UNIVERSITY OF TRENTO - Italy

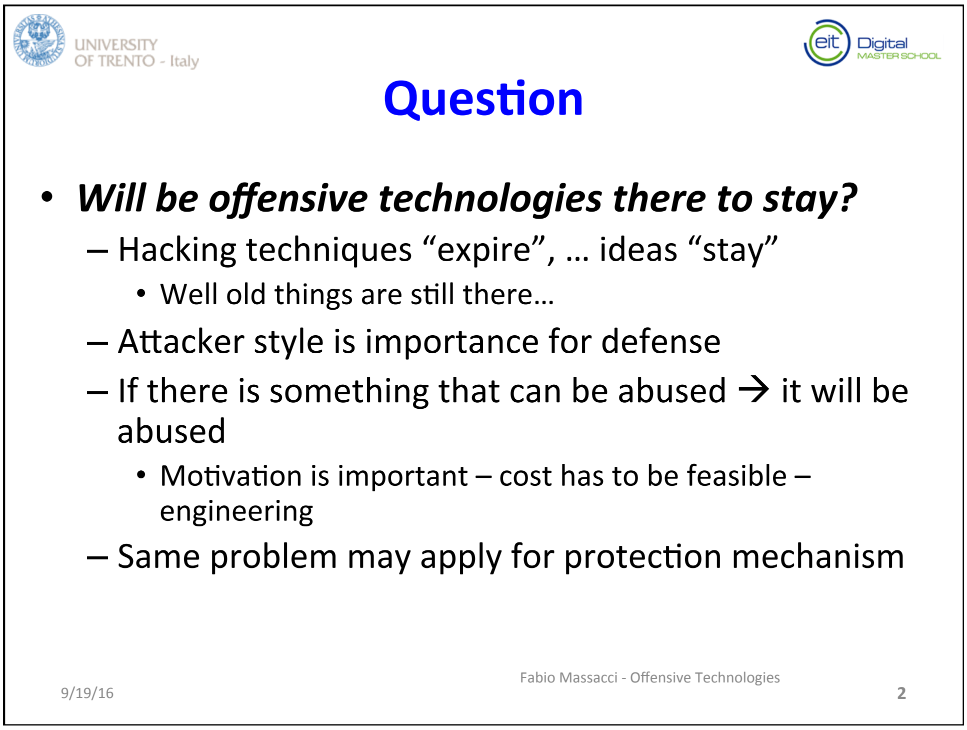
eit Digital MASTER SCHOOL

Offensive technologies
Fall 2016

Lecture 1

Introduction

Fabio Massacci



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Question

- ***Will be offensive technologies there to stay?***
  - Hacking techniques “expire”, … ideas “stay”
    - Well old things are still there…
  - Attacker style is importance for defense
  - If there is something that can be abused → it will be abused
    - Motivation is important – cost has to be feasible – engineering
  - Same problem may apply for protection mechanism

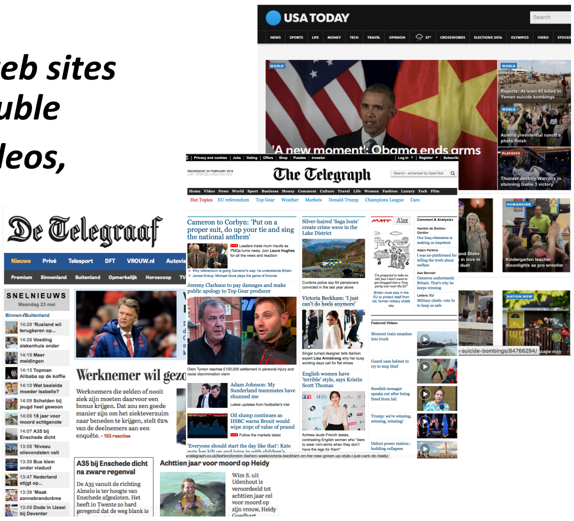
Do you trust these organisations?

- ***S-TRUST Authentication and Encryption Root***
  - Deutscher Sparkassen Verlag GmbH, Stuttgart, Baden-Wuerttemberg (DE)
- ***NetLock Kozjegyzoi Tanusitvanykiado***
  - Tanusitvanykiadok, NetLock Halozatbiztonsagi Kft., Budapest, Hungary
- ***TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı***
  - Bilgiİletişim ve Bilişim Güvenliği Hizmetleri A.Ş. ANKARA, Turkey
- ***CA 沃通根证书***
  - WoSign CA Limited, China

- ***To guarantee that a website is really what it claims to be?***

So, what’s that?

- ***It is just some web sites without any trouble***
- ***just pictures, videos, and text***

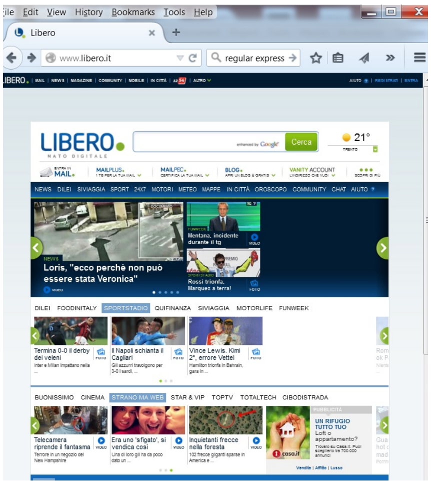

USA TODAY
'A new moment': Obama ends arms
The Telegraph
De Telegraaf
SNELNIEUWS
Werknemer wil gezo
A35 bij Enschede dicht na zware regenval
Achttien jaar voor moord op Heidy

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What's this?

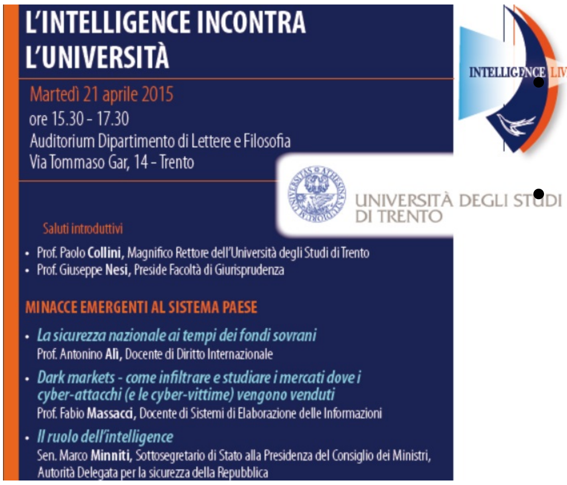
- ***ONE webpage***
  - Plenty of ads
- ***Process***
  - We DON'T look at the ads
  - Only click on mail
- ***And download the program of the infosec conference***


File Edit View History Bookmarks Tools Help
Libero
www.libero.it
regular express
LIBERO
NATO DIGITALE
Cerca
21°
MAIL
NEWS DILEI SIVIAGGIA SPORT 24x7 MOTORI METEO MAPPE IN CITTÀ OROSCOPO COMMUNITY CHAT AUTO
Loris, "ecco perché non può essere stata Veronica"
Mentana, incidente durante il tg
Rossi trionfa, Marquez a terra!
DILEI FOODINITALY SPORTSTADIO QUIFINANZA SIVIAGGIA MOTORLIFE FUNWEEK
Termina 0-0 il derby dei veleni
Il Napoli schianta il Cagliari
Vince Lewis. Kimi 2°, errore Vettel
BUONISSIMO CINEMA STRANO MA WEB STAR & VIP TOPTV TOTALTECH CIBODISTRADA
Telecamera riprende il fantasma
Era uno 'sfigato', si vendica così
Inquietanti frecce nella foresta
UN RIFUGIO TUTTO TUO

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What's this?



L'INTELLIGENCE INCONTRA L'UNIVERSITÀ

Martedì 21 aprile 2015
ore 15.30 - 17.30
Auditorium Dipartimento di Lettere e Filosofia
Via Tommaso Gar, 14 - Trento

Saluti introduttivi

- Prof. Paolo **Collini**, Magnifico Rettore dell'Università degli Studi di Trento
- Prof. Giuseppe **Nesi**, Preside Facoltà di Giurisprudenza

MINACCE EMERGENTI AL SISTEMA PAESE

- *La sicurezza nazionale ai tempi dei fondi sovrani*
  Prof. Antonino **Ali**, Docente di Diritto Internazionale
- *Dark markets - come infiltrare e studiare i mercati dove i cyber-attacchi (e le cyber-vittime) vengono venduti*
  Prof. Fabio **Massacci**, Docente di Sistemi di Elaborazione delle Informazioni
- *Il ruolo dell'intelligence*
  Sen. Marco **Minniti**, Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri, Autorità Delegata per la sicurezza della Repubblica

- ONE PDF file, essentially an image
- What happens if we open it?
  - Nothing
  - Acrobat Reader shows the image on the monitor

What's this?

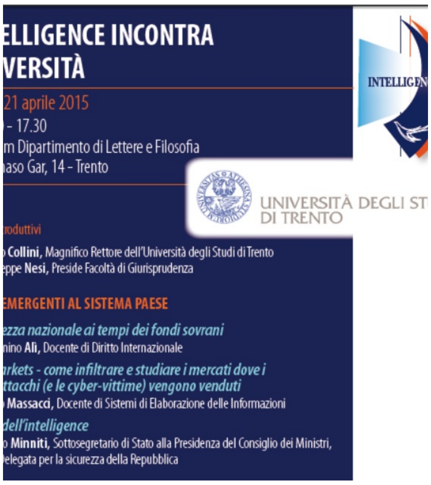
- *A photocopier*
- *A printer*
- *You send a file, and it prints*

What *really is* this? Just like that!

Xerox computer to just print a file:
Intel Celeron - 733 MHZ – 128MB

NASA computer to land Apollo 16 to the Moon
AGC – 1 MHz – 4KB RAM

What *really* is this?



ELLIGENCE INCONTRA
VERSITÀ
21 aprile 2015
- 17.30
m Dipartimento di Lettere e Filosofia
aso Gar, 14 - Trento

UNIVERSITÀ DEGLI ST
DI TRENTO

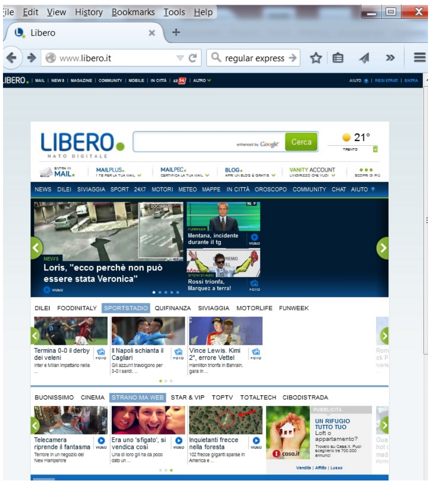
roduttivi
Collini, Magnifico Rettore dell'Università degli Studi di Trento
eppe Nesi, Preside Facoltà di Giurisprudenza

EMERGENTI AL SISTEMA PAESE
ezza nazionale ai tempi dei fondi sovrani
nino Alì, Docente di Diritto Internazionale
arkets - come infiltrare e studiare i mercati dove i
ttacchi (e le cyber-vittime) vengono venduti
Massacci, Docente di Sistemi di Elaborazione delle Informazioni
dell'intelligence
Minniti, Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri,
elegata per la sicurezza della Repubblica

- ***That's a program containing***
  - at least 1682 instructions
- ***What happens when we open it?***
  - All instructions are executed
  - Not necessarily true that the result is displayed
- ***PDF language is Turing Complete***
  - ANY function can be written in PDF language
  - Opening a PDF file can seamlessly display an image and simultaneously solve Fermat's little theorem

What *really* is this?

- ***When we type www.libero.it on the browser, YOUR computer will:***
- ***Execute***
  - 186 local functions
  - 15 functions from ***external*** sites
- ***Aggregate static contents from***
  - 676 websites of which
  - 370 external websites
  - 193 may be just images
- ***Aggregate dynamic content from***
  - 8 advertisers (at least)
- ***Are all of these actions "good" ones?***



File Edit View History Bookmarks Tools Help
Libero
www.libero.it
regular express
LIBERO. MAIL NEWS MAGAZINE COMMUNITY MOBILE IN CITTÀ ALTRO
AIUTO REGISTRATI ENTRA
LIBERO. NATO DIGITALE
enhanced by Google
Cerca
21°
TRENTO
ENTRA IN MAIL.
MAILPLUS. 1 TB PER LA TUA MAIL
MAILPEC. CERTIFICA LA TUA MAIL
BLOG. APRI UN BLOG È GRATIS
VANITY ACCOUNT L'INDIRIZZO CHE VUOI
SCOPRI DI PIÙ
NEWS DILEI SIVIAGGIA SPORT 24X7 MOTORI METEO MAPPE IN CITTÀ OROSCOPO COMMUNITY CHAT AIUTO
DILEI FOODINITALY SPORTSTADIO QUIFINANZA SIVIAGGIA MOTORLIFE FUNWEEK
BUONISSIMO CINEMA STRANO MA WEB STAR & VIP TOPTV TOTALTECH CIBODISTRADA
PUBBLICITÀ
casa.it
Vendita | Affitto | Lusso

NEWS Loris, "ecco perchè non può essere stata Veronica" VIDEO

FUNWEEK Mentana, incidente durante il tg VIDEO

SPORTSTADIO Rossi trionfa, Marquez a terra! FOTO

Termina 0-0 il derby dei veleni FOTO
Inter e Milan impattano nella ...

Il Napoli schianta il Cagliari FOTO
Gli azzurri travolgono per 3-0 i sardi, ...

Vince Lewis. Kimi 2°, errore Vettel FOTO
Hamilton trionfa in Bahrain, gara in ...

Telecamera riprende il fantasma VIDEO
Terrore in un negozio del New Hampshire

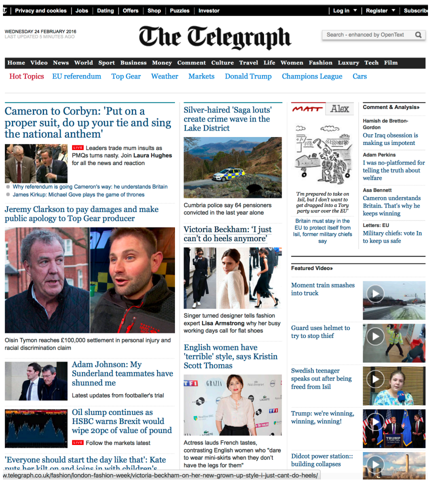
Era uno 'sfigato', si vendica così VIDEO
Una di loro gli ha da poco dato un ...

Inquietanti frecce nella foresta VIDEO
102 frecce giganti sparse in America e ...

UN RIFUGIO TUTTO TUO
Loft o appartamento?
Trovalo su Casa.it. Puoi sceglierlo tra 700.000 annunci

Cyberlife is never what it seems - UK

- *What it REALLY is*
- ***~~It is ONE web site without any trouble just picture and text~~***
- ***12 web trackers for advertising***
- ***72 javascript snips executed by your browser while you load it***
- ***More than 100 references to different sites, some of them executing code***
  - http://player.ooyala.com
  - http://widget.cloud.opta.net
  - Some of them dynamically created on the fly e.g. by b.scorecardresearch.com
- ***>100 errors/warnings in processing***
- ***How can you tell what's good what's bad?***



The Telegraph

Cameron to Corbyn: 'Put on a proper suit, do up your tie and sing the national anthem'

Silver-haired 'Saga louts' create crime wave in the Lake District

Jeremy Clarkson to pay damages and make public apology to Top Gear producer

Victoria Beckham: 'I just can't do heels anymore'

English women have 'terrible' style, says Kristin Scott Thomas

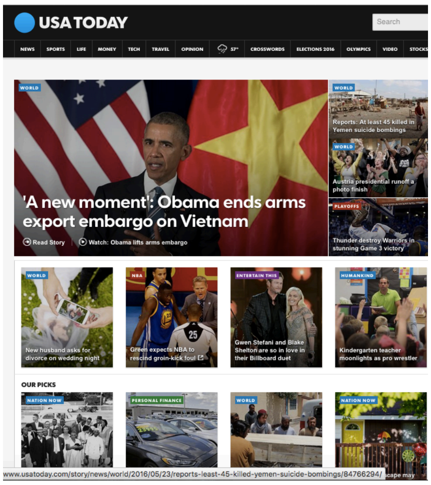
Adam Johnson: My Sunderland teammates have shunned me

Oil slump continues as HSBC warns Brexit would wipe 20pc of value of pound

Privacy and cookies | Jobs | Dating | Offers | Shop | Puzzles | Investor
Log in | Register | Subscribe
Home Video News World Sport Business Money Comment Culture Travel Life Women Fashion Luxury Tech Film
Hot Topics EU referendum Top Gear Weather Markets Donald Trump Champions League Cars
Featured Video

Cyberlife is never what it seems - US

- *What it REALLY is*
- ***~~It is ONE web site without any trouble just picture and text~~***
- ***8 web trackers for advertising***
- ***122 javascript snips executed by your browser <u>before</u> you see anything***
- ***More than 500 references to external sites, many executing code***
  - Garretn-cdn.com
  - Brightcove.com
  - Tags.tiqcdn.com
- ***>164 errors/warnings processing web page***
- ***How can you tell good from bad?***
- ***And I didn't load Flash, sorry …***



USA TODAY

'A new moment': Obama ends arms export embargo on Vietnam

Reports: At least 45 killed in Yemen suicide bombings

Austria presidential runoff a photo finish

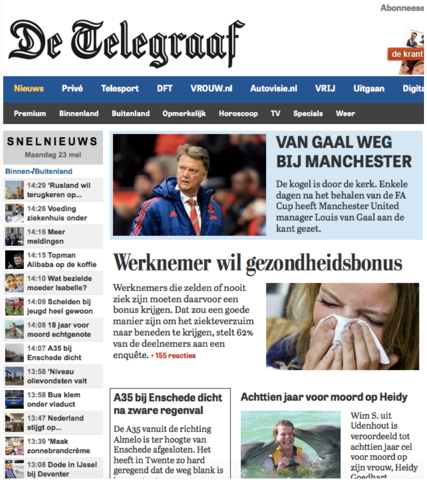
Thunder destroy Warriors in stunning Game 3 victory

NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION CROSSWORDS ELECTIONS 2016 OLYMPICS VIDEO STOCKS
Search
Read Story
Watch: Obama lifts arms embargo
OUR PICKS

www.usatoday.com/story/news/world/2016/05/23/reports-least-45-killed-yemen-suicide-bombings/84766294/

Cyberlife is never what it seems - NL

- *What it REALLY is*
- ~~*It is ONE web site without any trouble just picture and text*~~
- *13 web trackers for advertising*
- *207 javascript snips executed by your browser before you see anything!*
- *> 200 references to different sites, some of them executing code*
  - Easypoll
  - Hotjar
  - Tiq
- *>100 errors/warnings in processing the web page*
- *How can you tell good vs bad?*
- *And they wanted me to disable the adblocker! Sorry mates…*



SNELNIEUWS
Maandag 23 mei

Binnen-/Buitenland

14:29 'Rusland wil terugkeren op...

14:26 Voeding ziekenhuis onder

14:16 Meer meldingen

14:15 Topman Alibaba op de koffie

14:10 Wat bezielde moeder Isabelle?

14:09 Schelden bij jeugd heel gewoon

14:08 18 jaar voor moord echtgenote

14:07 A35 bij Enschede dicht

13:58 'Niveau olievondsten valt

13:58 Bus klem onder viaduct

13:47 Nederland stijgt op...

13:39 'Maak zonnebrandcrème

13:08 Dode in IJssel bij Deventer

VAN GAAL WEG BIJ MANCHESTER

De kogel is door de kerk. Enkele dagen na het behalen van de FA Cup heeft Manchester United manager Louis van Gaal aan de kant gezet.

Werknemer wil gezondheidsbonus

Werknemers die zelden of nooit ziek zijn moeten daarvoor een bonus krijgen. Dat zou een goede manier zijn om het ziekteverzuim naar beneden te krijgen, stelt 62% van de deelnemers aan een enquête. • 155 reacties

A35 bij Enschede dicht na zware regenval

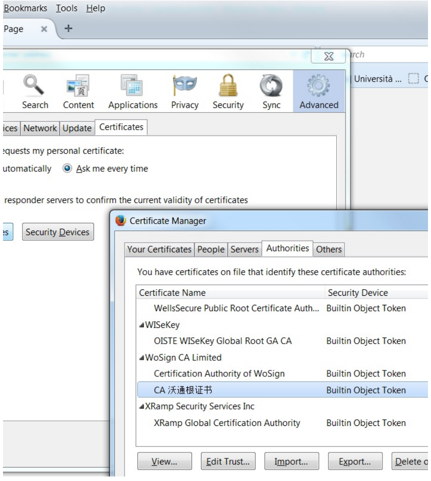
De A35 vanuit de richting Almelo is ter hoogte van Enschede afgesloten. Het heeft in Twente zo hard geregend dat de weg blank is

Achttien jaar voor moord op Heidy

Wim S. uit Udenhout is veroordeeld tot achttien jaar cel voor moord op zijn vrouw, Heidy Goedhart

Who trusts these? Everybody.

- ***S-TRUST Authentication and Encryption Root***
  - Deutscher Sparkassen Verlag GmbH, Stuttgart, Baden-Wuerttemberg (DE)
- ***NetLock Kozjegyzoi Tanusitvanykiado***
  - Tanusitvanykiadok, NetLock Halozatbiztonsagi Kft., Budapest, Hungary
- ***TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı***
  - Bilgiİletişim ve Bilişim Güvenliği Hizmetleri A.Ş. ANKARA, Turkey
- ***沃通根证书***
  - WoSign CA Limited, China



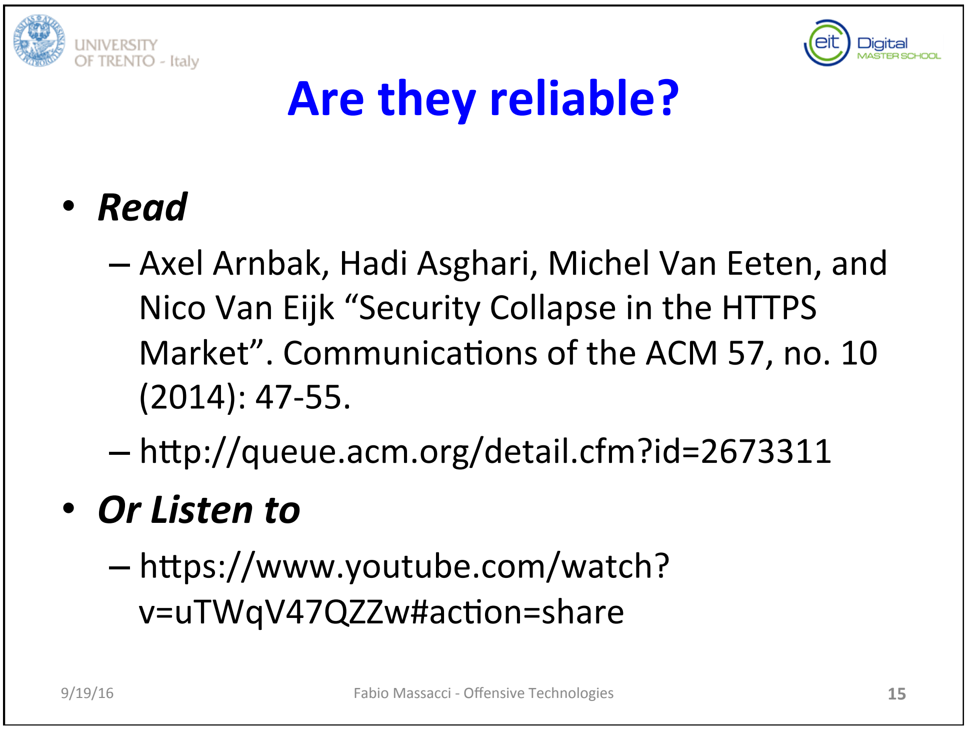
equests my personal certificate:

utomatically ● Ask me every time

responder servers to confirm the current validity of certificates

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
WellsSecure Public Root Certificate Auth...	Builtin Object Token
◢WISeKey	
OISTE WISeKey Global Root GA CA	Builtin Object Token
◢WoSign CA Limited	
Certification Authority of WoSign	Builtin Object Token
CA 沃通根证书	Builtin Object Token
◢XRamp Security Services Inc	
XRamp Global Certification Authority	Builtin Object Token



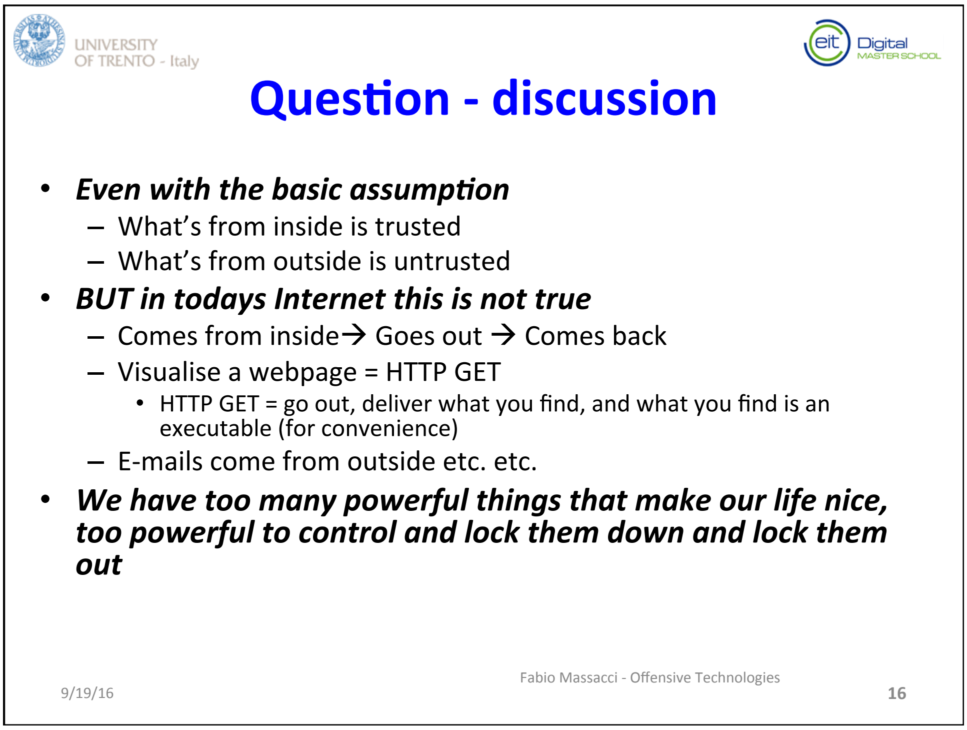
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Are they reliable?

- ***Read***
  - Axel Arnbak, Hadi Asghari, Michel Van Eeten, and Nico Van Eijk "Security Collapse in the HTTPS Market". Communications of the ACM 57, no. 10 (2014): 47-55.
  - http://queue.acm.org/detail.cfm?id=2673311
- ***Or Listen to***
  - https://www.youtube.com/watch?v=uTWqV47QZZw#action=share

9/19/16 Fabio Massacci - Offensive Technologies 15



UNIVERSITY OF TRENTO - Italy

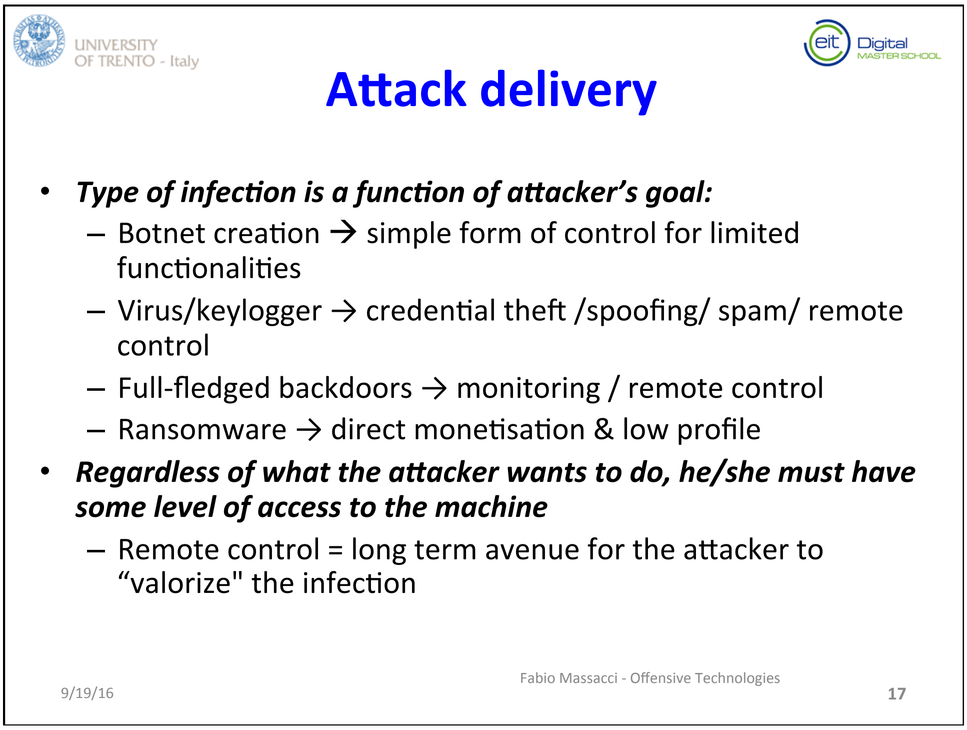
eit Digital MASTER SCHOOL

Question - discussion

- ***Even with the basic assumption***
  - What's from inside is trusted
  - What's from outside is untrusted
- ***BUT in todays Internet this is not true***
  - Comes from inside→ Goes out → Comes back
  - Visualise a webpage = HTTP GET
    - HTTP GET = go out, deliver what you find, and what you find is an executable (for convenience)
  - E-mails come from outside etc. etc.
- ***We have too many powerful things that make our life nice, too powerful to control and lock them down and lock them out***

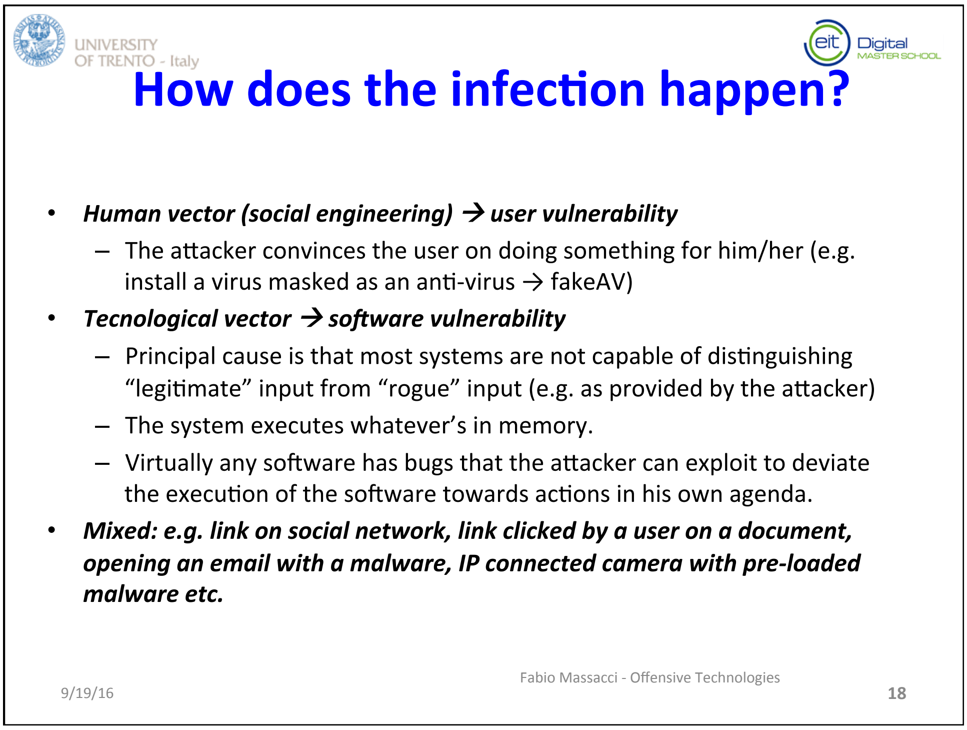
Fabio Massacci - Offensive Technologies

9/19/16 16



Attack delivery

- ***Type of infection is a function of attacker's goal:***
  - Botnet creation → simple form of control for limited functionalities
  - Virus/keylogger → credential theft /spoofing/ spam/ remote control
  - Full-fledged backdoors → monitoring / remote control
  - Ransomware → direct monetisation & low profile
- ***Regardless of what the attacker wants to do, he/she must have some level of access to the machine***
  - Remote control = long term avenue for the attacker to "valorize" the infection

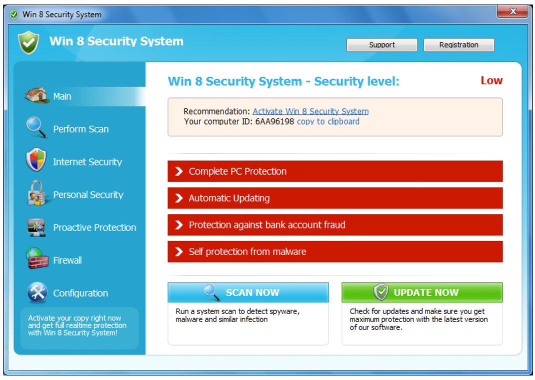


How does the infection happen?

- ***Human vector (social engineering) → user vulnerability***
  - The attacker convinces the user on doing something for him/her (e.g. install a virus masked as an anti-virus → fakeAV)
- ***Tecnological vector → software vulnerability***
  - Principal cause is that most systems are not capable of distinguishing "legitimate" input from "rogue" input (e.g. as provided by the attacker)
  - The system executes whatever's in memory.
  - Virtually any software has bugs that the attacker can exploit to deviate the execution of the software towards actions in his own agenda.
- ***Mixed: e.g. link on social network, link clicked by a user on a document, opening an email with a malware, IP connected camera with pre-loaded malware etc.***

Human vector: social engineering

- ***Attacker convinces the user to install a virus masked as a legitimate application***
- ***The example here is a fake antivirus product called "Win 8 Security System"***
  - User thinks it's actual AV
  - In reality it infects the system



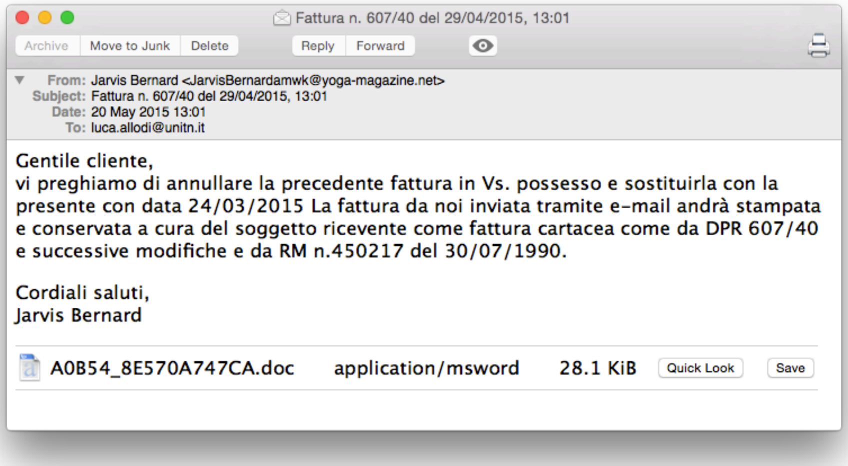
Recommendation: Activate Win 8 Security System
Your computer ID: 6AA96198 copy to clipboard

Activate your copy right now and get full realtime protection with Win 8 Security System!

Run a system scan to detect spyware, malware and similar infection

Check for updates and make sure you get maximum protection with the latest version of our software.

Example of attempted infection



Fattura n. 607/40 del 29/04/2015, 13:01

From: Jarvis Bernard <JarvisBernardamwk@yoga-magazine.net>
Subject: Fattura n. 607/40 del 29/04/2015, 13:01
Date: 20 May 2015 13:01
To: luca.allodi@unitn.it

Gentile cliente,
vi preghiamo di annullare la precedente fattura in Vs. possesso e sostituirla con la presente con data 24/03/2015 La fattura da noi inviata tramite e-mail andrà stampata e conservata a cura del soggetto ricevente come fattura cartacea come da DPR 607/40 e successive modifiche e da RM n.450217 del 30/07/1990.

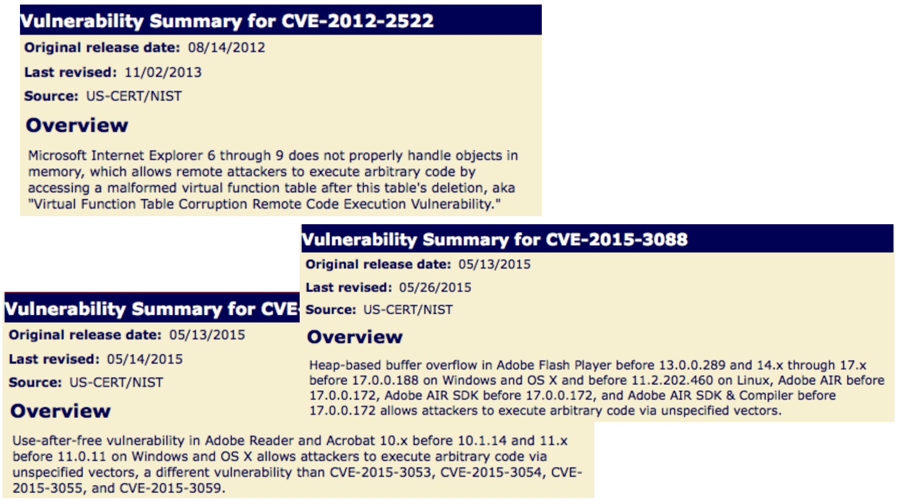
Cordiali saluti,
Jarvis Bernard

A0B54_8E570A747CA.doc application/msword 28.1 KiB

Technological vector

- ***The attack usually exploits some vulnerability in software***
- ***System is fed with computationally valid codes in input to a vulnerable software → code is executed***
- ***Several types of vulnerabilities***
  - XSS
  - Buffer overflow
  - SQLi
  - Privilege escalation
  - …
- ***More exercises and details in***
  - Network Security Course
  - Security Testing Course

Vulnerability examples



Vulnerability Summary for CVE-2012-2522

Original release date: 08/14/2012

Last revised: 11/02/2013

Source: US-CERT/NIST

Overview

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a malformed virtual function table after this table's deletion, aka "Virtual Function Table Corruption Remote Code Execution Vulnerability."

Vulnerability Summary for CVE-2015-3088

Original release date: 05/13/2015

Last revised: 05/26/2015

Source: US-CERT/NIST

Overview

Heap-based buffer overflow in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.

Vulnerability Summary for CVE

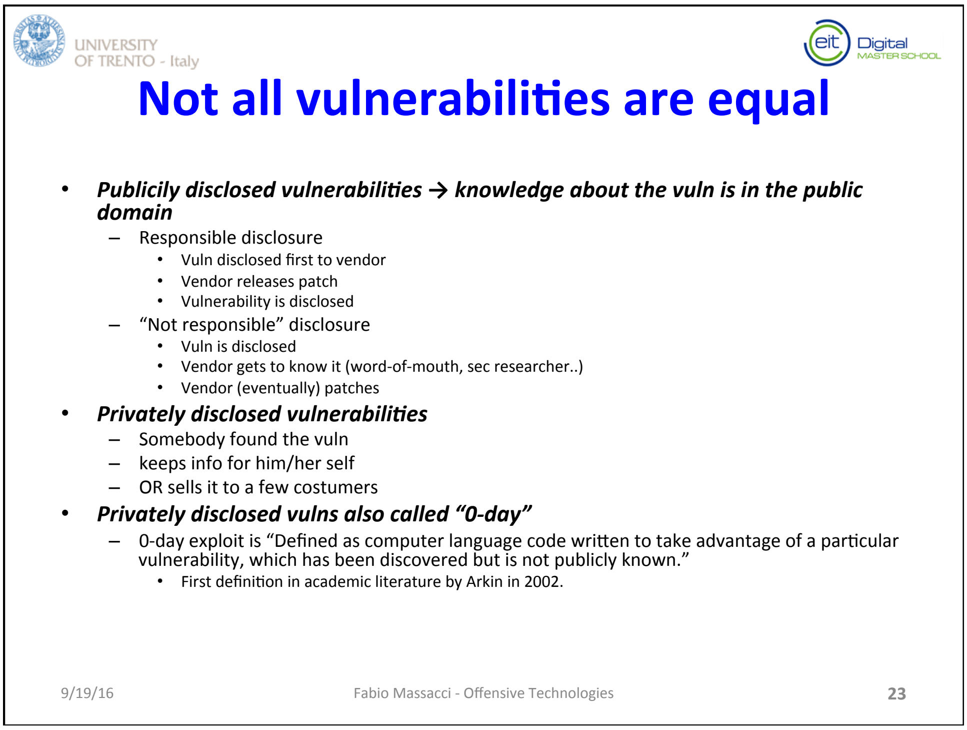
Original release date: 05/13/2015

Last revised: 05/14/2015

Source: US-CERT/NIST

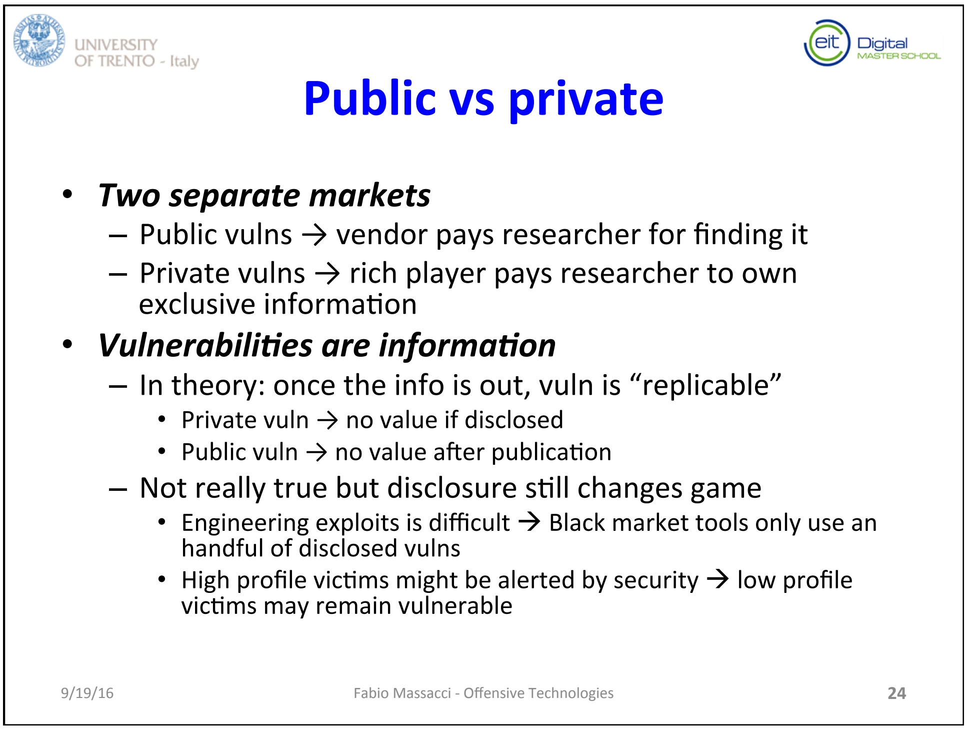
Overview

Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3053, CVE-2015-3054, CVE-2015-3055, and CVE-2015-3059.



Not all vulnerabilities are equal

- ***Publicily disclosed vulnerabilities → knowledge about the vuln is in the public domain***
  - Responsible disclosure
    - Vuln disclosed first to vendor
    - Vendor releases patch
    - Vulnerability is disclosed
  - “Not responsible” disclosure
    - Vuln is disclosed
    - Vendor gets to know it (word-of-mouth, sec researcher..)
    - Vendor (eventually) patches
- ***Privately disclosed vulnerabilities***
  - Somebody found the vuln
  - keeps info for him/her self
  - OR sells it to a few costumers
- ***Privately disclosed vulns also called “0-day”***
  - 0-day exploit is “Defined as computer language code written to take advantage of a particular vulnerability, which has been discovered but is not publicly known.”
    - First definition in academic literature by Arkin in 2002.



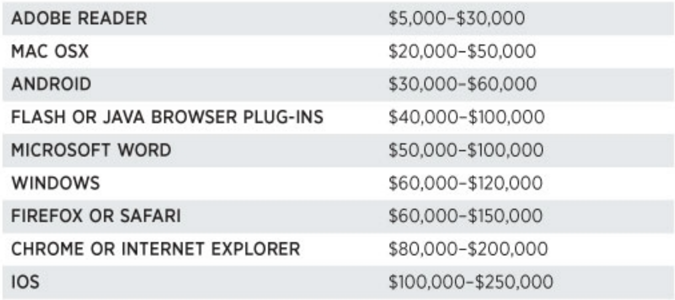
Public vs private

- ***Two separate markets***
  - Public vulns → vendor pays researcher for finding it
  - Private vulns → rich player pays researcher to own exclusive information
- ***Vulnerabilities are information***
  - In theory: once the info is out, vuln is “replicable”
    - Private vuln → no value if disclosed
    - Public vuln → no value after publication
  - Not really true but disclosure still changes game
    - Engineering exploits is difficult → Black market tools only use an handful of disclosed vulns
    - High profile victims might be alerted by security → low profile victims may remain vulnerable

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Alledged (1st time) price list for 0-days



ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

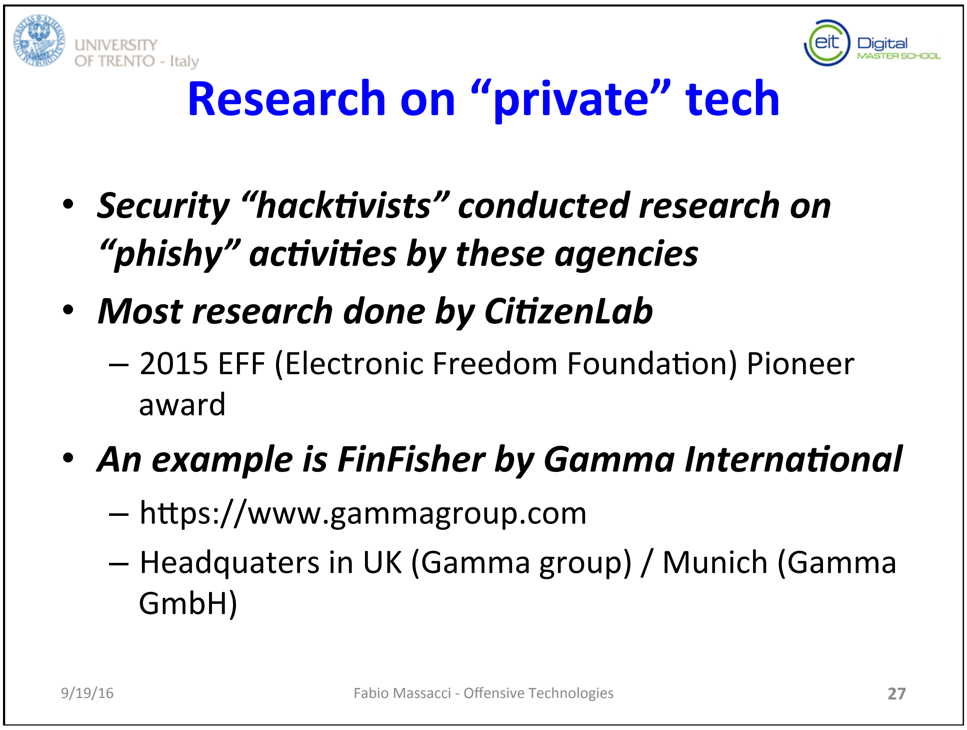
- ***http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

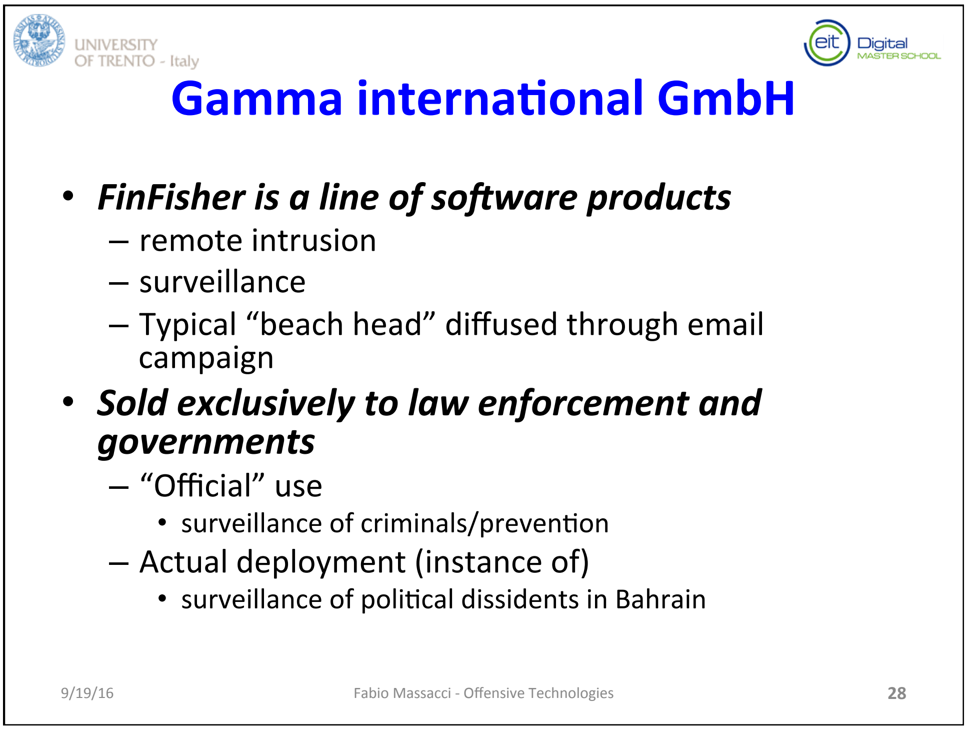
Who buys into these markets?

- ***Allegedly (2nd time), mostly governments***
- ***Ok, but from whom?***
- ***Allegedly (3rd time), from private agencies that sell malware and exploits to governments***
  - Which governments?
  - Mostly oppressive ones (yes, allegedly, 4th time)
- ***Sample of agency names***
  - VuPEN (used to be in France)
  - Gamma International (UK/Germany)
  - Hacking Team (Italy)



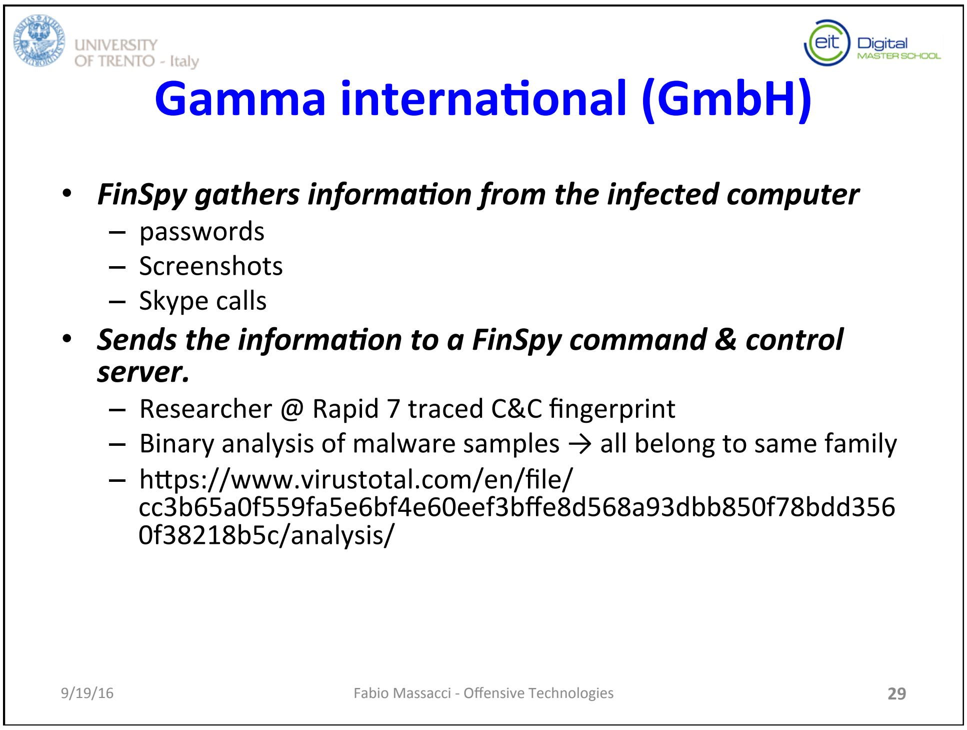
Research on “private” tech

- ***Security “hacktivists” conducted research on “phishy” activities by these agencies***
- ***Most research done by CitizenLab***
  - 2015 EFF (Electronic Freedom Foundation) Pioneer award
- ***An example is FinFisher by Gamma International***
  - https://www.gammagroup.com
  - Headquaters in UK (Gamma group) / Munich (Gamma GmbH)



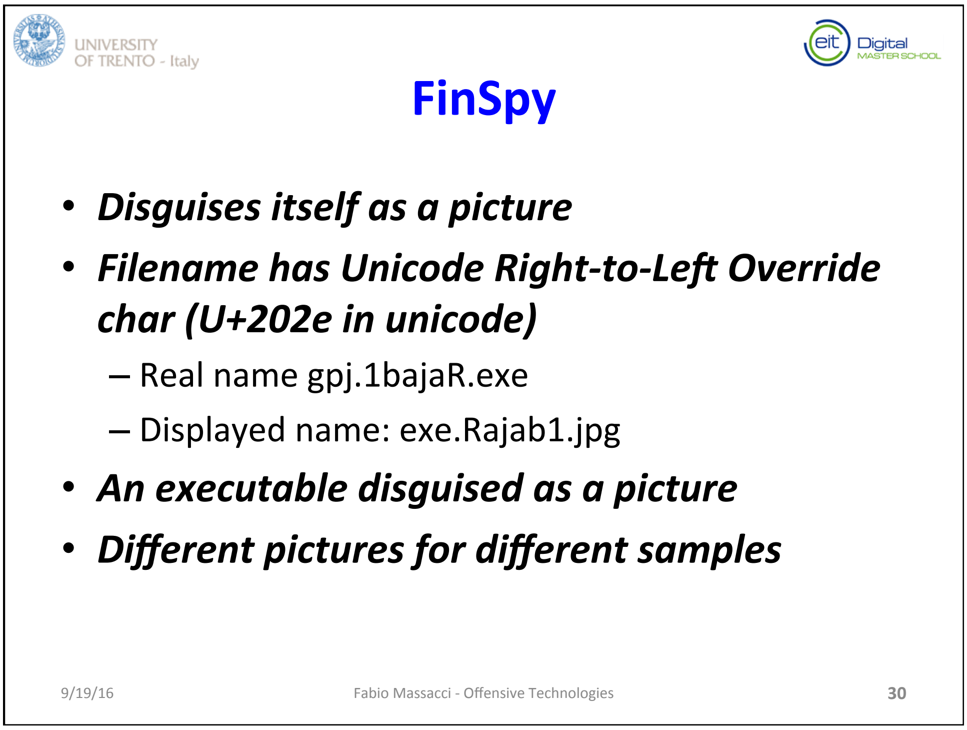
Gamma international GmbH

- ***FinFisher is a line of software products***
  - remote intrusion
  - surveillance
  - Typical “beach head” diffused through email campaign
- ***Sold exclusively to law enforcement and governments***
  - “Official” use
    - surveillance of criminals/prevention
  - Actual deployment (instance of)
    - surveillance of political dissidents in Bahrain



Gamma international (GmbH)

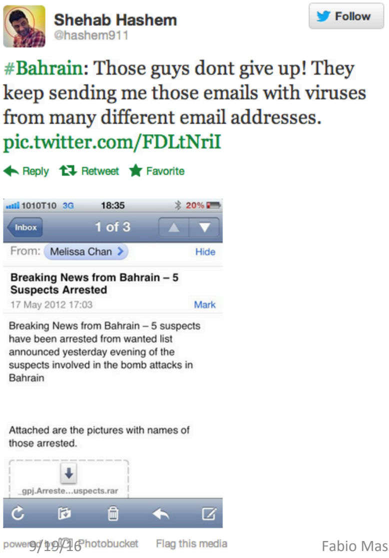
- ***FinSpy gathers information from the infected computer***
  - passwords
  - Screenshots
  - Skype calls
- ***Sends the information to a FinSpy command & control server.***
  - Researcher @ Rapid 7 traced C&C fingerprint
  - Binary analysis of malware samples → all belong to same family
  - https://www.virustotal.com/en/file/cc3b65a0f559fa5e6bf4e60eef3bffe8d568a93dbb850f78bdd3560f38218b5c/analysis/



FinSpy

- ***Disguises itself as a picture***
- ***Filename has Unicode Right-to-Left Override char (U+202e in unicode)***
  - Real name gpj.1bajaR.exe
  - Displayed name: exe.Rajab1.jpg
- ***An executable disguised as a picture***
- ***Different pictures for different samples***

FinSpy - delivery



Shehab Hashem
@hashem911

#Bahrain: Those guys dont give up! They keep sending me those emails with viruses from many different email addresses. pic.twitter.com/FDLtNriI

1010T10 3G 18:35 20%

Inbox 1 of 3

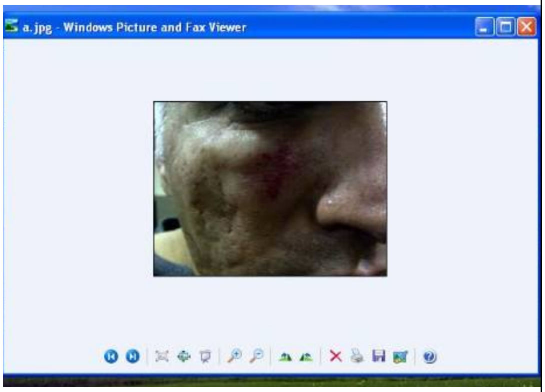
From: Melissa Chan

Breaking News from Bahrain – 5 Suspects Arrested
17 May 2012 17:03

Breaking News from Bahrain – 5 suspects have been arrested from wanted list announced yesterday evening of the suspects involved in the bomb attacks in Bahrain

Attached are the pictures with names of those arrested.

_gpj.Arreste...uspects.rar



FinSpy – Execution (1)

- ***Creates random dirname***
  - C:\DOCUME~1\User\LOCALS~1\Temp\ \TMP44D8C9F9
- ***Drops copy of itself and launches***
  - C:\DOCUME~1\User\LOCALS~1\Temp\\driverw.sys
  - Driver already seen in other samples of FinFisher malware
    - Functionality unknown
  - New random dir to store screenshots, logs, etc. to send to C&C

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

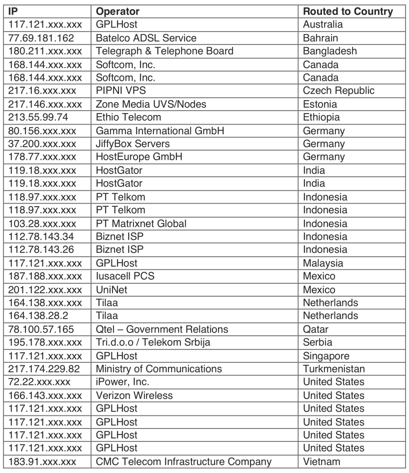
FinSpy – Execution (2)

- ***Actual malware functionality upon reboot***
- ***Injects itself in winlogon***
  - Spawns legitimate processes and then replaces code image with malicious one (process hollowing)
  - Hooks on several system functions
  - Catches call and sends data to C&C

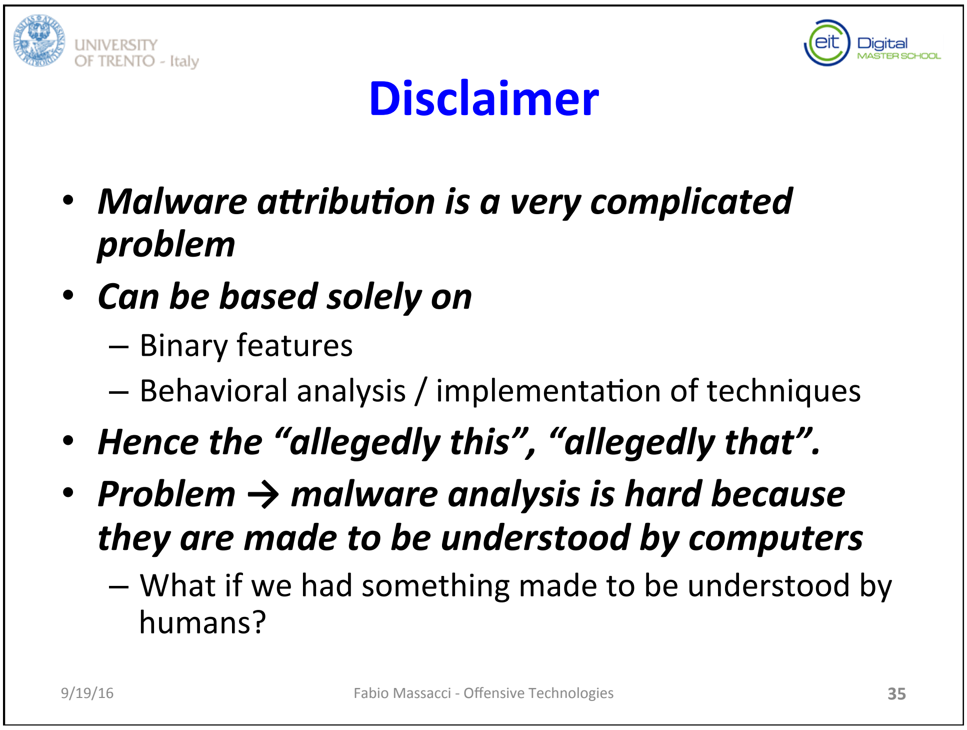
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Some C&C IPs

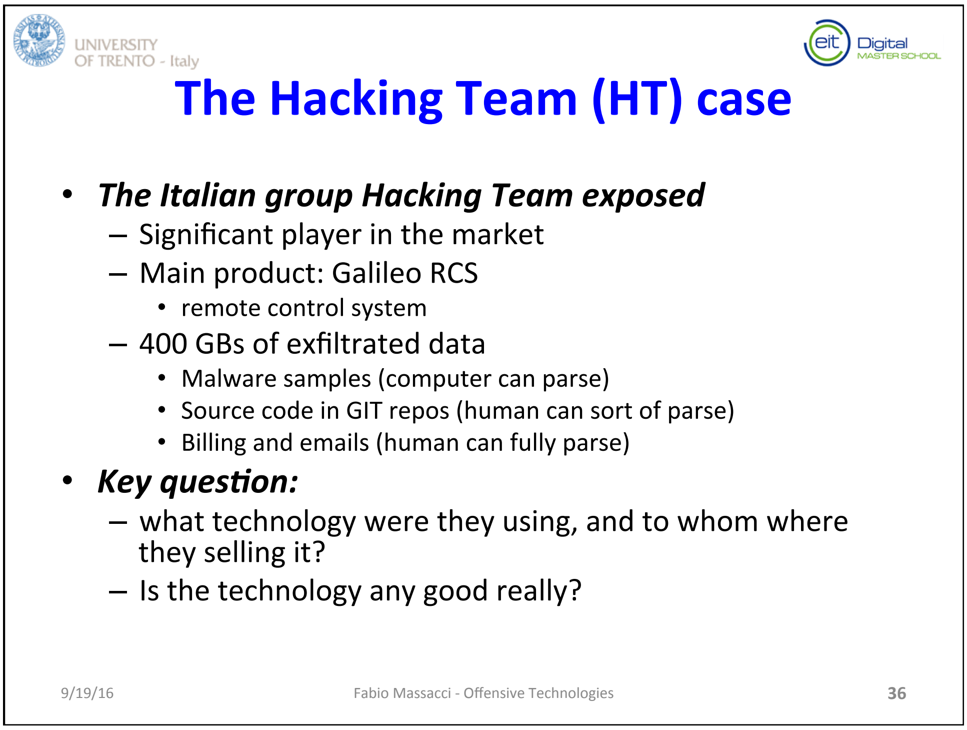


IP	Operator	Routed to Country
117.121.xxx.xxx	GPLHost	Australia
77.69.181.162	Batelco ADSL Service	Bahrain
180.211.xxx.xxx	Telegraph & Telephone Board	Bangladesh
168.144.xxx.xxx	Softcom, Inc.	Canada
168.144.xxx.xxx	Softcom, Inc.	Canada
217.16.xxx.xxx	PIPNI VPS	Czech Republic
217.146.xxx.xxx	Zone Media UVS/Nodes	Estonia
213.55.99.74	Ethio Telecom	Ethiopia
80.156.xxx.xxx	Gamma International GmbH	Germany
37.200.xxx.xxx	JiffyBox Servers	Germany
178.77.xxx.xxx	HostEurope GmbH	Germany
119.18.xxx.xxx	HostGator	India
119.18.xxx.xxx	HostGator	India
118.97.xxx.xxx	PT Telkom	Indonesia
118.97.xxx.xxx	PT Telkom	Indonesia
103.28.xxx.xxx	PT Matrixnet Global	Indonesia
112.78.143.34	Biznet ISP	Indonesia
112.78.143.26	Biznet ISP	Indonesia
117.121.xxx.xxx	GPLHost	Malaysia
187.188.xxx.xxx	Iusacell PCS	Mexico
201.122.xxx.xxx	UniNet	Mexico
164.138.xxx.xxx	Tilaa	Netherlands
164.138.28.2	Tilaa	Netherlands
78.100.57.165	Qtel – Government Relations	Qatar
195.178.xxx.xxx	Tri.d.o.o / Telekom Srbija	Serbia
117.121.xxx.xxx	GPLHost	Singapore
217.174.229.82	Ministry of Communications	Turkmenistan
72.22.xxx.xxx	iPower, Inc.	United States
166.143.xxx.xxx	Verizon Wireless	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
183.91.xxx.xxx	CMC Telecom Infrastructure Company	Vietnam



Disclaimer

- ***Malware attribution is a very complicated problem***
- ***Can be based solely on***
  - Binary features
  - Behavioral analysis / implementation of techniques
- ***Hence the “allegedly this”, “allegedly that”.***
- ***Problem → malware analysis is hard because they are made to be understood by computers***
  - What if we had something made to be understood by humans?



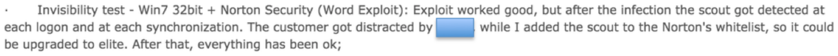
The Hacking Team (HT) case

- ***The Italian group Hacking Team exposed***
  - Significant player in the market
  - Main product: Galileo RCS
    - remote control system
  - 400 GBs of exfiltrated data
    - Malware samples (computer can parse)
    - Source code in GIT repos (human can sort of parse)
    - Billing and emails (human can fully parse)
- ***Key question:***
  - what technology were they using, and to whom where they selling it?
  - Is the technology any good really?

UNIVERSITY OF TRENTO - Italy

Governmental malware: is it that sophisticated?

- ***FinSpy malware is not particularly complex***
  - No polymorphism
  - Delivery mechanism == email attachment
- ***What is the actual sophistication of the technology developed and deployed by these players?***
- ***From the HT dump:***



· Invisibility test - Win7 32bit + Norton Security (Word Exploit): Exploit worked good, but after the infection the scout got detected at each logon and at each synchronization. The customer got distracted by [redacted] while I added the scout to the Norton's whitelist, so it could be upgraded to elite. After that, everything has been ok;

- ***"Good" guy distracts the victim while other guy whitelists the malware***
  - .. Lame
  - Is this really the nature of the game, or is there more to it?

UNIVERSITY OF TRENTO - Italy

Additional Readings

- ***First academic paper mentioning 0-days (that I know of)***
  - O. Arkin. "Tracing Hackers: Part 1." *Computers and Security*, 2002.
- ***Insight in the market***
  - C. Miller. The Legitimate Vulnerability Market. *Workshop on Economics of Information Security, 2006.*
  - Axel Arnbak, Hadi Asghari, Michel Van Eeten, and Nico Van Eijk "Security Collapse in the HTTPS Market". Communications of the ACM 57, no. 10 (2014): 47-55.
- ***Some different perspectives on cybercrime***
  - Nick Nykodym et al. "Criminal profiling and insider cyber crime." *Digital Investigation*, 2005.
  - D. Florencio et al. "Sex, Lies and Cybercrime Surveys". *Workshop on Economics of Information Security, 2006.*
  - J. Franklin. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants". *ACM Conference on Computer and Communication Security*, 2007
- ***A tutorial on the difficulty of attribution***
  - M. Marquis-Boire. Big Game Hunting: The Peculiarities of Nation-State Malware Research. *BlackHat USA, 2015.*