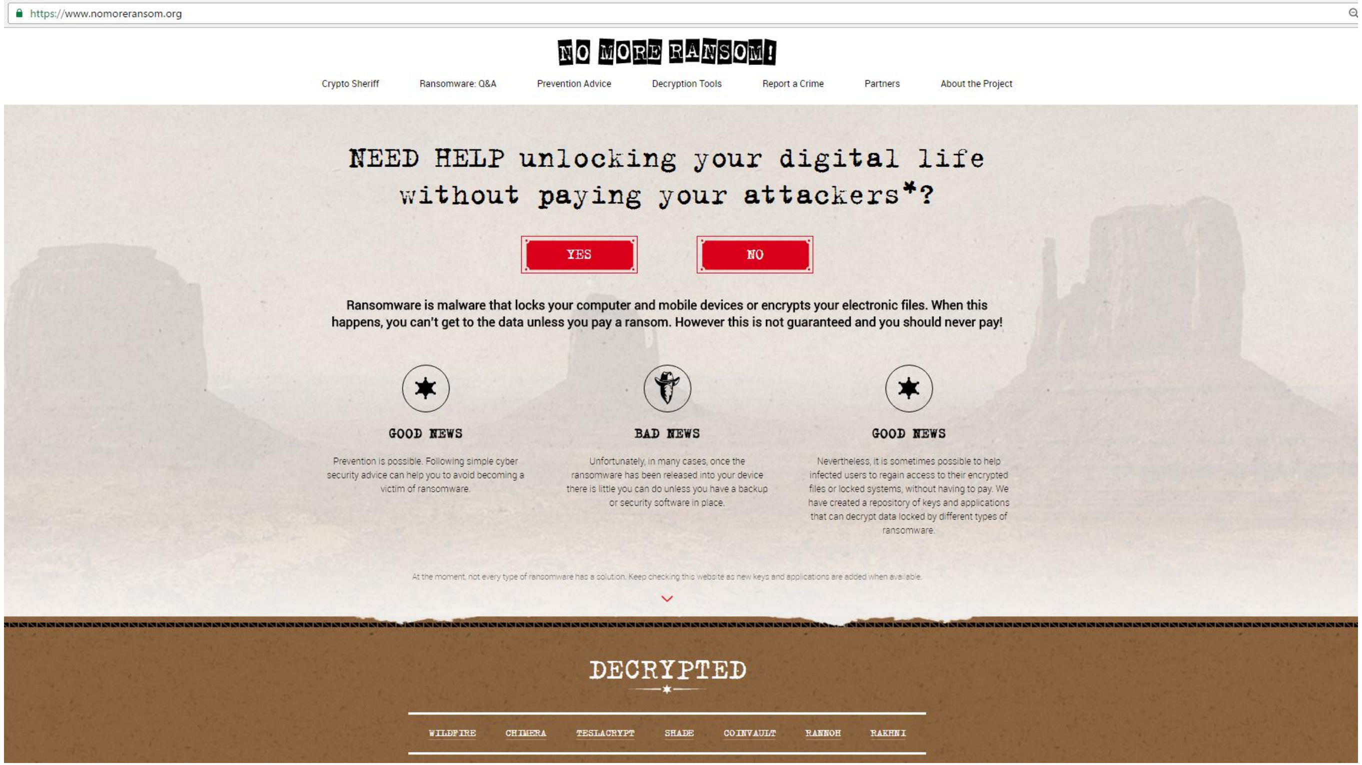
NO MORE RANSOM



GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

NO MORE RANSOM MOVEMENT



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

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

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

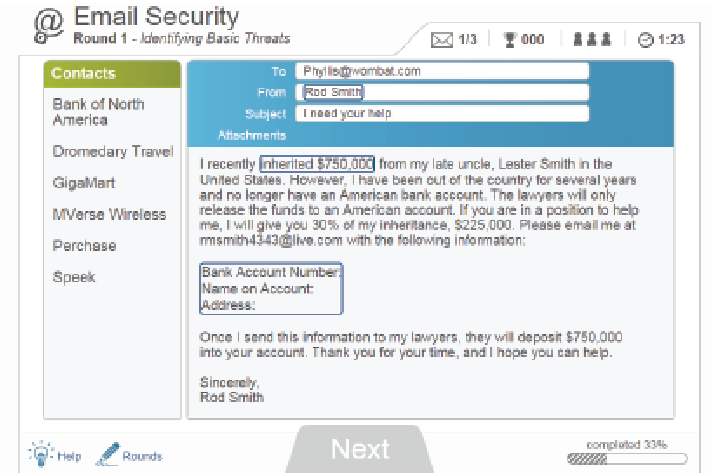
At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

DECRYPTED

HOW CAN WE HELP?

KASPERSKY’S CYBER SECURITY TRAINING

- Work through typical scenarios and situations
- Gain greater knowledge and understanding of potential threats and how to deal with them
- Skills Assessment
- Measurable education plan



To: Phyllis@wombat.com
From: Rod Smith
Subject: I need your help
Attachments

I recently inherited $750,000 from my late uncle, Lester Smith in the United States. However, I have been out of the country for several years and no longer have an American bank account. The lawyers will only release the funds to an American account. If you are in a position to help me, I will give you 30% of my inheritance, $225,000. Please email me at rmsmith4343@live.com with the following information:

Bank Account Number:
Name on Account:
Address:

Once I send this information to my lawyers, they will deposit $750,000 into your account. Thank you for your time, and I hope you can help.

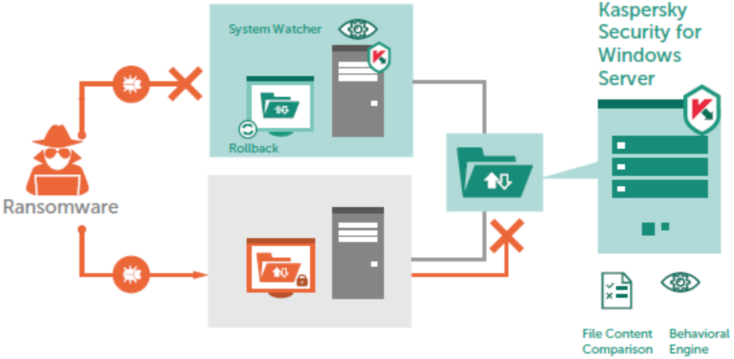
Sincerely,
Rod Smith

On Line Learning Modules:

- ✓ Anti-Phishing
- ✓ Data Protection
- ✓ Safe Social Networks
- ✓ Physical Security
- ✓ Smartphone Security
- ✓ Safer Web Browsing
- ✓ Security beyond the Office
- ✓ Social Engineering
- ✓ URL Training
- ✓ Email Security
- ✓ Passwords

KASPERSKY'S SYSTEM WATCHER

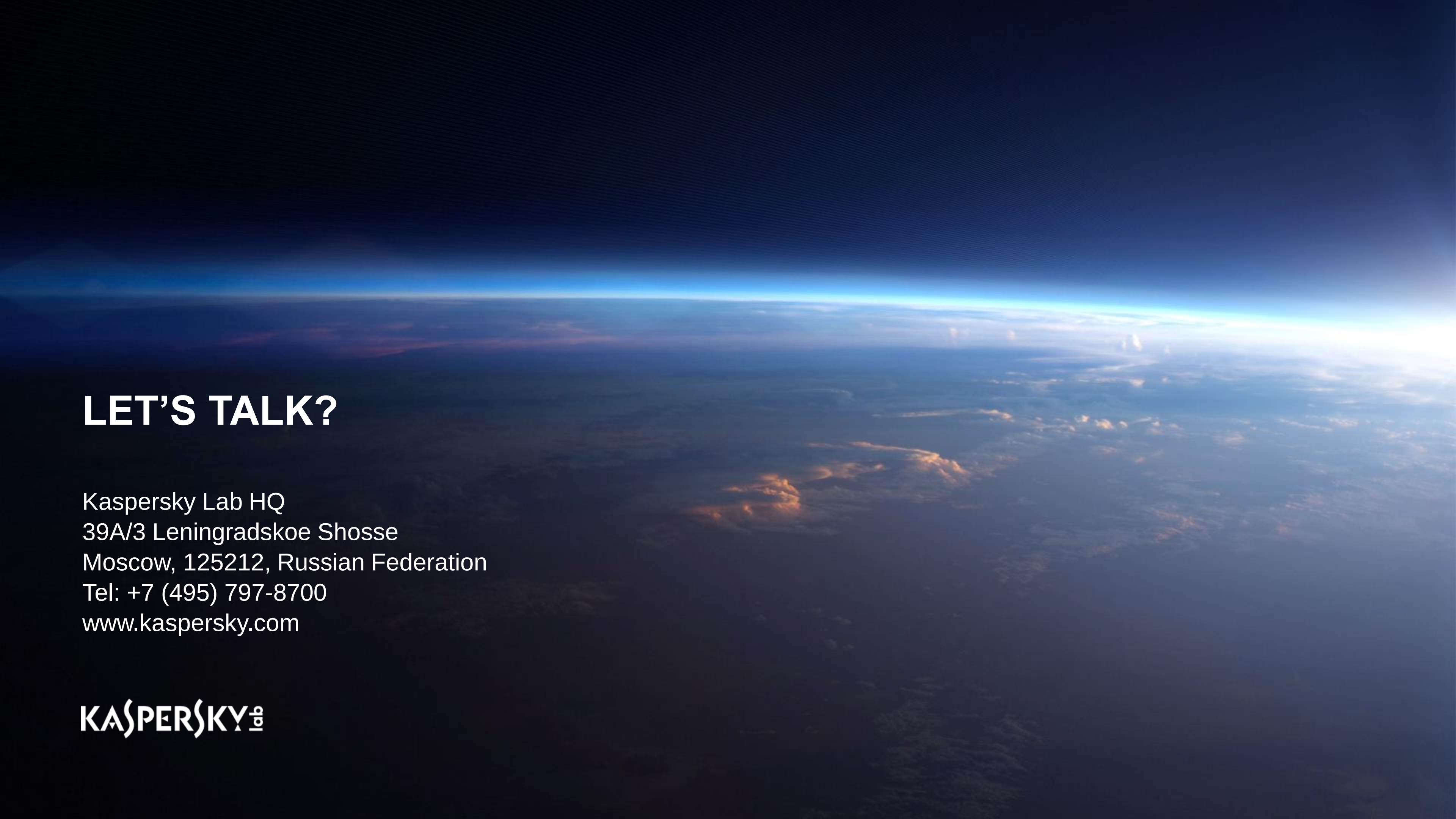
- If suspicious application attempts to open users personal files, it makes a local protected back up copy
- If is found to be crypto-malware, automatically rolls back unsolicited changes to system files.



KASPERSKY'S ANTI CRYPTOR FOR FILE SERVER

- Detects encryption algorithm from endpoint to file server
- Severs connection so no further encryption can occur

REMEMBER, DON’T PAY THE RANSOM!



LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab