ISACA®

Trust in, and value from, information systems

Prepare against Ransomware

Prof. Claudio Cilli, Ph.D., CISA, CISM, CRISC, CGEIT
University of Rome, Italy

Cyber Attack

- The Prussian philosopher Karl von Clauswitz observed: "Every age has its own kind of war, its own limiting conditions and its own peculiar preconceptions."
- We live in an age of TECHNOLOGY focused warfare

Al servizio dei professionisti dell'IT Governance

Rome Chapter

How ransomware works

- Recent poll on ransomware

44% of businesses infected

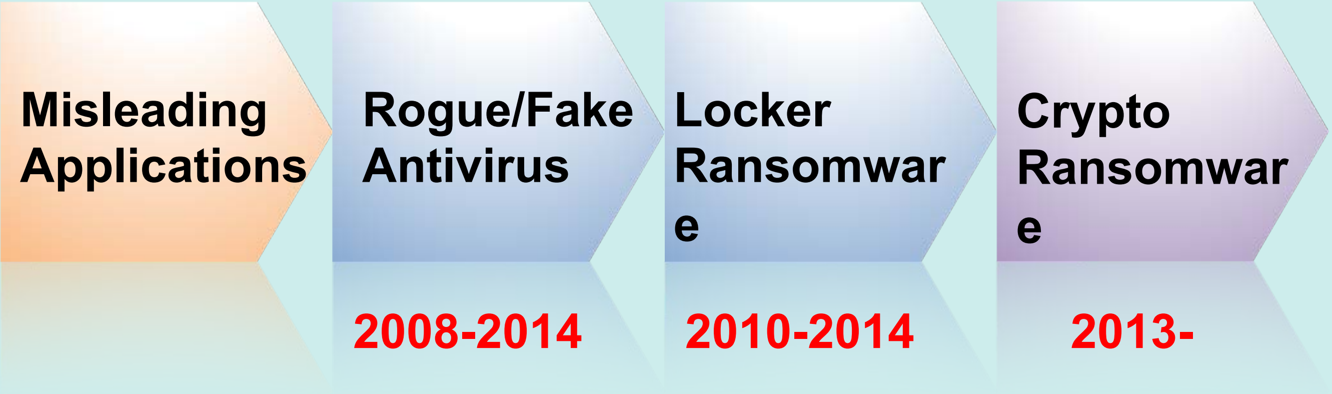
60% had backups

65% paid the ransom

Average ransom sum €540

Loss of business productivity comes on top, exceeding ransom

Ransomware Evolution



Misleading Applications

Rogue/Fake Antivirus

2008-2014

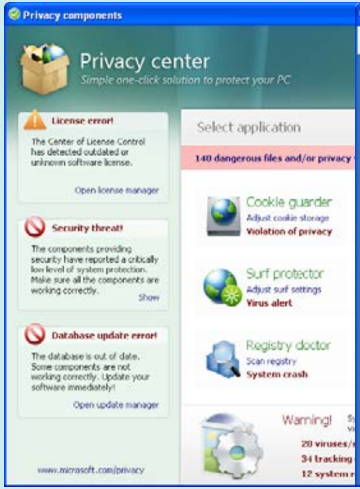
Locker Ransomware

2010-2014

Crypto Ransomware

2013-

Misleading Applications



License error!

The Center of License Control has detected outdated or unknown software license.

Security threat!

The components providing security have reported a critically low level of system protection. Make sure all the components are working correctly.

Database update error!

The database is out of date. Some components are not working correctly. Update your software immediately!

140 dangerous files and/or privacy

Violation of privacy

Virus alert

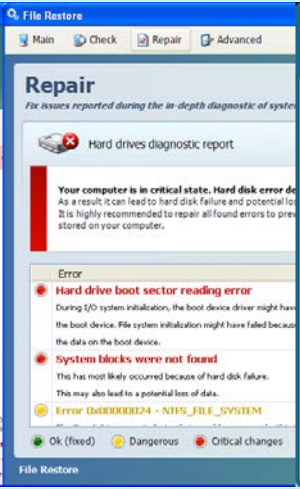
System crash

Warning!

20 viruses/

34 tracking

12 system



Repair

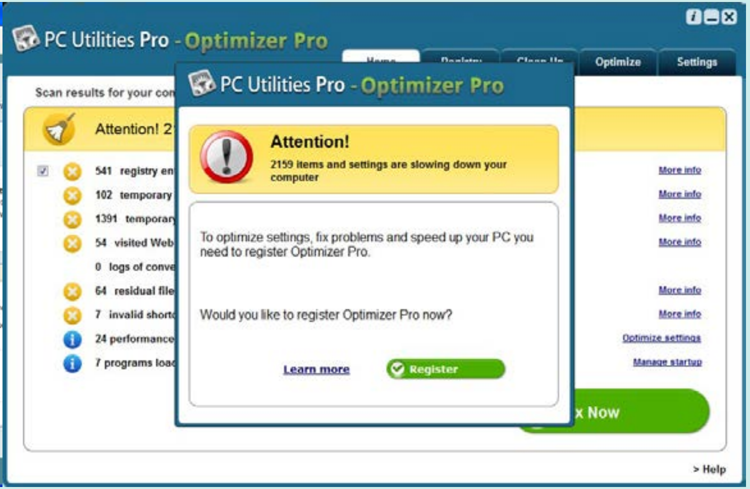
Fix issues reported during the in-depth diagnostic of system

Hard drives diagnostic report

Your computer is in critical state. Hard disk error de
As a result it can lead to hard disk failure and potential los
It is highly recommended to repair all found errors to prev
stored on your computer.

	Error
●	**Hard drive boot sector reading error** During I/O system initialization, the boot device driver might hav the boot device. File system initialization might have failed becaus the data on the boot device.
●	**System blocks were not found** This has most likely occurred because of hard disk failure. This may also lead to a potential loss of data.
●	Error 0x00000024 - NTFS_FILE_SYSTEM

● Ok (fixed) ● Dangerous ● Critical changes



Scan results for your com

Attention! 2

☑ 541 registry en

102 temporary

1391 temporary

54 visited Web

0 logs of conve

64 residual file

7 invalid shortc

24 performance

7 programs load

PC Utilities Pro - Optimizer Pro

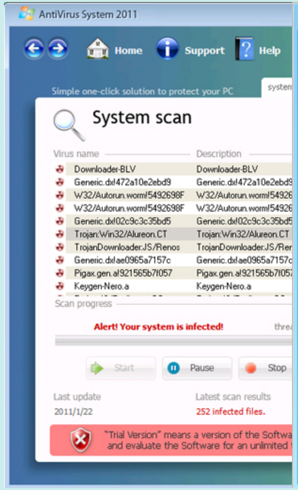
Attention!

2159 items and settings are slowing down your computer

To optimize settings, fix problems and speed up your PC you need to register Optimizer Pro.

Would you like to register Optimizer Pro now?

Rogue/Fake Antivirus



AntiVirus System 2011

Simple one-click solution to protect your PC

System scan

Virus name	Description
Downloader-BLV	Downloader-BLV
Generic.dx!472a10e2ebd9	Generic.dx!472a10e2ebd9
W32/Autorun.worm!5492698F	W32/Autorun.worm!54926
W32/Autorun.worm!5492698F	W32/Autorun.worm!54926
Generic.dx!02c9c3c35bd5	Generic.dx!02c9c3c35bd5
Trojan:Win32/Alureon.CT	Trojan:Win32/Alureon.CT
TrojanDownloader:JS/Renos	TrojanDownloader:JS/Ren
Generic.dx!ae0965a7157c	Generic.dx!ae0965a7157c
Pigax.gen.a!921565b7f057	Pigax.gen.a!921565b7f057
Keygen-Nero.a	Keygen-Nero.a

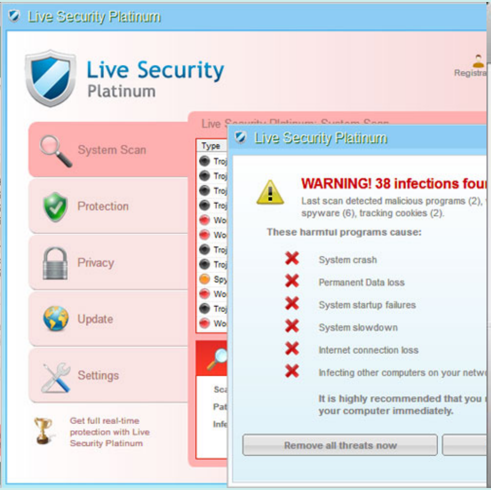
Scan progress

Alert! Your system is infected! threa

Last update: 2011/1/22

Latest scan results: 252 infected files.

"Trial Version" means a version of the Softwa
and evaluate the Software for an unlimited



Live Security Platinum

Live Security Platinum

Get full real-time protection with Live Security Platinum

Live Security Platinum

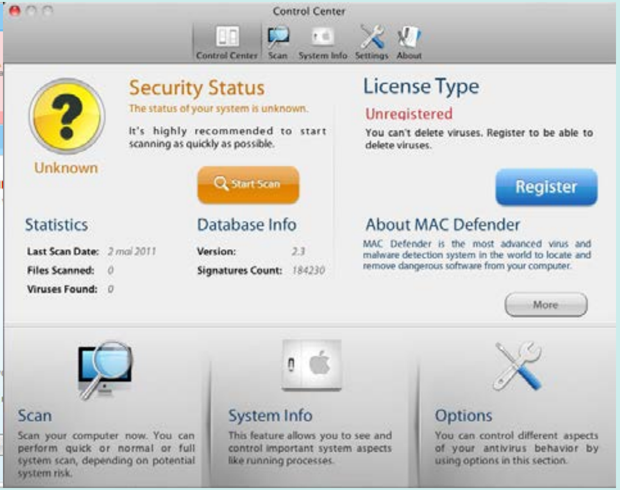
WARNING! 38 infections fou

Last scan detected malicious programs (2),
spyware (6), tracking cookies (2).

These harmful programs cause:

- ✗ System crash
- ✗ Permanent Data loss
- ✗ System startup failures
- ✗ System slowdown
- ✗ Internet connection loss
- ✗ Infecting other computers on your netw

It is highly recommended that you
your computer immediately.



Control Center

Security Status

The status of your system is unknown.

It's highly recommended to start scanning as quickly as possible.

License Type

Unregistered

You can't delete viruses. Register to be able to delete viruses.

Statistics

Last Scan Date: 2 mai 2011
Files Scanned: 0
Viruses Found: 0

Database Info

Version: 2.3
Signatures Count: 184230

About MAC Defender

MAC Defender is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.

Scan

Scan your computer now. You can perform quick or normal or full system scan, depending on potential system risk.

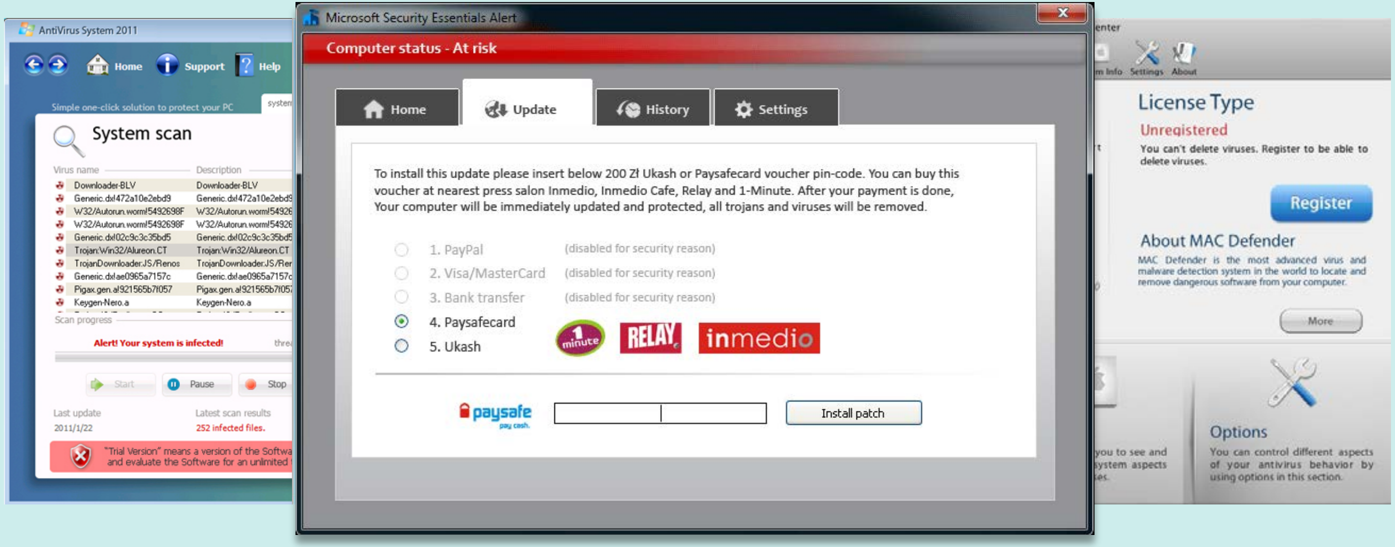
System Info

This feature allows you to see and control important system aspects like running processes.

Options

You can control different aspects of your antivirus behavior by using options in this section.

Rogue/Fake Antivirus



AntiVirus System 2011

Simple one-click solution to protect your PC

System scan

Virus name	Description
Downloader-BLV	Downloader-BLV
Generic.dx!472a10e2ebd9	Generic.dx!472a10e2ebd9
W32/Autorun.worm!5492698F	W32/Autorun.worm!54926
W32/Autorun.worm!5492698F	W32/Autorun.worm!54926
Generic.dx!02c9c3c35bd5	Generic.dx!02c9c3c35bd5
Trojan:Win32/Alureon.CT	Trojan:Win32/Alureon.CT
TrojanDownloader:JS/Renos	TrojanDownloader:JS/Ren
Generic.dx!ae0965a7157c	Generic.dx!ae0965a7157c
Pigax.gen.a!921565b7f057	Pigax.gen.a!921565b7f057
Keygen-Nero.a	Keygen-Nero.a

Scan progress

Alert! Your system is infected!

Last update: 2011/1/22

Latest scan results: 252 infected files.

"Trial Version" means a version of the Softwa
and evaluate the Software for an unlimited

Microsoft Security Essentials Alert

Computer status - At risk

To install this update please insert below 200 Zł Ukash or Paysafecard voucher pin-code. You can buy this voucher at nearest press salon Inmedio, Inmedio Cafe, Relay and 1-Minute. After your payment is done, Your computer will be immediately updated and protected, all trojans and viruses will be removed.

○ 1. PayPal (disabled for security reason)
○ 2. Visa/MasterCard (disabled for security reason)
○ 3. Bank transfer (disabled for security reason)
● 4. Paysafecard
○ 5. Ukash

License Type

Unregistered

You can't delete viruses. Register to be able to delete viruses.

About MAC Defender

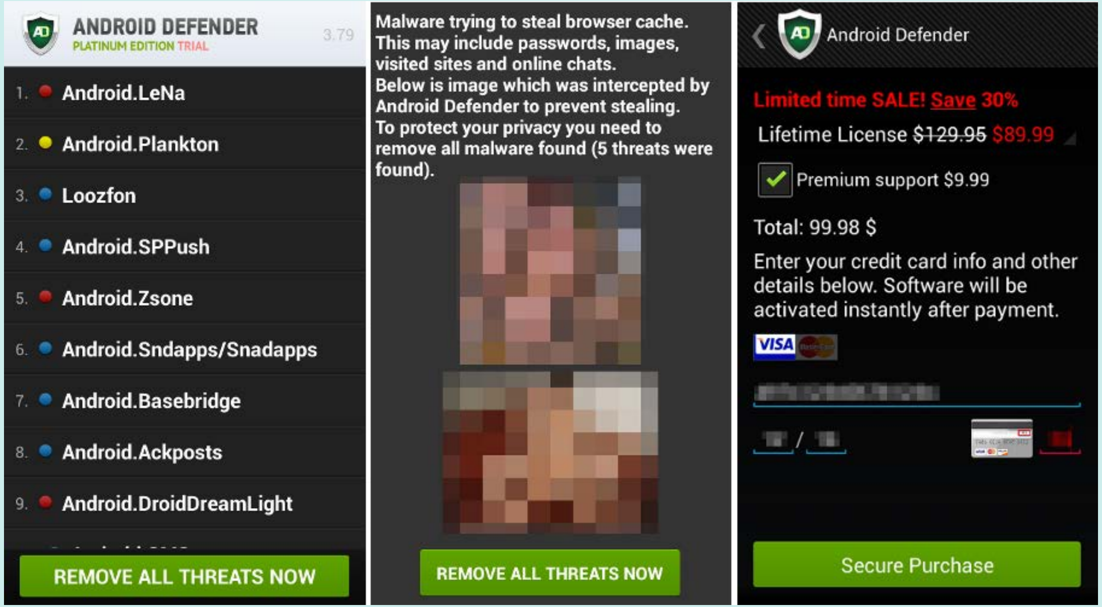
MAC Defender is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.

you to see and
system aspects
ses.

Options

You can control different aspects of your antivirus behavior by using options in this section.

Rogue/Fake Antivirus (Android)



1. Android.LeNa
2. Android.Plankton
3. Loozfon
4. Android.SPPush
5. Android.Zsone
6. Android.Sndapps/Snadapps
7. Android.Basebridge
8. Android.Ackposts
9. Android.DroidDreamLight

Malware trying to steal browser cache. This may include passwords, images, visited sites and online chats.
Below is image which was intercepted by Android Defender to prevent stealing.
To protect your privacy you need to remove all malware found (5 threats were found).

Limited time SALE! Save 30%

Lifetime License ~~$129.95~~ $89.99

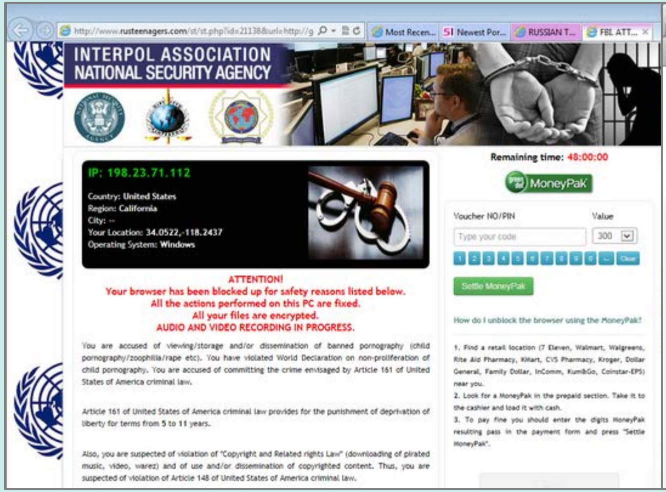
☑ Premium support $9.99

Total: 99.98 $

Enter your credit card info and other details below. Software will be activated instantly after payment.

[redacted]

(Browser) Locker Ransomware



IP: 198.23.71.112

Country: United States
Region: California
City: --
Your Location: 34.0522,-118.2437
Operating System: Windows

ATTENTION!
Your browser has been blocked up for safety reasons listed below.
All the actions performed on this PC are fixed.
All your files are encrypted.
AUDIO AND VIDEO RECORDING IN PROGRESS.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

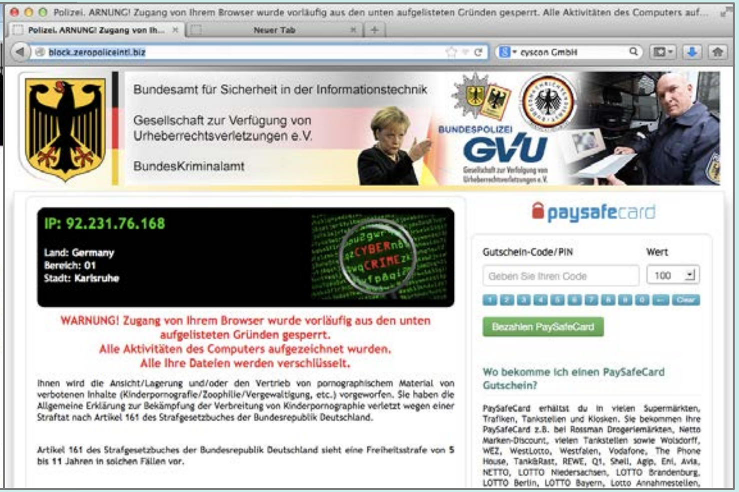
Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, warez) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 148 of United States of America criminal law.

Remaining time: 48:00:00

Voucher NO/PIN: Type your code
Value: 300

How do I unblock the browser using the MoneyPak?

1. Find a retail location (7 Eleven, Walmart, Walgreens, Rite Aid Pharmacy, KMart, CVS Pharmacy, Kroger, Dollar General, Family Dollar, InComm, Kum&Go, Coinstar-EPS) near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash.
3. To pay fine you should enter the digits MoneyPak resulting pass in the payment form and press "Settle MoneyPak".


Polizei. ARNUNG! Zugang von Ihrem Browser wurde vorläufig aus den unten aufgelisteten Gründen gesperrt. Alle Aktivitäten des Computers auf...
Polizei. ARNUNG! Zugang von Ih...
Neuer Tab
block.zeropoliceintl.biz
cyscon GmbH
Bundesamt für Sicherheit in der Informationstechnik
Gesellschaft zur Verfügung von Urheberrechtsverletzungen e.V.
BundesKriminalamt
BUNDESPOLIZEI
GVU
Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V.
CYBER CRIME
paysafecard
1 2 3 4 5 6 7 8 9 0 ← Clear
Bezahlen PaySafeCard

IP: 92.231.76.168

Land: Germany
Bereich: 01
Stadt: Karlsruhe

WARNUNG! Zugang von Ihrem Browser wurde vorläufig aus den unten aufgelisteten Gründen gesperrt.
Alle Aktivitäten des Computers aufgezeichnet wurden.
Alle Ihre Dateien werden verschlüsselt.

Ihnen wird die Ansicht/Lagerung und/oder den Vertrieb von pornographischem Material von verbotenen Inhalte (Kinderpornografie/Zoophilie/Vergewaltigung, etc.) vorgeworfen. Sie haben die Allgemeine Erklärung zur Bekämpfung der Verbreitung von Kinderpornographie verletzt wegen einer Straftat nach Artikel 161 des Strafgesetzbuches der Bundesrepublik Deutschland.

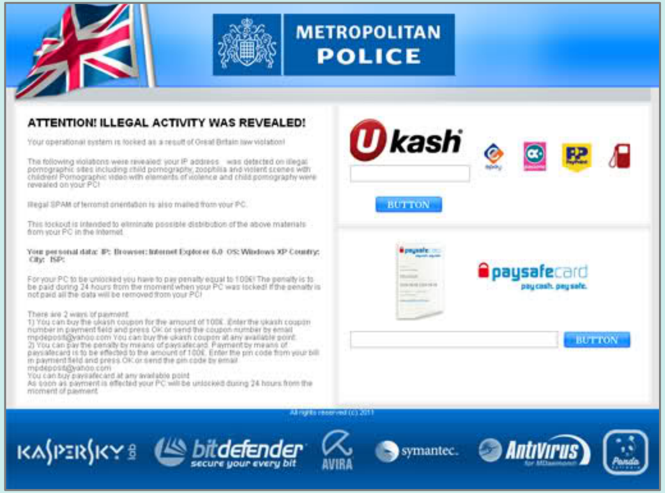
Artikel 161 des Strafgesetzbuches der Bundesrepublik Deutschland sieht eine Freiheitsstrafe von 5 bis 11 Jahren in solchen Fällen vor.

Gutschein-Code/PIN: Geben Sie Ihren Code
Wert: 100

Wo bekomme ich einen PaySafeCard Gutschein?

PaySafeCard erhältst du in vielen Supermärkten, Trafiken, Tankstellen und Kiosken. Sie bekommen Ihre PaySafeCard z.B. bei Rossman Drogeriemärkten, Netto Marken-Discount, vielen Tankstellen sowie Wolsdorff, WEZ, WestLotto, Westfalen, Vodafone, The Phone House, Tank&Rast, REWE, Q1, Shell, Agip, Eni, Avia, NETTO, LOTTO Niedersachsen, LOTTO Brandenburg, LOTTO Berlin, LOTTO Bayern, Lotto Annahmestellen,

Locker Ransomware



ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mailed from your PC.

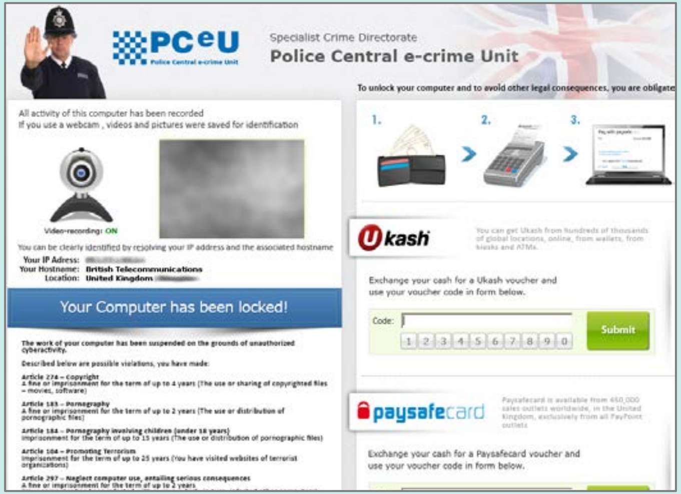
This lockout is intended to eliminate possible distribution of the above materials from your PC in the Internet.

Your personal data: IP: Browser: Internet Explorer 6.0 OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100€! The penalty is to be paid during 24 hours from the moment when your PC was locked! If the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:
1) You can buy the ukash coupon for the amount of 100€. Enter the ukash coupon number in payment field and press OK or send the coupon number by email mpdeposit@yahoo.com You can buy the ukash coupon at any available point.
2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected to the amount of 100€. Enter the pin code from your bill in payment field and press OK or send the pin code by email mpdeposit@yahoo.com
You can buy paysafecard at any available point
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

All rights reserved (c) 2011



Specialist Crime Directorate

Police Central e-crime Unit

To unlock your computer and to avoid other legal consequences, you are obligate

All activity of this computer has been recorded
If you use a webcam , videos and pictures were saved for identification

Video-recording: ON

You can be clearly identified by resolving your IP address and the associated hostname

Your IP Adress: [redacted]
Your Hostname: British Telecommunications
Location: United Kingdom [redacted]

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)

Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)

Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)

Article 104 – Promoting Terrorism
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)

Article 297 – Neglect computer use, entailing serious consequences
A fine or imprisonment for the term of up to 2 years

You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.

Exchange your cash for a Ukash voucher and use your voucher code in form below.

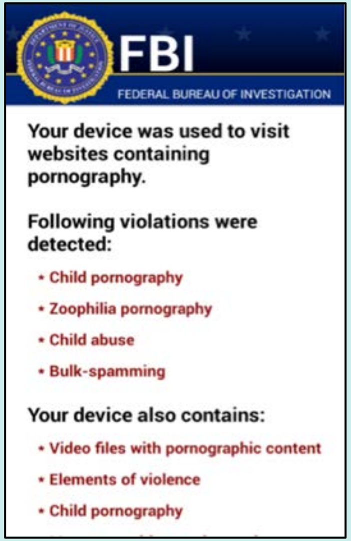
Code:

Paysafecard is available from 450,000 sales outlets worldwide, in the United Kingdom, exclusively from all PayPoint outlets

Exchange your cash for a Paysafecard voucher and use your voucher code in form below.

ISACA®
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Locker Ransomware (Android)



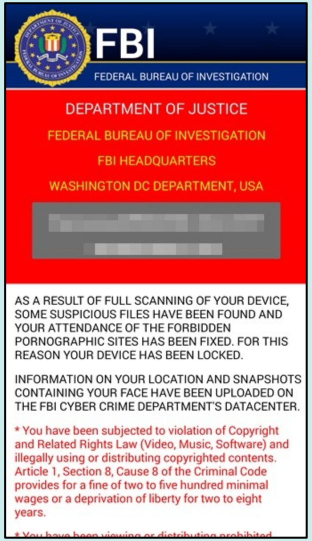
Your device was used to visit websites containing pornography.

Following violations were detected:

- Child pornography
- Zoophilia pornography
- Child abuse
- Bulk-spamming

Your device also contains:

- Video files with pornographic content
- Elements of violence
- Child pornography



DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WASHINGTON DC DEPARTMENT, USA

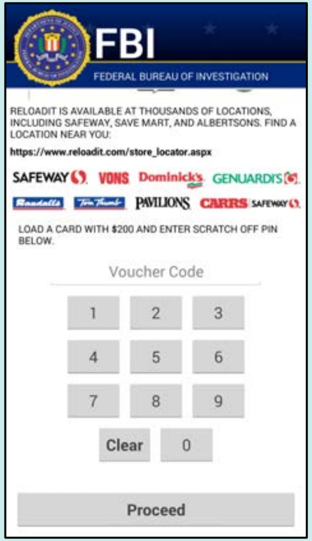
[redacted]

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

* You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents. Article 1, Section 8, Cause 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



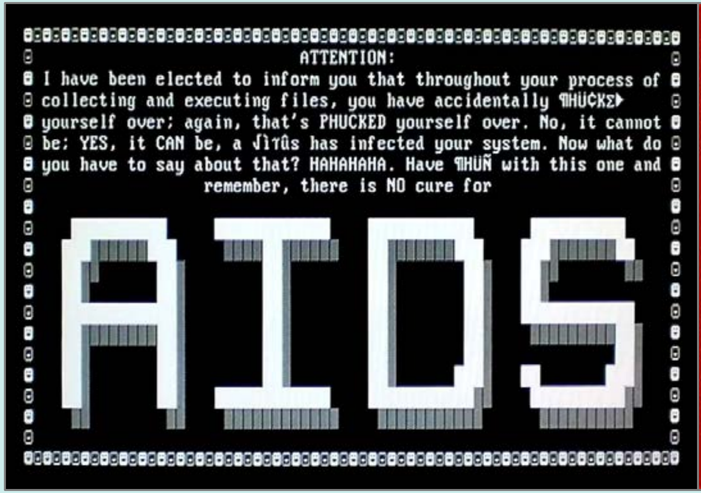
RELOADIT IS AVAILABLE AT THOUSANDS OF LOCATIONS, INCLUDING SAFEWAY, SAVE MART, AND ALBERTSONS. FIND A LOCATION NEAR YOU:

https://www.reloadit.com/store_locator.aspx

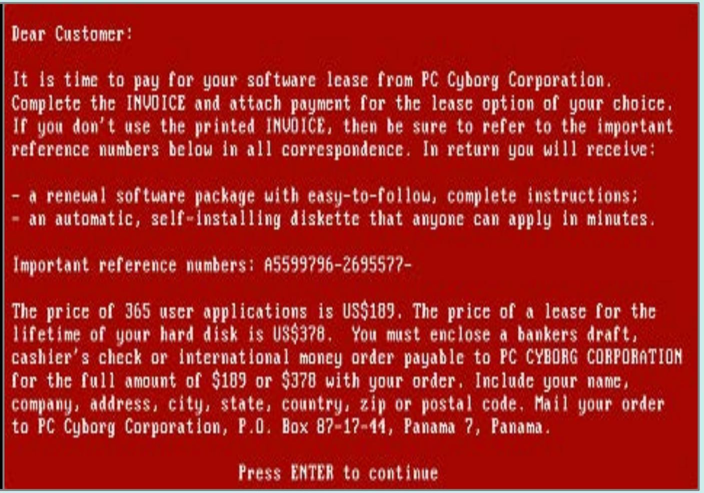
LOAD A CARD WITH $200 AND ENTER SCRATCH OFF PIN BELOW.

Voucher Code

Ransomware (AIDS / PC Cyborg) (1989)

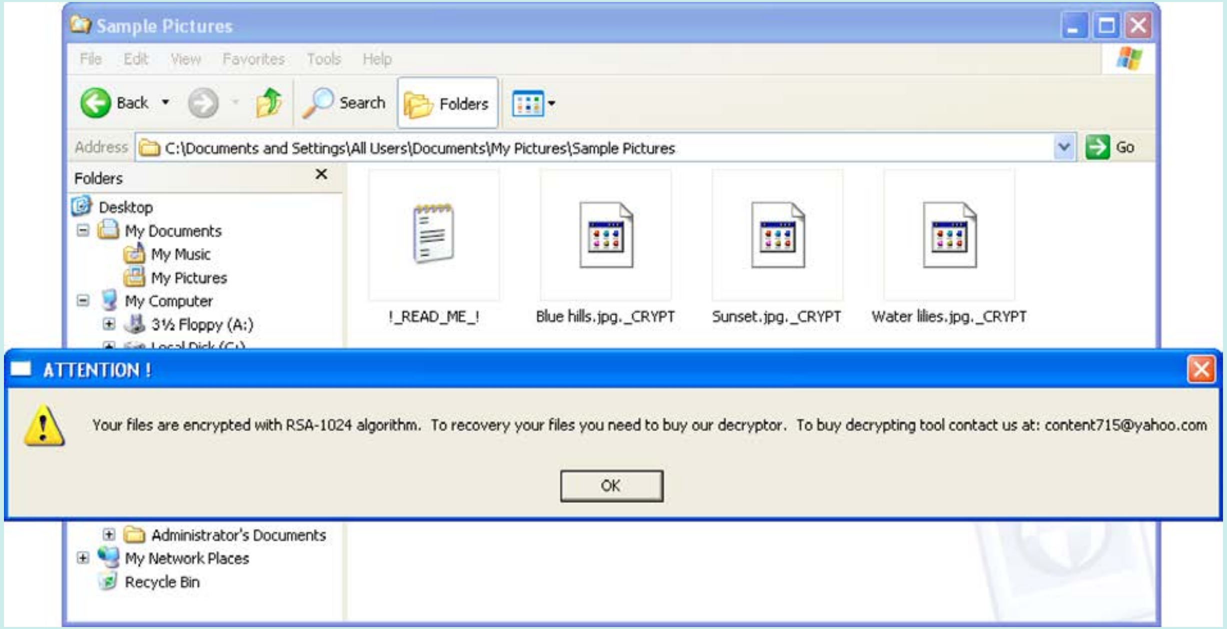


```
                              ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accidentally ¶HÜ¢KΣ▶
yourself over; again, that's PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a √ìτûs has infected your system. Now what do
you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and
                    remember, there is NO cure for

                                 AIDS
```



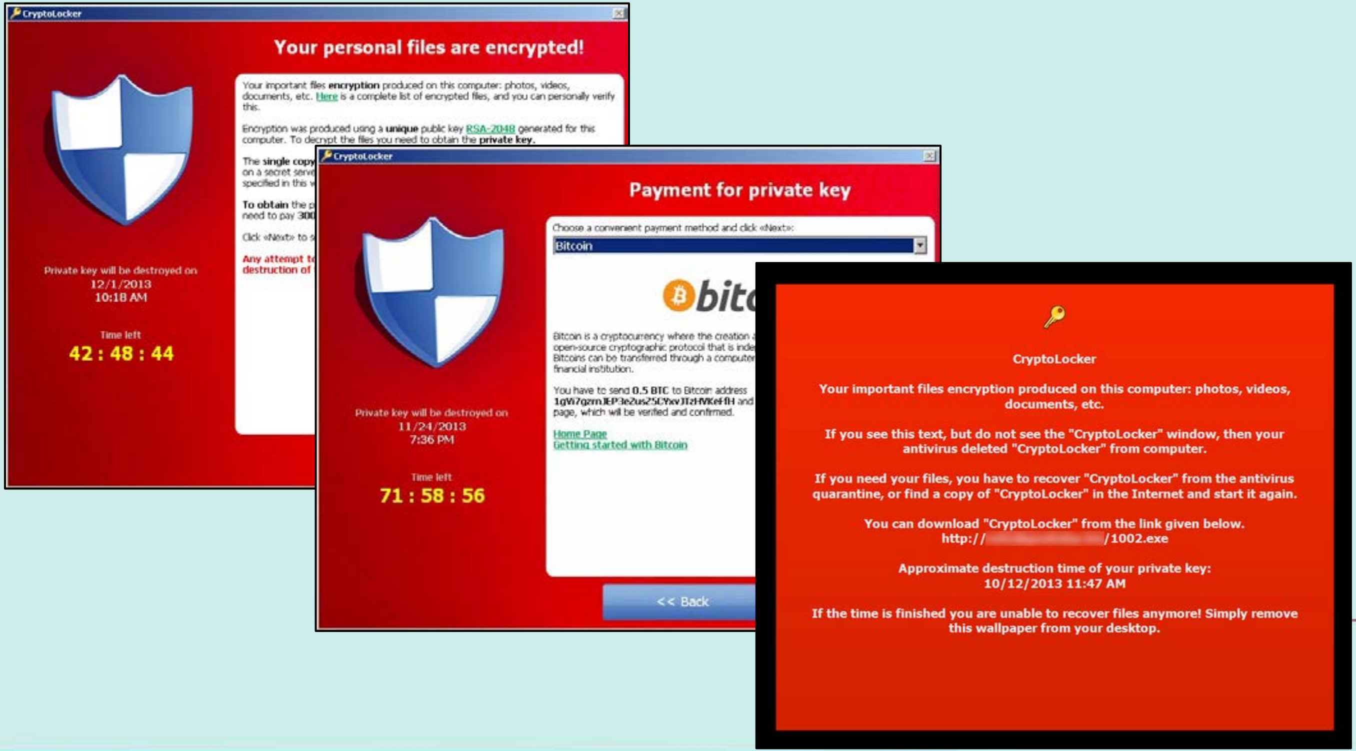
```
Dear Customer:

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
```

Crypto-Ransomware (Gpcode) (2005)



Your files are encrypted with RSA-1024 algorithm. To recovery your files you need to buy our decryptor. To buy decrypting tool contact us at: content715@yahoo.com

Crypto-Ransomware (Cryptolocker) (2013)



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy**
on a secret serve
specified in this w

To obtain the p
need to pay **300**

Click «Next» to s

Any attempt to
destruction of

Private key will be destroyed on
12/1/2013
10:18 AM

Time left
42 : 48 : 44

Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin

Bitcoin is a cryptocurrency where the creation a
open-source cryptographic protocol that is inde
Bitcoins can be transferred through a computer
financial institution.

You have to send **0.5 BTC** to Bitcoin address
1gVi7gzmJEP3e2us25CYxvJTzHVKeFfH and
page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Private key will be destroyed on
11/24/2013
7:36 PM

Time left
71 : 58 : 56

CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
http://[redacted]/1002.exe

Approximate destruction time of your private key:
10/12/2013 11:47 AM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

200 Crypto-Ransomware Families

.CryptoHasYou., 777, 7ev3n, 7h9r, 8lock8, **Alfa Ransomware**, **Alma Ransomware**, Alpha Ransomware, AMBA, Apocalypse, ApocalypseVM, AutoLocky, BadBlock, BaksoCrypt, Bandarchor, Bart, BitCryptor, BitStak, BlackShades Crypter, Blocatto, Booyah, Brazilian, BrLock, Browlock, Bucbi, BuyUnlockCode, Cerber, Chimera, CoinVault, Coverton, Cryaki, Crybola, CryFile, CryLocker, **CrypMIC**, Crypren, Crypt38, Cryptear, **CryptFile2**, CryptInfinite, CryptoBit, CryptoDefense, CryptoFinancial, CryptoFortress, CryptoGraphic Locker, CryptoHost, CryptoJoker, **CryptoLocker**, Cryptolocker 2.0, CryptoMix, CryptoRoger, CryptoShocker, CryptoTorLocker2015, CryptoWall 1, CryptoWall 2, CryptoWall 3, CryptoWall 4, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, **CryptXXX 3.1**, CTB-Faker, **CTB-Locker**, CTB-Locker WEB, CuteRansomware, DeCrypt Protect, DEDCryptor, DetoxCrypto, DirtyDecrypt, DMALocker, DMALocker 3.0, Domino, EDA2 / HiddenTear, EduCrypt, El-Polocker, Enigma, FairWare, Fakben, Fantom, Fonco, Fsociety, Fury, GhostCrypt, Globe, GNL Locker, Gomasom, Goopic, Gopher, Harasom, Herbst, Hi Buddy!, Hitler, HolyCrypt, HydraCrypt, iLock, iLockLight, International Police Association, JagerDecryptor, Jeiphoos, Jigsaw, Job Crypter, **KeRanger**, KeyBTC, KEYHolder, KimcilWare, Korean, Kozy.Jozy, KratosCrypt, KryptoLocker, LeChiffre, Linux.Encoder, Locker, **Locky**, Lortok, LowLevel04, Mabouia, Magic, MaktubLocker, MIRCOP, MireWare, Mischa, MM Locker, Mobef, NanoLocker, Nemucod, NoobCrypt, Nullbyte, ODCODC, Offline ransomware, OMG! Ransomware, Operation Global III, PadCrypt, Pclock, **Petya**, PizzaCrypts, PokemonGO, PowerWare, PowerWorm, PRISM, R980, RAA encryptor, Radamant, Rakhni,, Rannoh, Ransom32, RansomLock, Rector, RektLocker, RemindMe, Rokku, Samas-Samsam, Sanction, Satana, Scraper, Serpico, Shark, ShinoLocker, Shujin, Simple_Encoder, SkidLocker / Pompous, Smrss32, SNSLocker, Sport, Stampado, Strictor, Surprise, SynoLocker, SZFLocker, TeslaCrypt 0.x - 2.2.0, TeslaCrypt 3.0+, TeslaCrypt 4.1A, TeslaCrypt 4.2, Threat Finder, **TorrentLocker**, TowerWeb, Toxcrypt, Troldesh, TrueCrypter, Turkish Ransom, UmbreCrypt, Ungluk, Unlock92, VaultCrypt, VenusLocker, Virlock, Virus-Encoder, WildFire Locker, Xorist, XRTN, Zcrypt, **Zepto**, Zimbra, Zlader / Russian, Zyklon

Crypto-Ransomware (Targets)

OS Disk

Local Disk(s)

Connected Device(s)
(USB)
(e.g. Backup Disk)

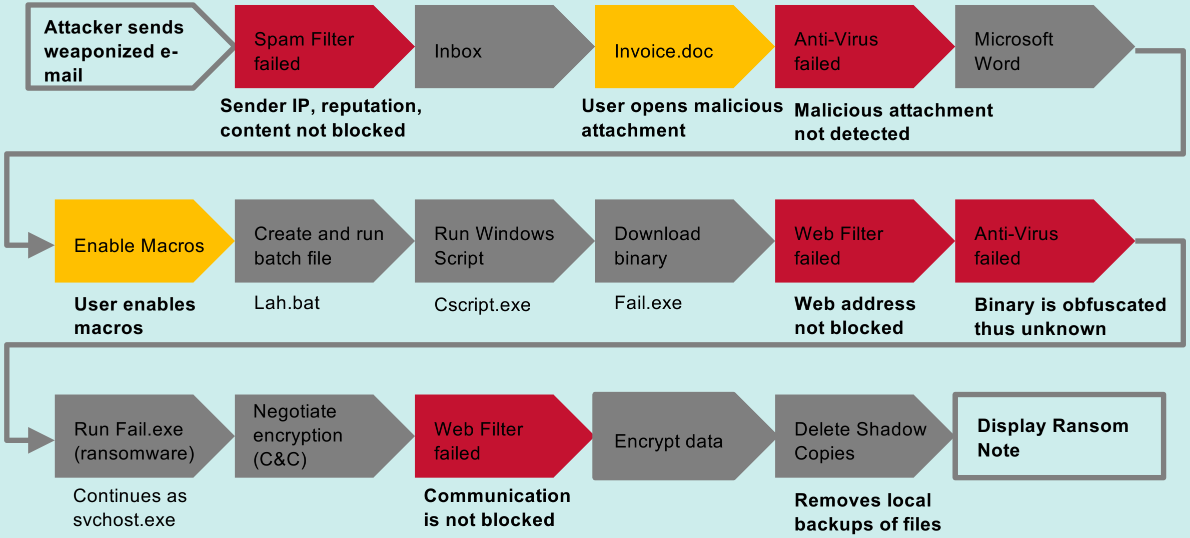
Mapped Network Drive(s)
(e.g. NAS / File Servers)

Other Accessible Folders / Shared Local Network
(e.g. NAS / File Servers)

Dropbox

OneDrive

Social Engineering Flow (Locky ransomware, .doc)



Attacker sends weaponized e-mail

Spam Filter failed

Sender IP, reputation, content not blocked

Inbox

Invoice.doc

User opens malicious attachment

Anti-Virus failed

Malicious attachment not detected

Microsoft Word

Enable Macros

User enables macros

Create and run batch file

Lah.bat

Run Windows Script

Cscript.exe

Download binary

Fail.exe

Web Filter failed

Web address not blocked

Anti-Virus failed

Binary is obfuscated thus unknown

Run Fail.exe (ransomware)

Continues as svchost.exe

Negotiate encryption (C&C)

Web Filter failed

Communication is not blocked

Encrypt data

Delete Shadow Copies

Removes local backups of files

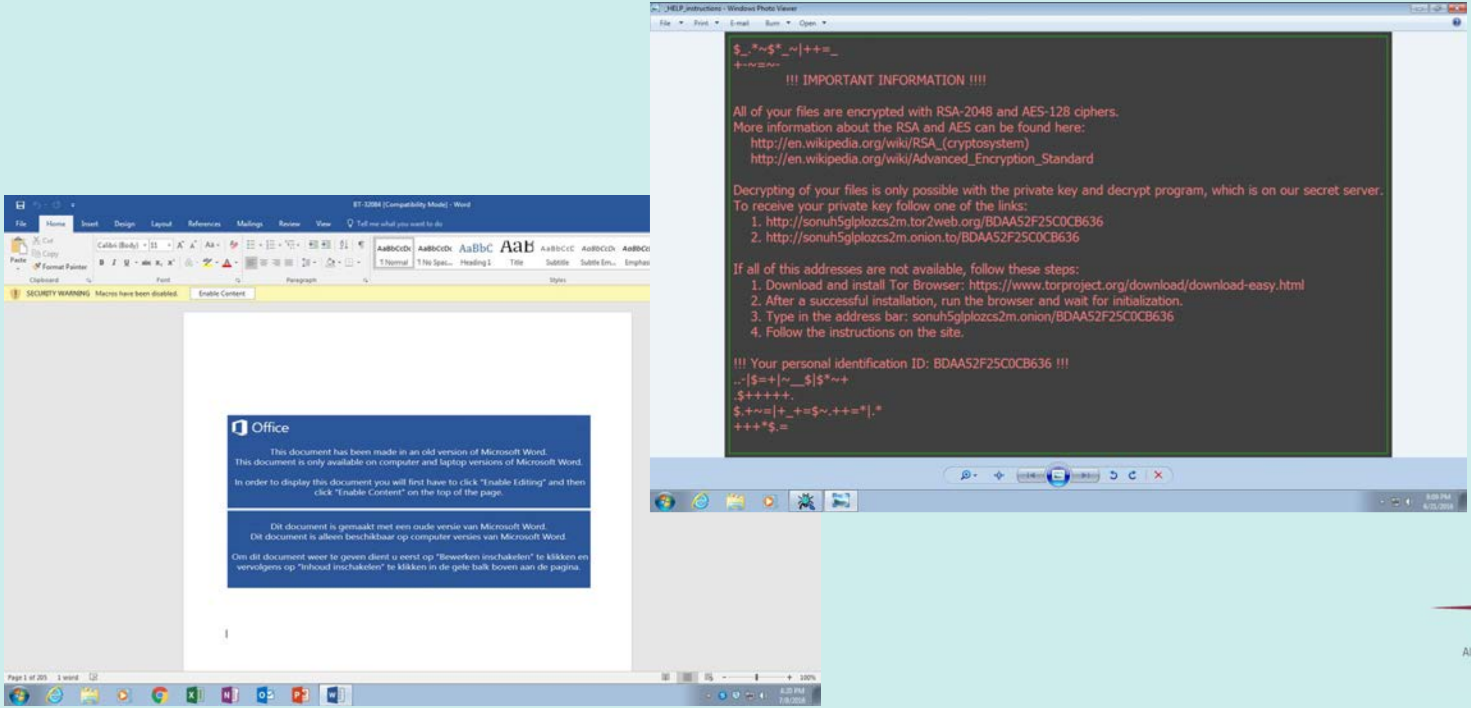
Display Ransom Note

ISACA®

Al servizio dei professionisti dell'IT Governance

Rome Chapter

Social Engineering Flow
(Locky ransomware, .docm)



SECURITY WARNING Macros have been disabled. Enable Content

Office

This document has been made in an old version of Microsoft Word.
This document is only available on computer and laptop versions of Microsoft Word.

In order to display this document you will first have to click "Enable Editing" and then click "Enable Content" on the top of the page.

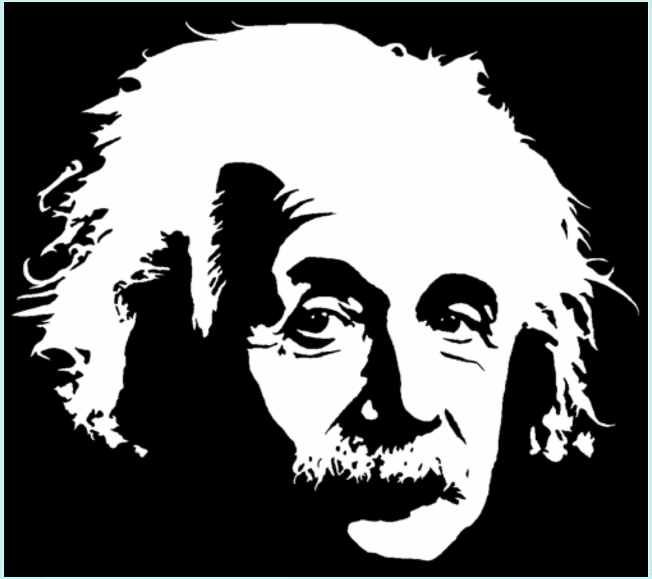
Dit document is gemaakt met een oude versie van Microsoft Word.
Dit document is alleen beschikbaar op computer versies van Microsoft Word.

Om dit document weer te geven dient u eerst op "Bewerken inschakelen" te klikken en vervolgens op "Inhoud inschakelen" te klikken in de gele balk boven aan de pagina.

```
$_.*~$*_~|++=_
+-~=~-
        !!! 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/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://sonuh5glplozcs2m.tor2web.org/BDAA52F25C0CB636
   2. http://sonuh5glplozcs2m.onion.to/BDAA52F25C0CB636

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: sonuh5glplozcs2m.onion/BDAA52F25C0CB636
   4. Follow the instructions on the site.

!!! Your personal identification ID: BDAA52F25C0CB636 !!!
..-|$=+|~__$|$*~+
.$+++++.
$.+~=|+_+=$~.++=*|.*
+++*$.=
```

Security Overview

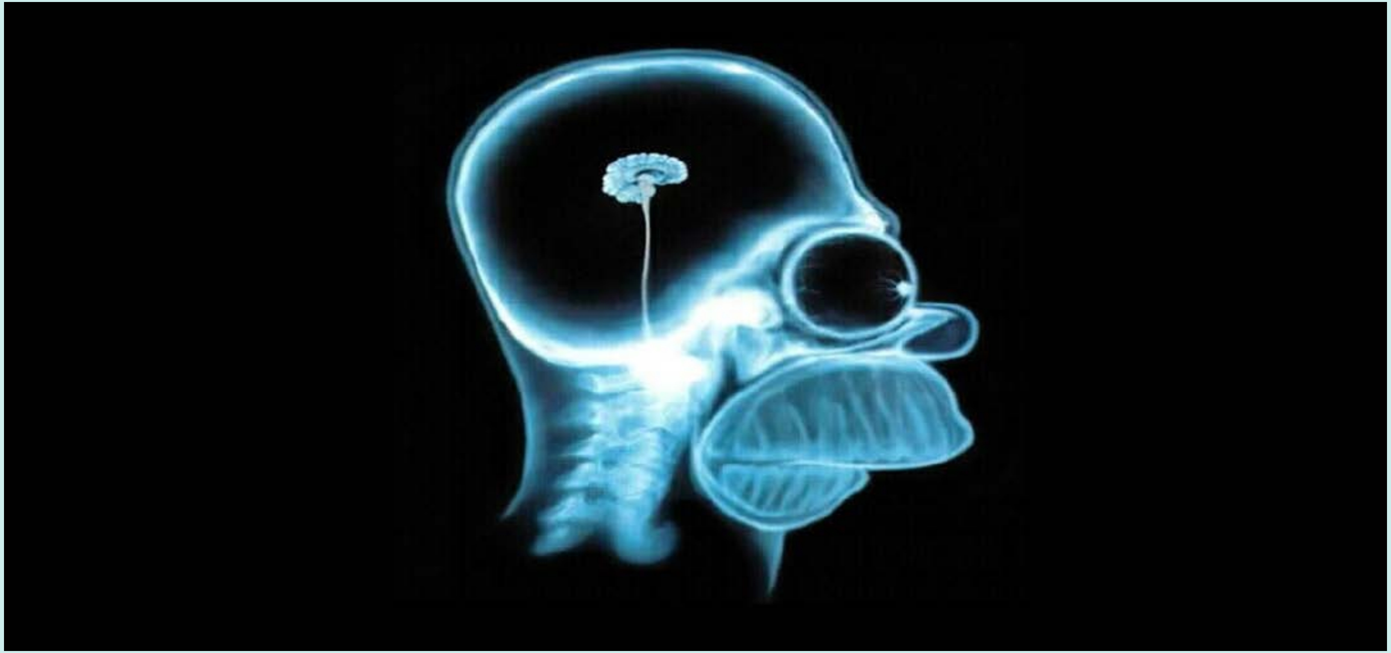
Today's approach to IT Security is **Falling Behind**



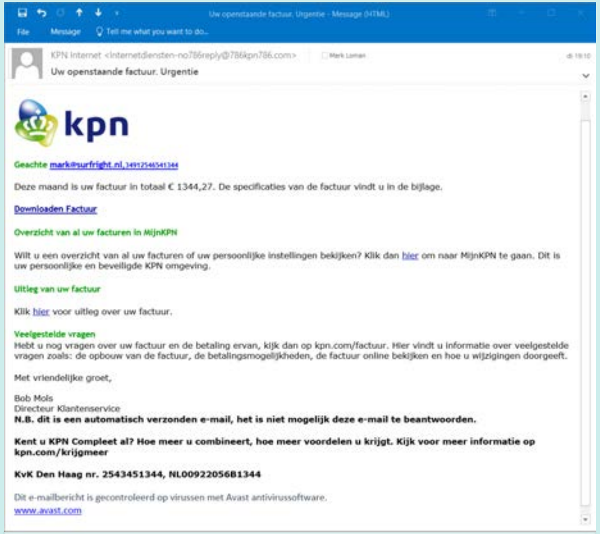
"Two things are infinite: The universe and human stupidity, and I'm not so sure about the former"

- Albert Einstein

What is social engineering?



Social Engineering Example


Uw openstaande factuur. Urgentie - Message (HTML)
File
Message
Tell me what you want to do...

KPN Internet <internetdiensten-no786reply@786kpn786.com> Mark Loman di 19:10

Uw openstaande factuur. Urgentie

Geachte mark@surfright.nl,34912546541344

Deze maand is uw factuur in totaal € 1344,27. De specificaties van de factuur vindt u in de bijlage.

Downloaden Factuur

Overzicht van al uw facturen in MijnKPN

Wilt u een overzicht van al uw facturen of uw persoonlijke instellingen bekijken? Klik dan hier om naar MijnKPN te gaan. Dit is uw persoonlijke en beveiligde KPN omgeving.

Uitleg van uw factuur

Klik hier voor uitleg over uw factuur.

Veelgestelde vragen
Hebt u nog vragen over uw factuur en de betaling ervan, kijk dan op kpn.com/factuur. Hier vindt u informatie over veelgestelde vragen zoals: de opbouw van de factuur, de betalingsmogelijkheden, de factuur online bekijken en hoe u wijzigingen doorgeeft.

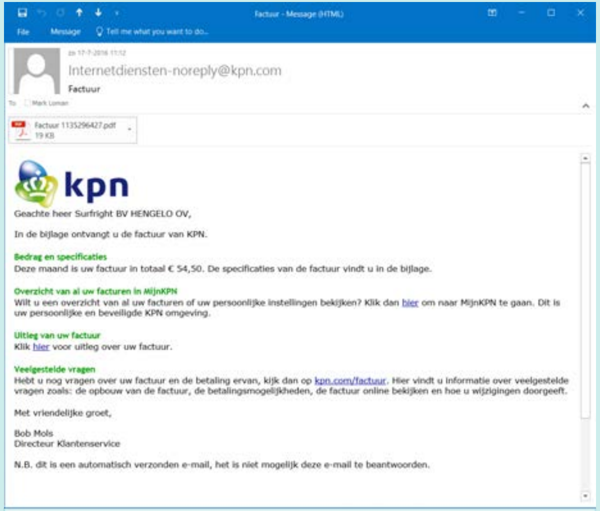
Met vriendelijke groet,

Bob Mols
Directeur Klantenservice
N.B. dit is een automatisch verzonden e-mail, het is niet mogelijk deze e-mail te beantwoorden.

Kent u KPN Compleet al? Hoe meer u combineert, hoe meer voordelen u krijgt. Kijk voor meer informatie op kpn.com/krijgmeer

KvK Den Haag nr. 2543451344, NL00922056B1344

Dit e-mailbericht is gecontroleerd op virussen met Avast antivirussoftware.
www.avast.com



za 17-7-2016 11:12

Internetdiensten-noreply@kpn.com

Factuur

To Mark Loman

Factuur 1135296427.pdf
19 KB

Geachte heer Surfright BV HENGELO OV,

In de bijlage ontvangt u de factuur van KPN.

Bedrag en specificaties
Deze maand is uw factuur in totaal € 54,50. De specificaties van de factuur vindt u in de bijlage.

Overzicht van al uw facturen in MijnKPN
Wilt u een overzicht van al uw facturen of uw persoonlijke instellingen bekijken? Klik dan hier om naar MijnKPN te gaan. Dit is uw persoonlijke en beveiligde KPN omgeving.

Uitleg van uw factuur
Klik hier voor uitleg over uw factuur.

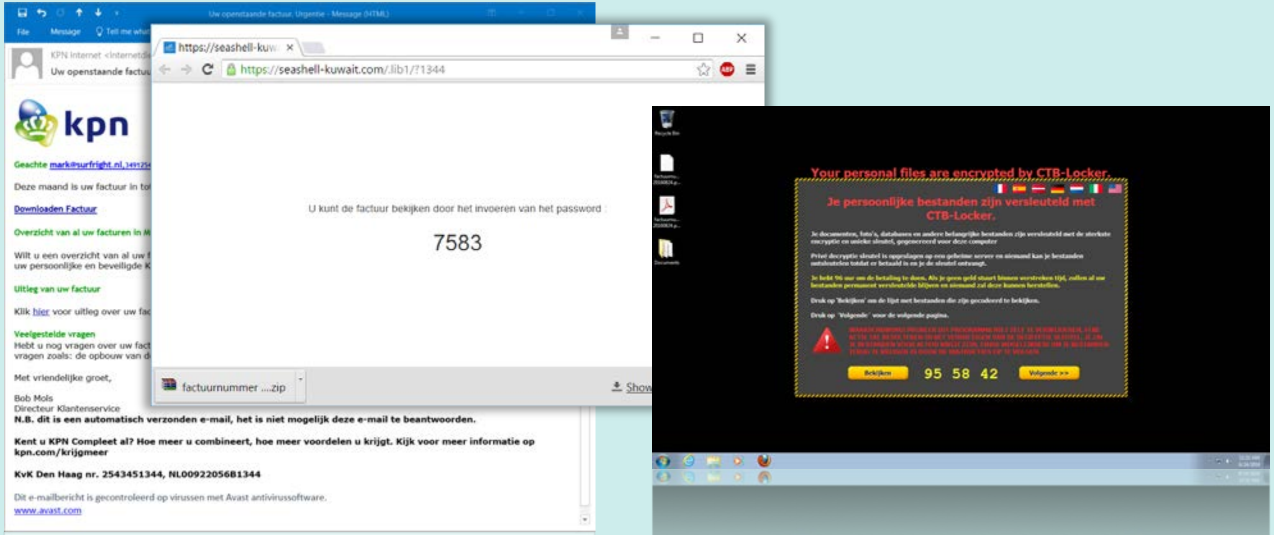
Veelgestelde vragen
Hebt u nog vragen over uw factuur en de betaling ervan, kijk dan op kpn.com/factuur. Hier vindt u informatie over veelgestelde vragen zoals: de opbouw van de factuur, de betalingsmogelijkheden, de factuur online bekijken en hoe u wijzigingen doorgeeft.

Met vriendelijke groet,

Bob Mols
Directeur Klantenservice

N.B. dit is een automatisch verzonden e-mail, het is niet mogelijk deze e-mail te beantwoorden.

Social Engineering Example



Uw openstaande factuur, Urgentie - Message (HTML)

KPN Internet <internetdi

Uw openstaande factuu

Geachte mark@surfright.nl,349125

Deze maand is uw factuur in to

Downloaden Factuur

Overzicht van al uw facturen in M

Wilt u een overzicht van al uw f
uw persoonlijke en beveiligde K

Uitleg van uw factuur

Klik hier voor uitleg over uw fac

Veelgestelde vragen
Hebt u nog vragen over uw fact
vragen zoals: de opbouw van d

Met vriendelijke groet,

Bob Mols
Directeur Klantenservice
N.B. dit is een automatisch verzonden e-mail, het is niet mogelijk deze e-mail te beantwoorden.

Kent u KPN Compleet al? Hoe meer u combineert, hoe meer voordelen u krijgt. Kijk voor meer informatie op kpn.com/krijgmeer

KvK Den Haag nr. 2543451344, NL009220566B1344

Dit e-mailbericht is gecontroleerd op virussen met Avast antivirussoftware.
www.avast.com

https://seashell-kuw

https://seashell-kuwait.com/.lib1/?1344

U kunt de factuur bekijken door het invoeren van het password :

7583

factuurnummer ....zip

Your personal files are encrypted by CTB-Locker.

Je persoonlijke bestanden zijn versleuteld met CTB-Locker.

Je documenten, foto's, databases en andere belangrijke bestanden zijn versleuteld met de sterkste encryptie en unieke sleutel, gegenereerd voor deze computer

Privé decryptie sleutel is opgeslagen op een geheime server en niemand kan je bestanden ontsleutelen totdat er betaald is en je de sleutel ontvangt.

Je hebt 96 uur om de betaling te doen. Als je geen geld stuurt binnen verstreken tijd, zullen al uw bestanden permanent versleutelde blijven en niemand zal deze kunnen herstellen.

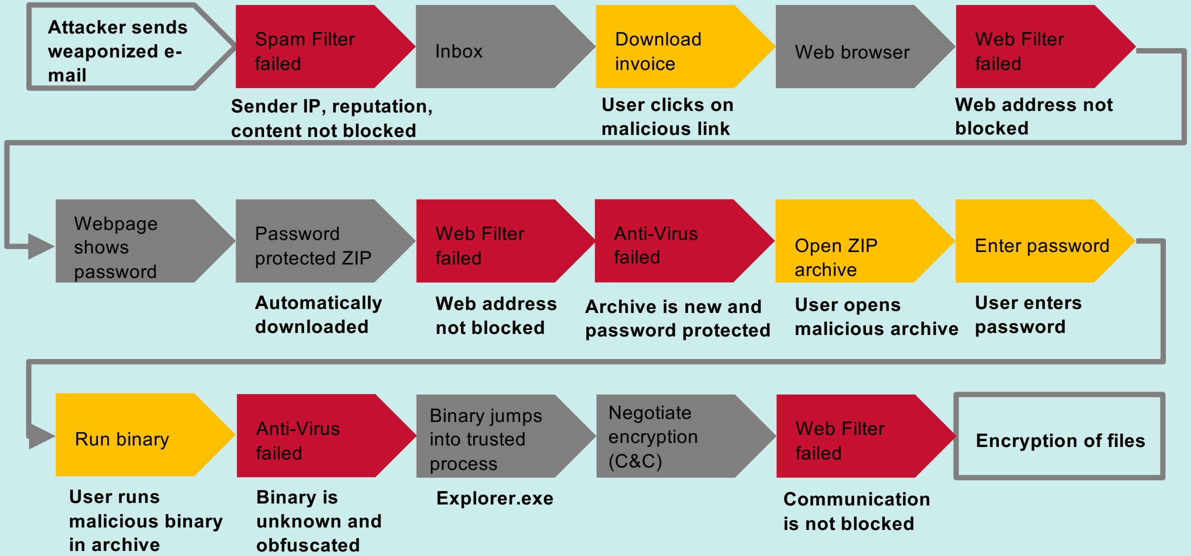
Druk op 'Bekijken' om de lijst met bestanden die zijn gecodeerd te bekijken.

Druk op 'Volgende' voor de volgende pagina.

[illegible]

Al servizio dei professionisti dell'IT Governance
Rome Chapter

Social Engineering Flow
(CTB-Locker ransomware)



Attacker sends weaponized e-mail

Spam Filter failed

Sender IP, reputation, content not blocked

Inbox

Download invoice

User clicks on malicious link

Web browser

Web Filter failed

Web address not blocked

Webpage shows password

Password protected ZIP

Automatically downloaded

Web Filter failed

Web address not blocked

Anti-Virus failed

Archive is new and password protected

Open ZIP archive

User opens malicious archive

Enter password

User enters password

Run binary

User runs malicious binary in archive

Anti-Virus failed

Binary is unknown and obfuscated

Binary jumps into trusted process

Explorer.exe

Negotiate encryption (C&C)

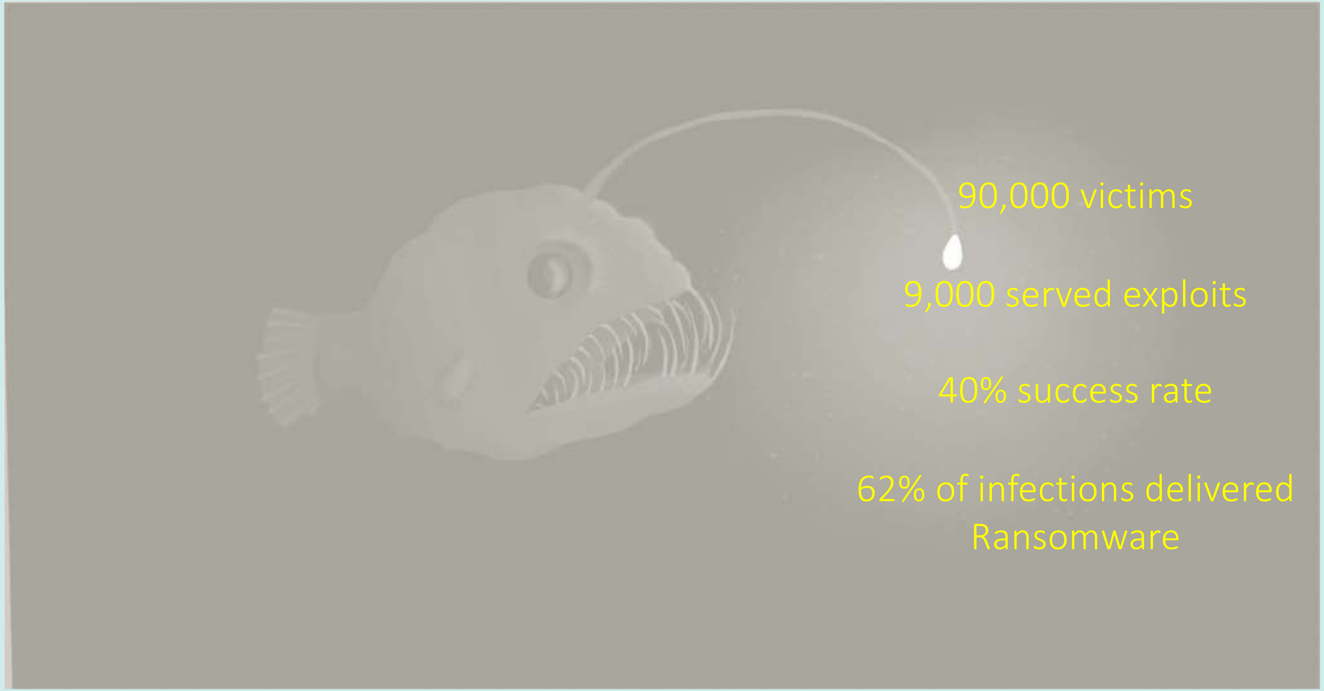
Web Filter failed

Communication is not blocked

Encryption of files

Comparison: Spam vs Exploit Kits
Why email?

Comparison: Spam vs Exploit Kits
Angler revenue in a day



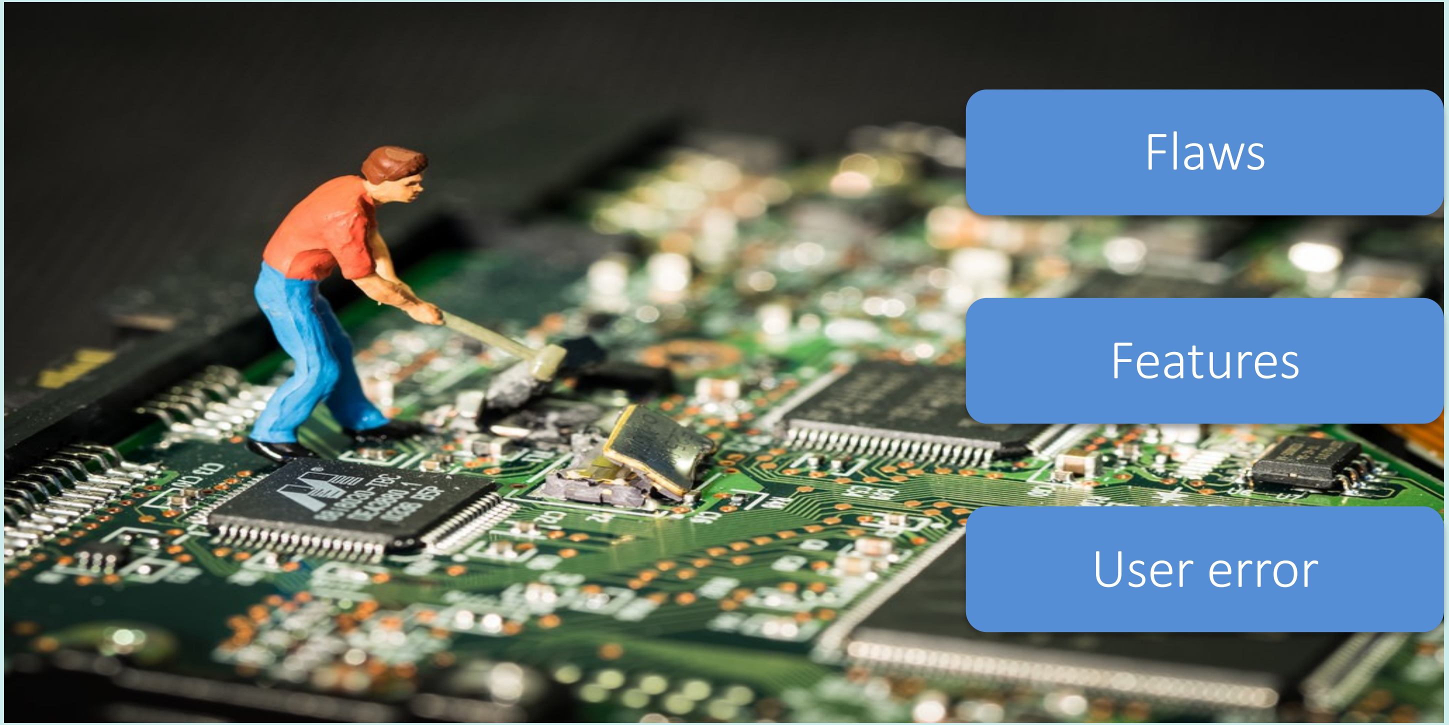
90,000 victims

9,000 served exploits

40% success rate

62% of infections delivered Ransomware

Understanding vulnerabilities



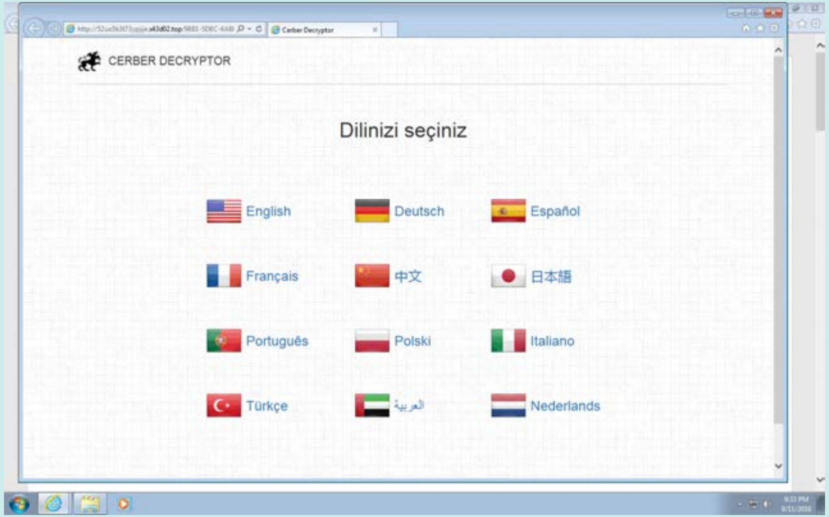
- Flaws
- Features
- User error

New tricks

- Use of other accepted file extensions (e.g. .WSF, .WSH, .HTA, .PUB files)
  - *Bypasses filters that proactively block known dangerous (ZIP) attachments (containing e.g. .EXE, .PDF.EXE, .JS, .DOCM as extension)*
- Use of a .DLL file (payload) instead of an .EXE (e.g. Locky/Zepto)
  - *In-memory attack; exploit attack delivers no files on the disk*
  - *Bypasses sandbox, signature and ‘math-based, next-gen’ products*
- Use of other active content in weaponized documents (no macros)
  - *e.g. RAA Ransomware*
- Use of only trusted binaries, part of the OS (no new code on machine)
  - *Bypasses application whitelisting, signature & ‘math-based, next-gen’ products*
- Manipulate timestamp, create extension-less copy, encrypt copy and delete original
  - *Cripple / shake off behavior-based monitoring*
- Multi-language support by attackers, to help victims pay the ransom
  - *Including chat support*

Cerber crypto-ransomware

- Ransomware-as-a-service
- Localized e-mail and chat support
- Audio warning



CERBER DECRYPTOR

Dilinizi seçiniz

English Deutsch Español

Français 中文 日本語

Português Polski Italiano

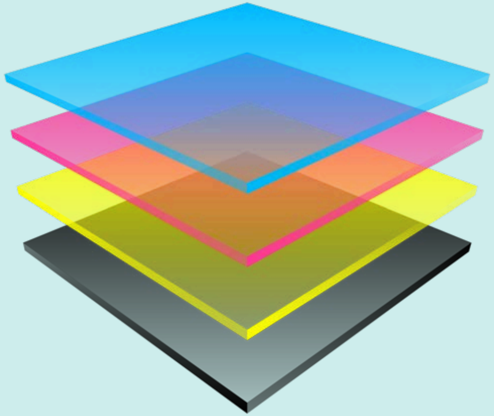
Türkçe العربية Nederlands

Synchronized Security

As a minimum you should:

- Deploy antivirus protection
- Block spam
- Use a sandboxing solution
- Block risky file extensions (javascript, vbscript, chm etc…)
- Password protect archive files
- Use URL filtering (block access to C&C servers)
- Use HTTPS filtering
- Use HIPS (host intrusion prevention service) & other signature-less technologies
- Activate your client firewalls
- Use a whitelisting solution

Enhancing layered security



Reducing the threat

”Additional Steps”

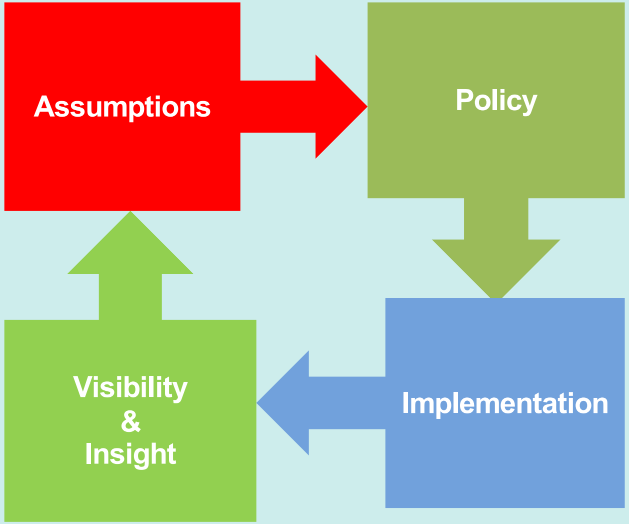
Education

Encrypt Company Data

Use Security Analysis Tools

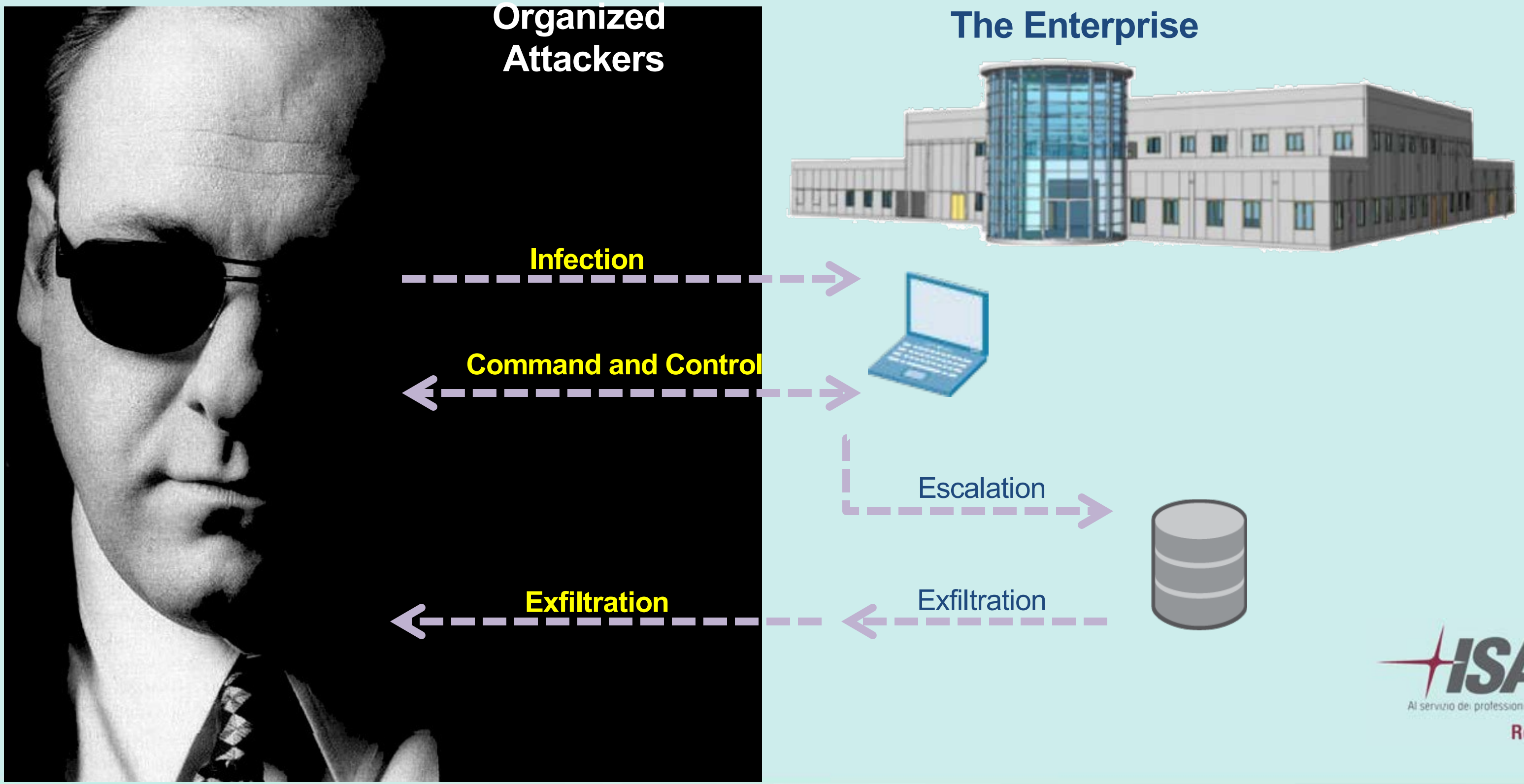
Security from Policy to Application

- What assumptions drive your security policy?
- Does your current security implementation adequately reflect that policy?
- Doss your current security implementation provide the visibility and insight needed to shape your policy?



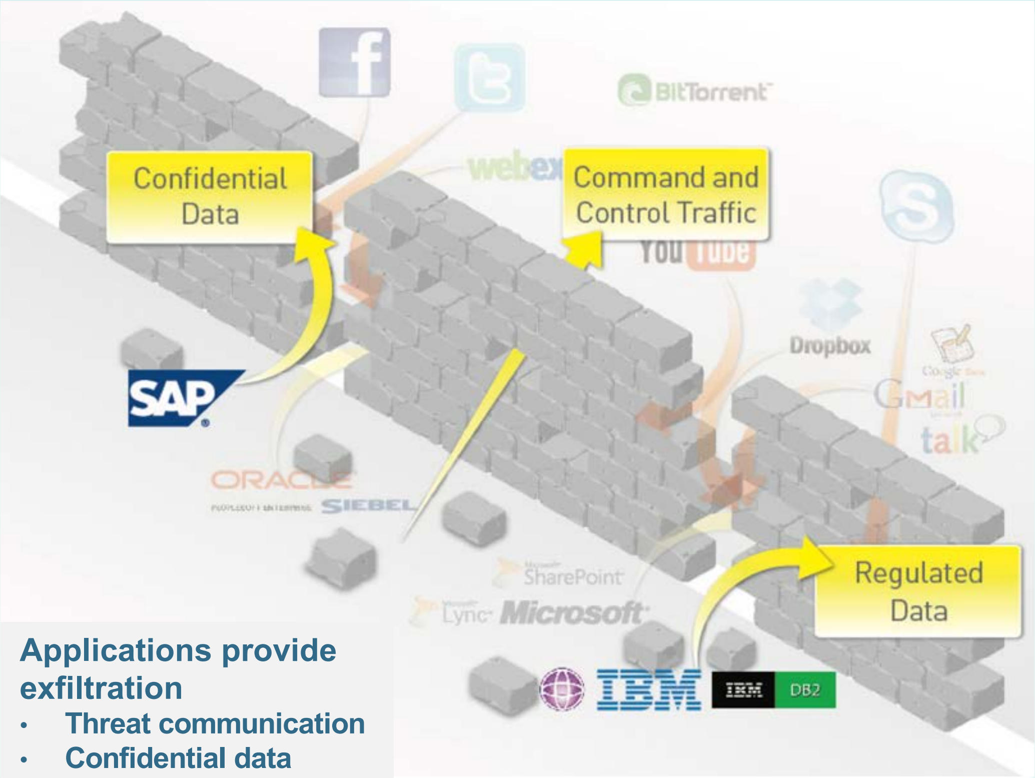
ISACA®
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Security Perimeter Paradigm



ISACA
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Is there Malware inside your network today?

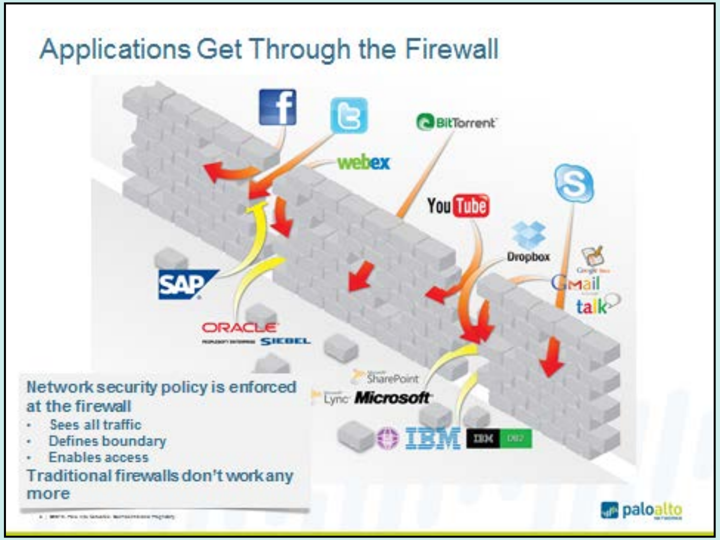


Applications provide exfiltration
- **Threat communication**
- **Confidential data**

ISACA® Al servizio dei professionisti dell'IT Governance Rome Chapter

Application Visibility

- Reduce attack surface
- Identify Applications that circumvent security policy
- Full traffic visibility that provides insight to drive policy
- Identify and inspect unknown traffic



Applications Get Through the Firewall

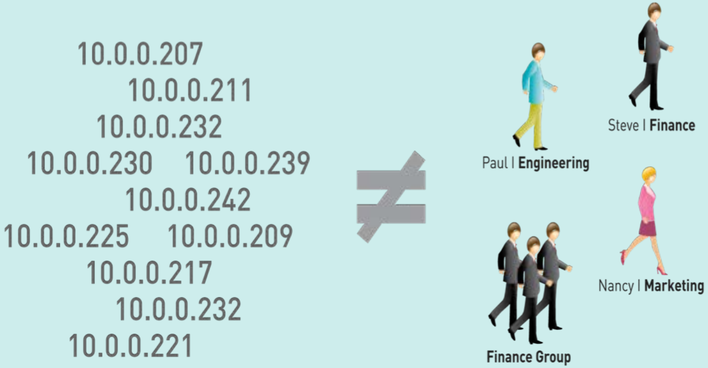
Network security policy is enforced at the firewall
- Sees all traffic
- Defines boundary
- Enables access

Traditional firewalls don't work any more

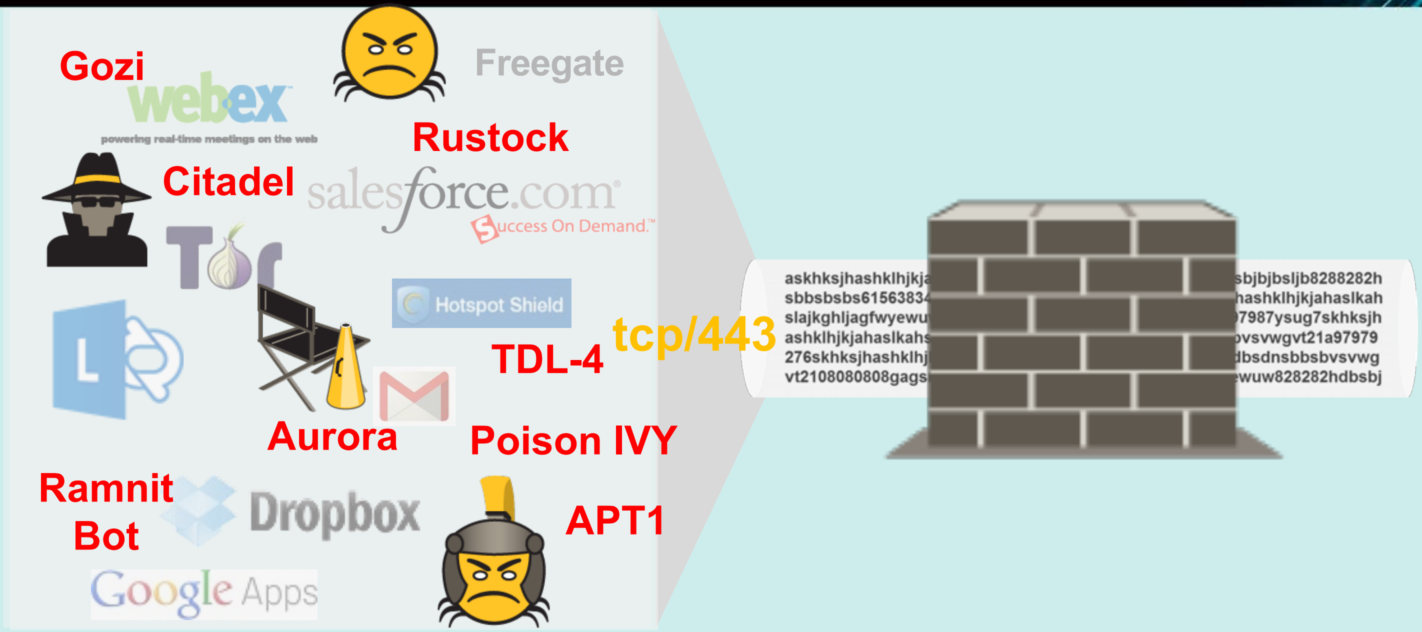
BitTorrent
webex
You Tube
Dropbox
Gmail
talk
SAP
ORACLE
SIEBEL
SharePoint
Lync
Microsoft
IBM
DB2
paloalto

Be suspicious

- Do NOT Trust, always verify all access
- Base security policy on users and their roles, not IP addresses.
- For groups of users, tie access to specific groups of applications
- Limit the amount of exfiltration via network segmentation



SSL/Port 443: The Universal Firewall Bypass

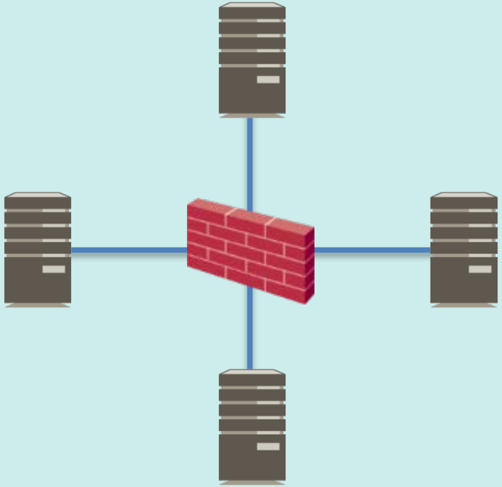


Challenge: Is SSL used to protect data and privacy, or to mask malicious actions?

Evolution of Network Segmentation & Datacenter Security

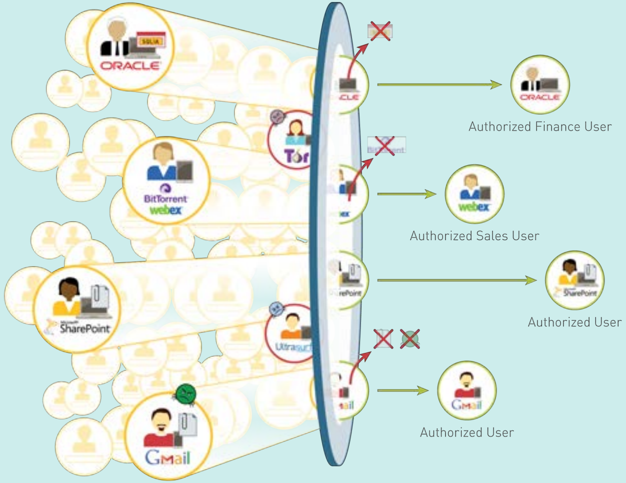
Packet Filtering, ACL's, IP/Port-based firewalling for known traffic?

Layer 1-4 Stateful Firewall



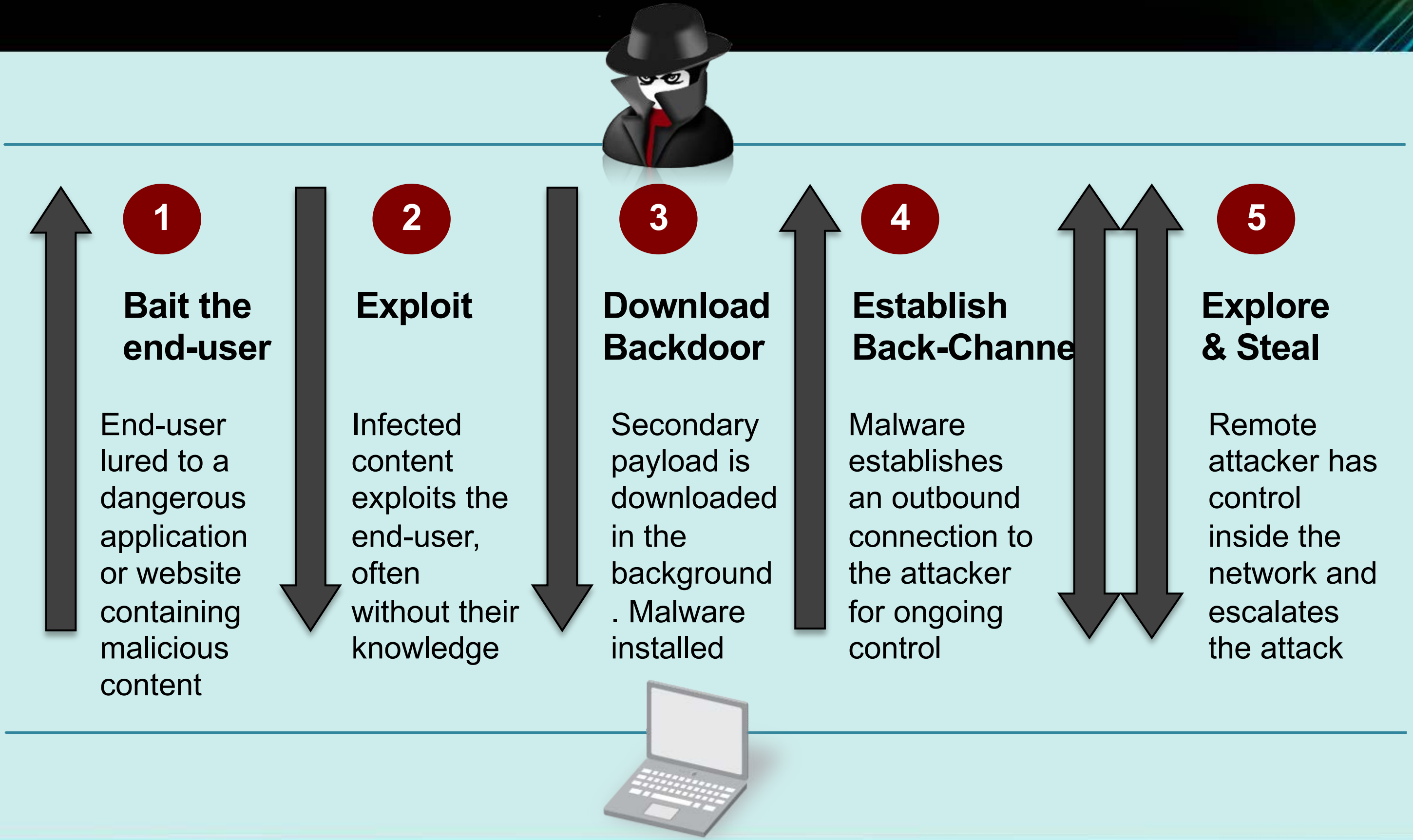
Port-hopping applications, Malware, Mobile Users – Different entry points into DC?

Layer 7 "Next Generation" Appliance



ISACA
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Modern Attacks Are Coordinated



Bait the end-user

End-user lured to a dangerous application or website containing malicious content

Exploit

Infected content exploits the end-user, often without their knowledge

Download Backdoor

Secondary payload is downloaded in the background . Malware installed

Establish Back-Channe

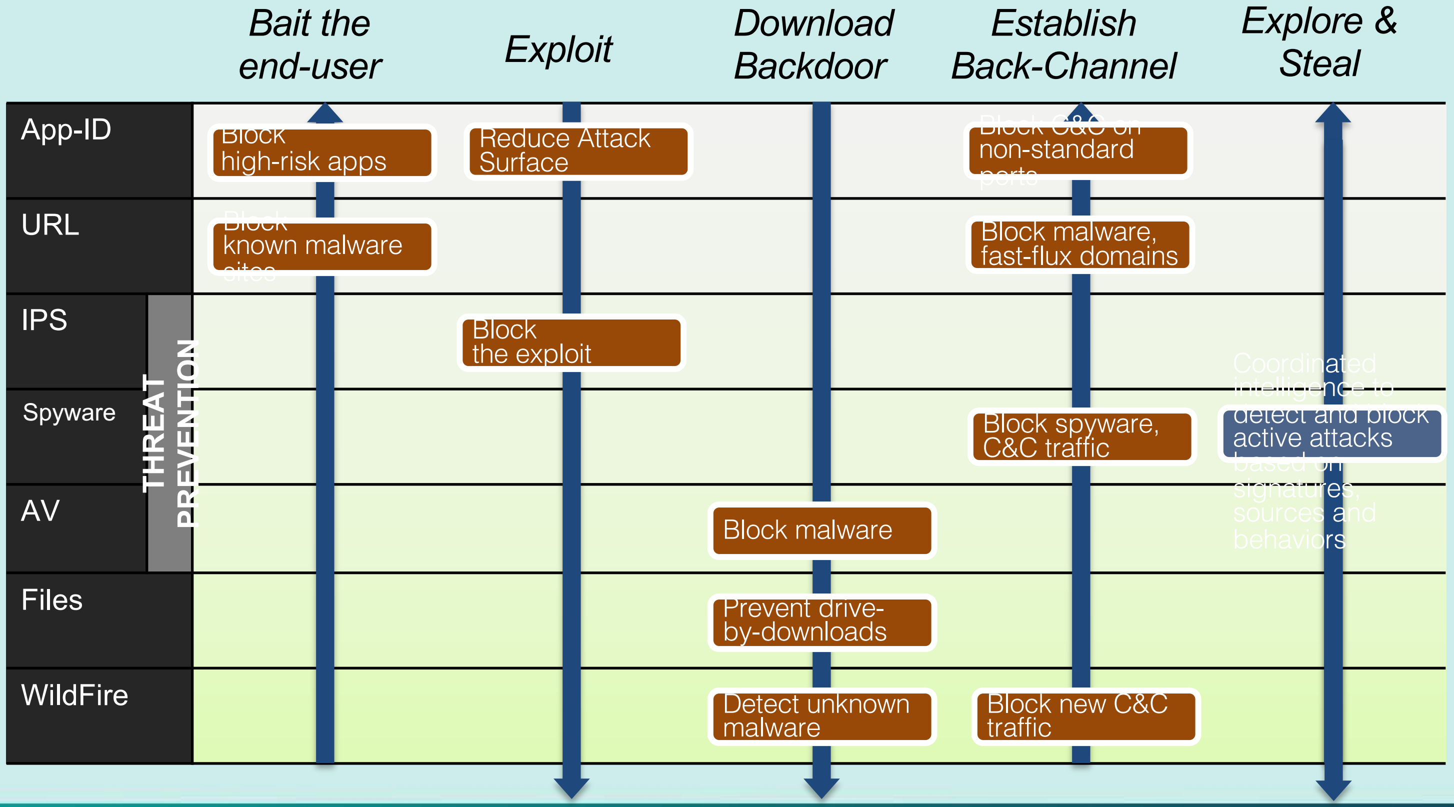
Malware establishes an outbound connection to the attacker for ongoing control

Explore & Steal

Remote attacker has control inside the network and escalates the attack

Coordinated Threat Prevention

An Integrated Approach to Threat Prevention

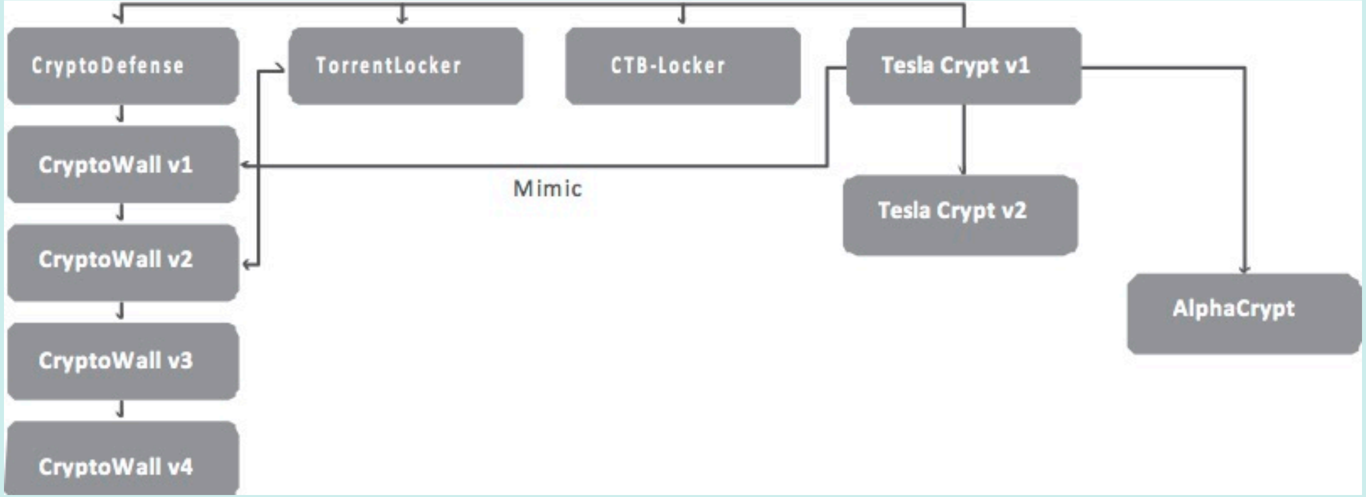


		Bait the end-user	*Exploit*	*Download Backdoor*	*Establish Back-Channel*	*Explore & Steal*
App-ID		Block high-risk apps	Reduce Attack Surface		Block C&C on non-standard ports	
URL		Block known malware sites			Block malware, fast-flux domains	
IPS	THREAT PREVENTION		Block the exploit			
Spyware					Block spyware, C&C traffic	Coordinated intelligence to detect and block active attacks based on signatures, sources and behaviors
AV				Block malware		
Files				Prevent drive-by-downloads		
WildFire				Detect unknown malware	Block new C&C traffic	

ISACA®
Al servizio dei professionisti dell'IT Governance
Rome Chapter

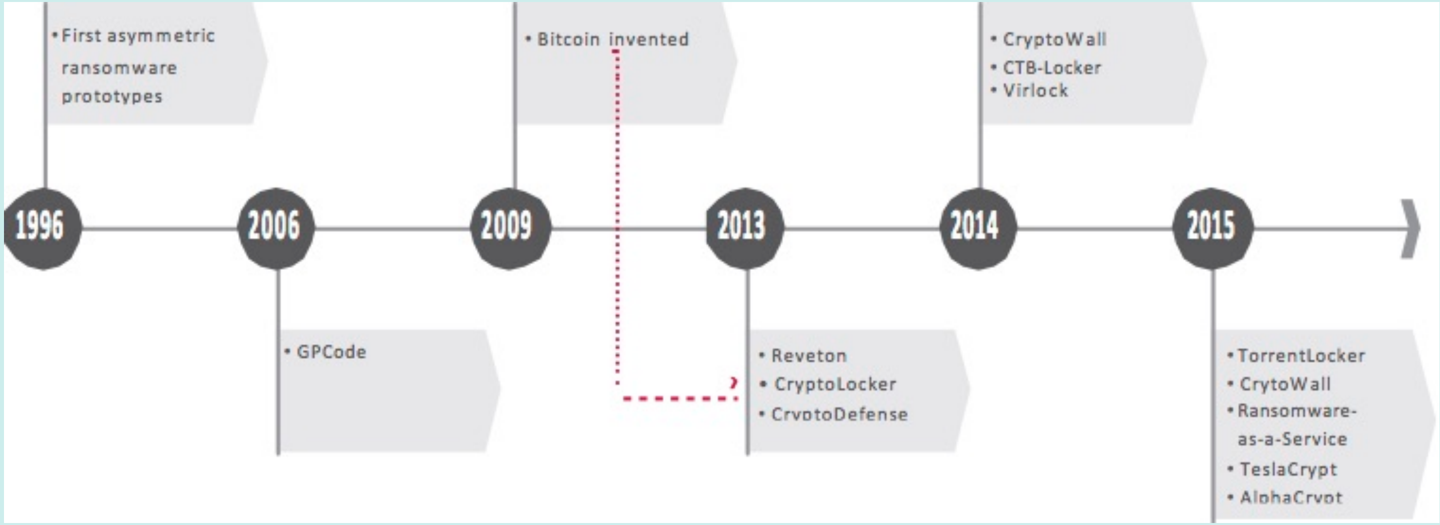
Configure your own PC

- Cryptolocker first appeared in 2013. It seems its authors gained about 27 million dollars in bitcoin
- Today – with its numerous variations – Cryptolocker is considered one of the greatest web danger



Configure your own PC

- Ransomware and spyware are successful because they exploit some weaknesses of human nature, mainly the natural tendency to give confidence to those we know or we think to know and not believing that these things can really happen



ISACA®
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Configure your own PC

- **Antivirus**
  - Even if the traditional virus no longer represent a significant threat (and not the most severe), it is good to have always active and constantly-updated the antivirus software
- **Personal firewall**
  - A personal firewall is a program installed on an ordinary personal computer (PC) that controls incoming and outgoing communications from the PC, allowing or prohibiting certain types of communication based on rules or security policies set by the user in the configuration phase

Together they constitute the main line of defense of our system

Configure your own PC

The main characteristics a personal firewall must have (*)

- Block or alert the user about all unauthorized inbound or outbound connection attempts
- Allows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt
- Hide the computer from port scans by not responding to unsolicited network traffic
- Monitor applications that are listening for incoming connections
- Monitor and regulate all incoming and outgoing Internet users
- Prevent unwanted network traffic from locally installed applications
- Provide information about the destination server with which an application is attempting to communicate
- Track recent incoming events, outgoing events, and intrusion events to see who has accessed or tried to access your computer.
- Personal Firewall blocks and prevents hacking attempt or attack from hackers

(*) From *Software Firewall Test Rankings, Matousec, 2014*

Free Internet?

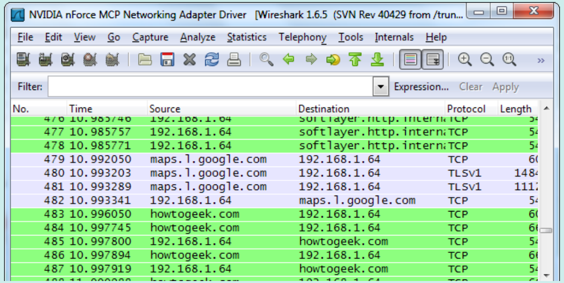
- Utilizing a public Wi-Fi access service or – worse – going to an Internet Cafe is dangerous even accessing to protected web which make use of SSL
- There're several serious problems when using a public Wi-Fi network:
  - The open nature of the network facilitates snooping (interceptions)
  - Compromised machines could be connected
  - Even more alarming – the hotspot itself could be dangerous

Never use a public Wi-Fi network for online banking or any other confidential activity!

ISACA®
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Free Internet?

- **Snooping**
  - When connecting to an open Wi-Fi network as in a bar or in an airport, the network is generally not encrypted - in fact it is not necessary to enter a personal password upon connection. The traffic is thus clearly visible to all
  - Software as Firesheep or Wireshark allow you to easily view web sessions of other users and capture and analyze network traffic


NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

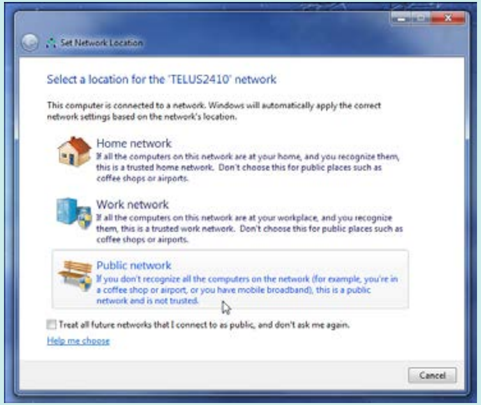
No.	Time	Source	Destination	Protocol	Length
476	10.985746	192.168.1.64	softlayer.http.intern	TCP	54
477	10.985757	192.168.1.64	softlayer.http.intern	TCP	54
478	10.985771	192.168.1.64	softlayer.http.intern	TCP	54
479	10.992050	maps.l.google.com	192.168.1.64	TCP	6
480	10.993203	maps.l.google.com	192.168.1.64	TLSv1	148
481	10.993289	maps.l.google.com	192.168.1.64	TLSv1	111
482	10.993341	192.168.1.64	maps.l.google.com	TCP	54
483	10.996050	howtogeek.com	192.168.1.64	TCP	6
484	10.997745	howtogeek.com	192.168.1.64	TCP	6
485	10.997800	192.168.1.64	howtogeek.com	TCP	54
486	10.997894	howtogeek.com	192.168.1.64	TCP	6
487	10.997919	192.168.1.64	howtogeek.com	TCP	54

Protections

1. *Only connect to sites that use cryptography*
2. *The browser extension "HTTPS Everywhere" can help to force the routing of the connection toward the protected pages when available*
3. *Use a reliable VPN (fee)*

Free Internet?

- **Compromised devices**
  - To the public network can be connected compromised devices which may start attacks against our system
  - The presence of viruses, spyware and other malicious software is constant in public Wi-Fi networks



Select a location for the 'TELUS2410' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.

□ Treat all future networks that I connect to as public, and don't ask me again.

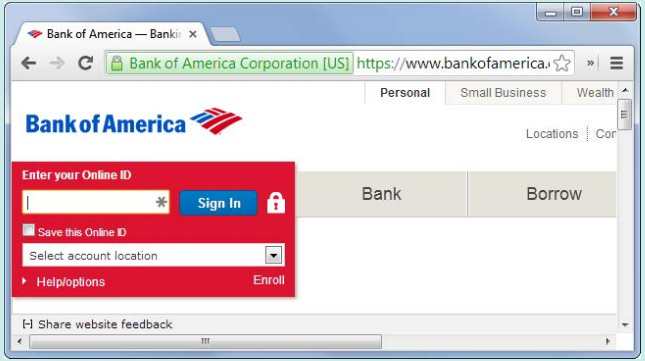
Help me choose

Protections

1. *Select the option "public network" when you connect*
2. *Verify that our computer is up to date*
3. *Enable the internal Personal Firewall (at least the Windows internal, if we don’t have bought one more reliable)*

Free Internet?

- **Malicious hotspot**
  - This may be due to the fact that the hotspot system has been compromised
  - We may be connected to a false network (honeypots). If you are connecting to a Wi-Fi "public", you cannot be completely certain that the network is the legitimate one and not a created in art by an attacker
  - Software like **sslstrip** can intercept transparently HTTP sessions
  - **WiFi Pineapple** is an easy-to-use device that allows you to achieve this type of attack



Protections

1. *Do not perform online banking or treat sensitive data, even if the sites use Encryption HTTP*
2. *Use a reliable VPN (not fee)*

ISACA
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Secure Messaging

- Even if messaging services such as **WhatsApp** and **iMessage** - after many insistence by users – to use encryption to protect the conversations, they are still insecure in other ways
  - WhatsApp, for example, maintains the metadata relating to our conversations (that include date, time-stamp, and phone numbers involved), and share user information with its parent application Facebook

Ricochet is a different approach to instant messaging that doesn't trust anyone in protecting your privacy

- Eliminate metadata. Nobody knows who you are, who you talk to, or what you say
- Stay anonymous
- Share what you want, without sharing your identity and location
- Nobody in the middle. There are no servers to monitor, censor, or hack
- Safe by default. Security isn't secure until it's automatic and easy to use

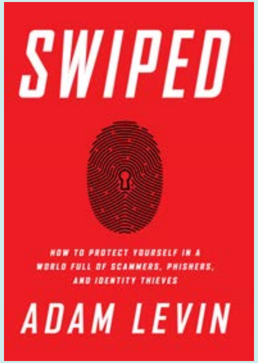
Chat with your friends, securely

Cryptocat is free software with a simple mission: everyone should be able to chat with their friends in privacy

- *Open source. All Cryptocat software is published transparently*
- *Encrypted by default. Every message is encrypted, always*
- *Forward secure. Chats are safe even if your keys are stolen*
- *Multiple devices. Devices receive messages even when offline*
- *File sharing. Securely share files with friends.*

Safe use of social media

- *“I was just doing it to tease her, basically.” It was a harmless tweet. A girl named Brooklyn from Prosper, Texas, sent a picture to her friend Alanna in reply to one of many tweets about a cute boy Alanna had seen while shopping at a big-box store in nearby Frisco. Then something fundamentally unknowable happened: the mysterious Internet phenomenon of going viral. … In the world of Big Data, with mobile, Internet-connected cameras in every pocket, we are always just a few clicks away from being everywhere. The young man whose picture went viral got a real-life taste of that fact when his total lack of privacy became apparent; he became an Internet sensation by doing nothing but bagging products at the checkout counter.*
- Adam Levin, “Swiped”, ed. Public Affairs, NY, 2015


SWIPED
HOW TO PROTECT YOURSELF IN A WORLD FULL OF SCAMMERS, PHISHERS, AND IDENTITY THIEVES
ADAM LEVIN

Help to protect our online identity

Apply these privacy settings to control what the most popular websites in the world know us:

Facebook

Facebook has a tendency to constantly change privacy settings without informing the users (Https://www.theguardian.com/technology/2016/jun/29/facebook-privacy-secret-profile-exposed). These simple elements lock our data and will guide us toward a safer navigation!

1. **Exit the targeted advertising**(**https://www.facebook.com/ads/preferences/edit/**).
   – Between memes and status (which we denote as 'like')(it's alarming to see how many things Mark Zuccurberg knows about us!
2. **Carry out the privacy checkup**(**https://www.facebook.com/about/basics**)
   – It is a reliable tool to check the privacy settings of Facebook, especially if we are at the beginning of the journey of customization. With this process, made up of three steps, you can control who can see our post and which applications have access to the data of our profile.
3. **Spend a little time with the control panel**
   – Do not make mistakes: the checkup tool is not robust like the entire Privacy Settings & Tools panel of Facebook (**https://www.facebook.com/settings? tab=privacy**). It can be a little difficult at the beginning, but it is worth spending five minutes to become familiar with it.

Help to protect our online identity

Google

The company, whose name is synonymous with "research", was notable for its share of the security problems (https://www.thrillist.com/news/nation/gooligan-malware-hack-13 million-google-account) and delays in fixing them. Better check if our email account has been violated (Https://haveibeenpwned.com/) because one of their recent security flaws.

4. **Complete the Google Security Checkup (https://myaccount.google.com/privacycheckup)**
   - The checkup of Google Security offers a great way to verify that recovery information is current and that applications and web sites linked to our account are those that still you still use and trust.
5. **Review the settings on advertising** (**https://myaccount.google.com/intro/privacy#ads/**)
   - The settings on the ads in Google does not offer the possibility to disable them as in Facebook. But allow you to deactivate the customization.
6. **”Let’s take control" of privacy settings** (**https://privacy.google.com/take-control.html**)
   - The Google privacy settings page of Google is as a glossary of the individual setup pages on privacy. From the history of the YouTube videos you have watched, to tracking with your mobile phone on maps, this is the best place to start the block of private data that we share with Google.

Help to protect our online identity

Amazon

Last year, a security breach (http://www.dailydot.com/debug/amazon-hack-80000-passwords-usernames/) made the information more than 80,000 customers of Amazon compromised. From here the hope that the data users are ultra secure in the near future made of "delivery-drones"…

7. **Keep the list(s) of secret desires**
   - Surprise! If we were already aware, it is good to know that the wish list at Amazon is public for all, unless we hide it. Fortunately this can be accomplished easily in the List Manager of Amazon (**https://www.amazon.com/gp/registry/side/manage/ref=cm_wl_mng_lists_nojs**).

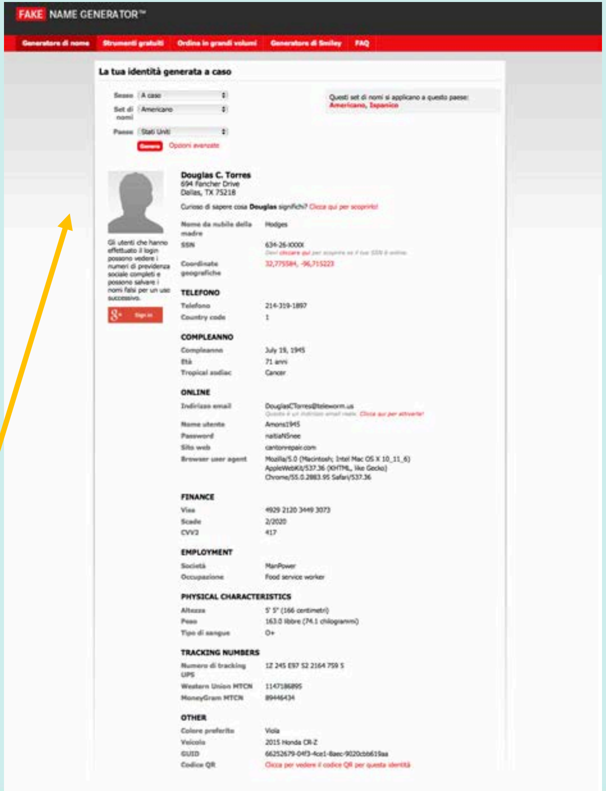
8. **Bring your own identity**
   - There is a bit of work to do for the privacy if we left the parameters of our profile on Amazon as default:
     1. Edit our profile (**https://www.amazon.com/profile**) so that the public reviews do not bring our full name;
     2. Go to 'edit privacy settings' (https://www.amazon.com/gp/profile/amzn1.account.AGBUQJ4BEKOGSC266MXRVQZAI5XQ/edit_public_activity_settings#)'and verify the data that we wish to share: by someone to all.

Real identity?

- Remember to always treat personal data as if they were money, because someone else is making money from them

Privacy is a value, protect our online data!

By the way: it is really necessary to always provide our real data?!



FAKE NAME GENERATOR™

La tua identità generata a caso

Sesso: A caso
Set di nomi: Americano
Paese: Stati Uniti

Questi set di nomi si applicano a questo paese: **Americano, Ispanico**

Gli utenti che hanno effettuato il login possono vedere i numeri di previdenza sociale completi e possono salvare i nomi falsi per un uso successivo.

Douglas C. Torres
694 Fancher Drive
Dallas, TX 75218

Curioso di sapere cosa **Douglas** significhi? Clicca qui per scoprirlo!

Nome da nubile della madre	Hodges
SSN	634-26-XXXX Devi cliccare qui per scoprire se il tuo SSN è online.
Coordinate geografiche	32,775584, -96,715223
TELEFONO	
Telefono	214-319-1897
Country code	1
COMPLEANNO	
Compleanno	July 19, 1945
Età	71 anni
Tropical zodiac	Cancer
ONLINE	
Indirizzo email	DouglasCTorres@teleworm.us Questo è un indirizzo email reale. Clicca qui per attivarlo!
Nome utente	Amons1945
Password	naitiaNSnee
Sito web	cantonrepair.com
Browser user agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36
FINANCE	
Visa	4929 2120 3449 3073
Scade	2/2020
CVV2	417
EMPLOYMENT	
Società	ManPower
Occupazione	Food service worker
PHYSICAL CHARACTERISTICS	
Altezza	5' 5" (166 centimetri)
Peso	163.0 libbre (74.1 chilogrammi)
Tipo di sangue	O+
TRACKING NUMBERS	
Numero di tracking UPS	1Z 245 E97 52 2164 759 5
Western Union MTCN	1147186895
MoneyGram MTCN	89446434
OTHER	
Colore preferito	Viola
Veicolo	2015 Honda CR-Z
GUID	66252679-04f3-4ce1-8aec-9020cbb619aa
Codice QR	Clicca per vedere il codice QR per questa identità

Awareness & Training

- Human factor is the weakest link of the security chain
  - Implementation of virus protection, firewalls, and content filtering technologies **may help** to control risk factors;
  - Careless or superficial user behavior **compromises** network security
  - User training is a **key measure** for network security strategy

Personnel awareness contributes to:

- safety and privacy of corporate information
- use of the Internet and the associated risks: dialer, Trojan horses, spyware, ransomware, etc.

ISACA®
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Thanks for your attention!

ISACA®

AI servizio dei professionisti dell'IT Governance

Rome Chapter

Questions?

ISACA®

Al servizio dei professionisti dell'IT Governance

Rome Chapter