Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

I rischi digitali: come difendersi

Roberto Cecchini

Corso di formazione sul trattamento dei dati personali
Laboratori Nazionali di Frascati, 28 Novembre 2018

Pericoli informatici

A chi fa gola il vostro pc?

- Hacker
- spammer
- virus / worm
- il vostro PC, se non opportunamente protetto e senza le ultime versioni del software installato (e anche con queste...), può essere facilmente compromesso (con, o anche senza, il vostro aiuto attivo).

… e perché?

- untore
- spam
- attacchi DDoS (Distributed Denial of Service)
- testa di ponte per altri attacchi
- deposito di materiale illegale
- cava di password
- recupero informazioni personali

Virus

- Un **virus** è un codice in grado di riprodursi attaccandosi ad un altro programma (o documento), in modo che venga eseguito ogni volta che lo sia il programma infettato.
  - Si propaga trasportato dal programma infetto
    - internet, cd rom, penna usb, floppy…
  - Di solito, ha bisogno di una qualche azione da parte dell'utente.

Worm

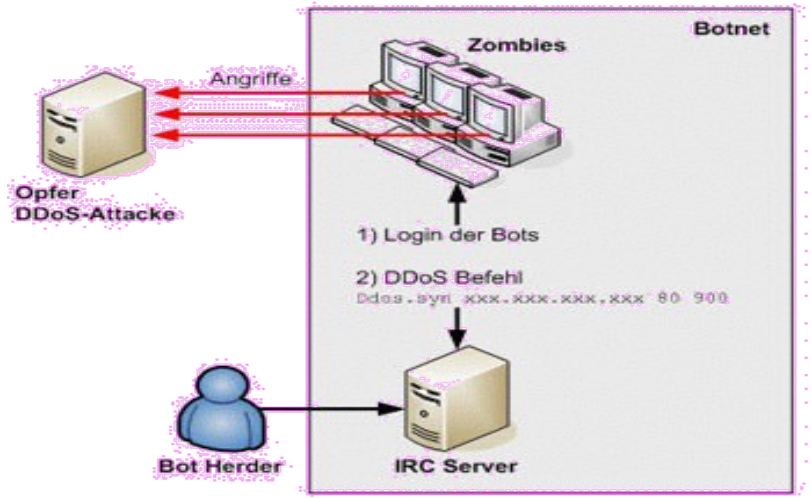
- Un **worm** è un eseguibile in grado di creare copie di sé stesso, senza infettare altri programmi (come fanno i virus).
  - Si propaga via posta elettronica o sfruttando difetti dei programmi installati.
  - Non necessita di azioni da parte dell'utente (a parte la trascuratezza …).

Virus & worm

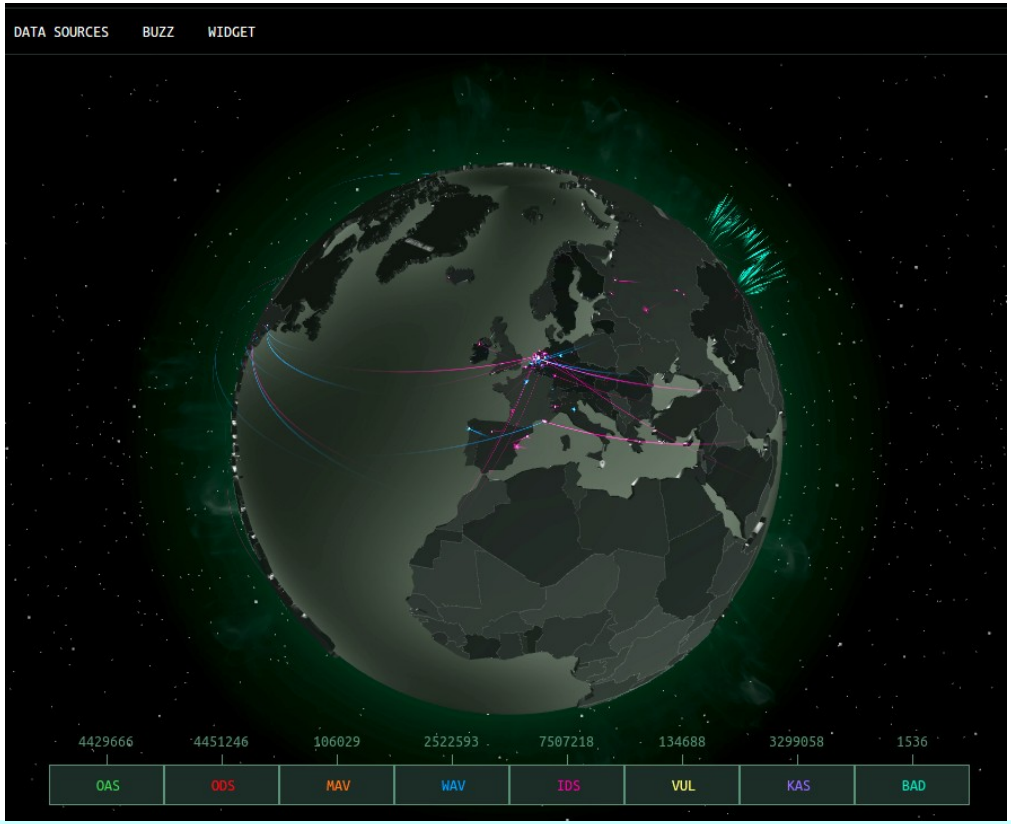
- Virus e worm, oltre a propagarsi, possono compiere un'infinità di altre azioni nocive:
  - cancellare file;
  - diffondere informazioni riservate (compresi i vostri mail privati …);
  - permettere ad intrusi di accedere alla vostra macchina;
  - spedire mail di spam
  - …

Botnet

- Una rete di software ro**bot**
  - installati su macchine compromesse
  - comandate remotamente
  - utilizzate per scopi criminali: spam, **attacchi DOS**.
- Le macchine facenti parte di una botnet sono stimate intorno ai **10 milioni**



Mappa real time attacchi

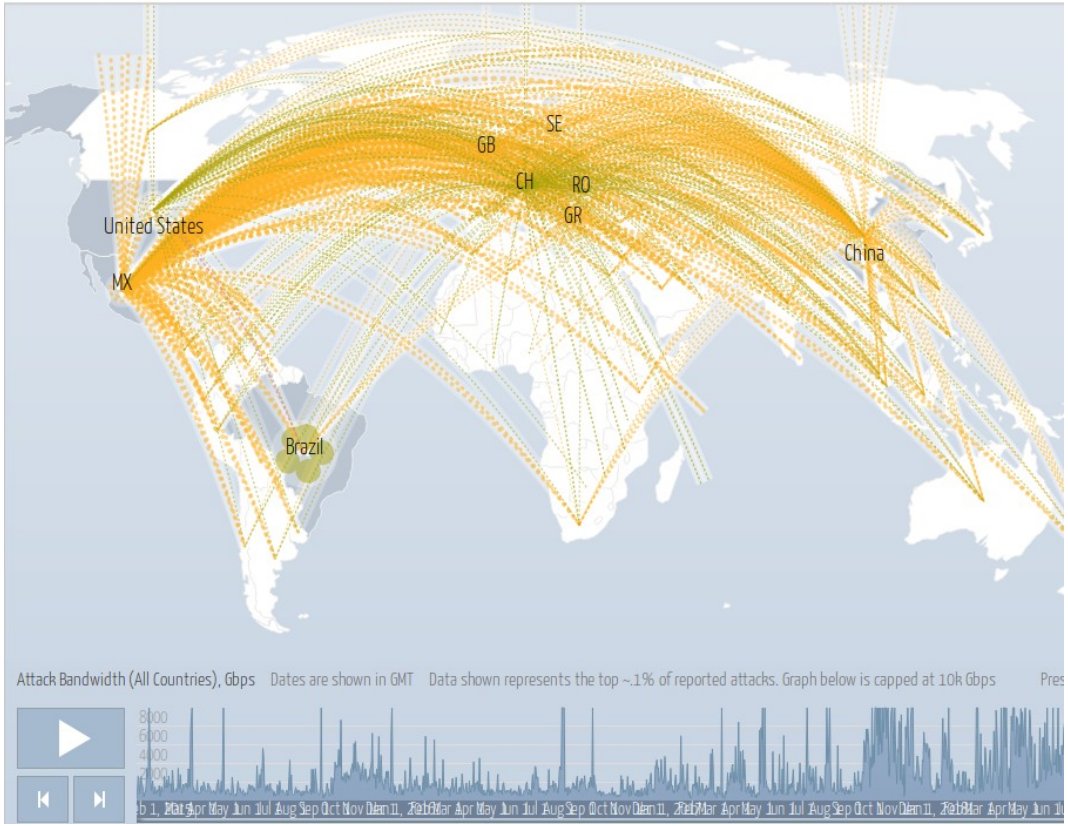


threatmap.checkpoint.com

cybermap.kaspersky.com

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

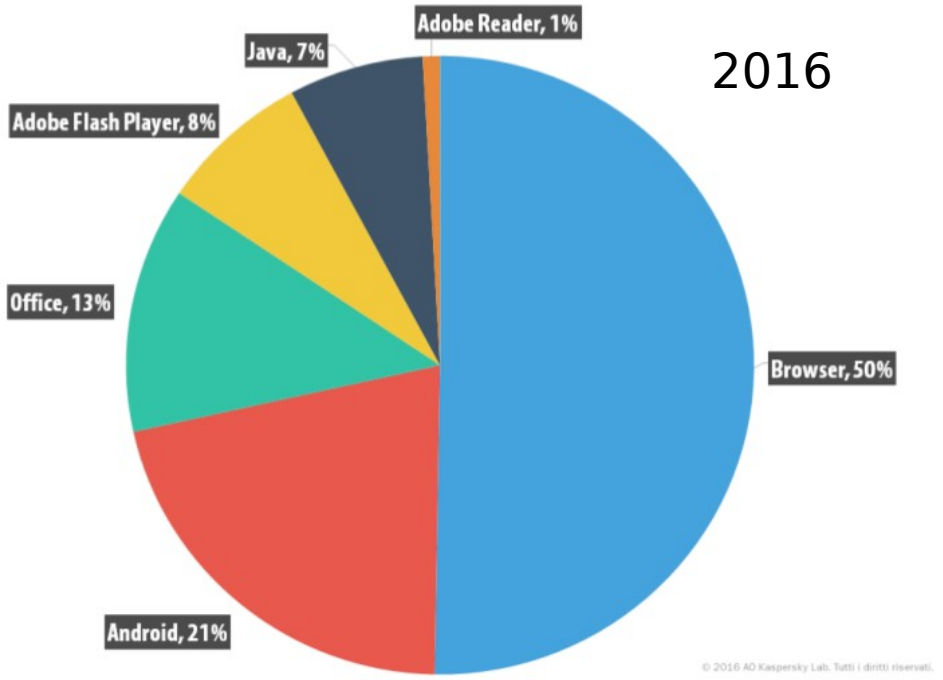
Mappa real time attacchi DDoS

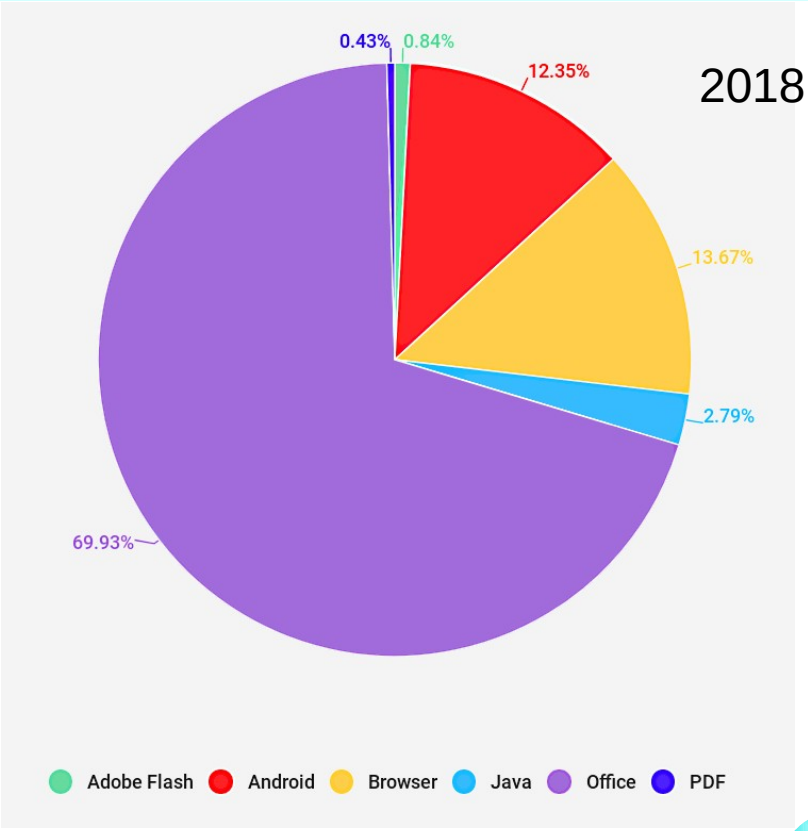


www.digitalattackmap.com

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Metodi di attacco, l'evoluzione





Fonte: Kasperski

Spam

- Un messaggio non richiesto
  - a carattere pubblicitario
  - truffe
    - nigeriana, amico in difficoltà, ecc. ecc.
- oltre il 50% degli email inviati!

Social engineering

- L'arte di manipolare le persone in modo che offrano informazioni riservate
  - sfrutta i sentimenti: autorevolezza, colpa, panico, desiderio, avidità, compassione
  - metodi:
    - phishing / spear phishing
    - pretexting
      - telefonata dal Servizio Calcolo
    - baiting
      - chiavetta abbandonata

Spyware

- Inseriti in altri programmi (ad es. client p2p, salvaschermo, sfondi), inviano informazioni sulle attività dell'utente
  - molti Internet Explorer toolbar add-on o finti anti-spyware
  - attenzione durante l'installazione di programmi quando vi viene chiesto se volete altre funzionalità

Phishing

- Un tentativo di carpire informazioni riservate e sensibili quali password o credenziali bancarie
- Un attacco di phishing inizia con l'invio di una mail che contiene un'offerta allettante o richiede un'azione quale:
  - compilare un modulo (ad es. cambio password)
  - cliccare su un link che conduce ad un sito fasullo
  - aprire un allegato infetto (ad es. uno zip che dovrebbe contenere una fattura).

Phishing

- Secondo Verizon è alla base del 90% degli incidenti di sicurezza
- La creazione di siti di phising al momento è stimata intorno a 1,4 milioni al mese
- Molto difficili da filtrare

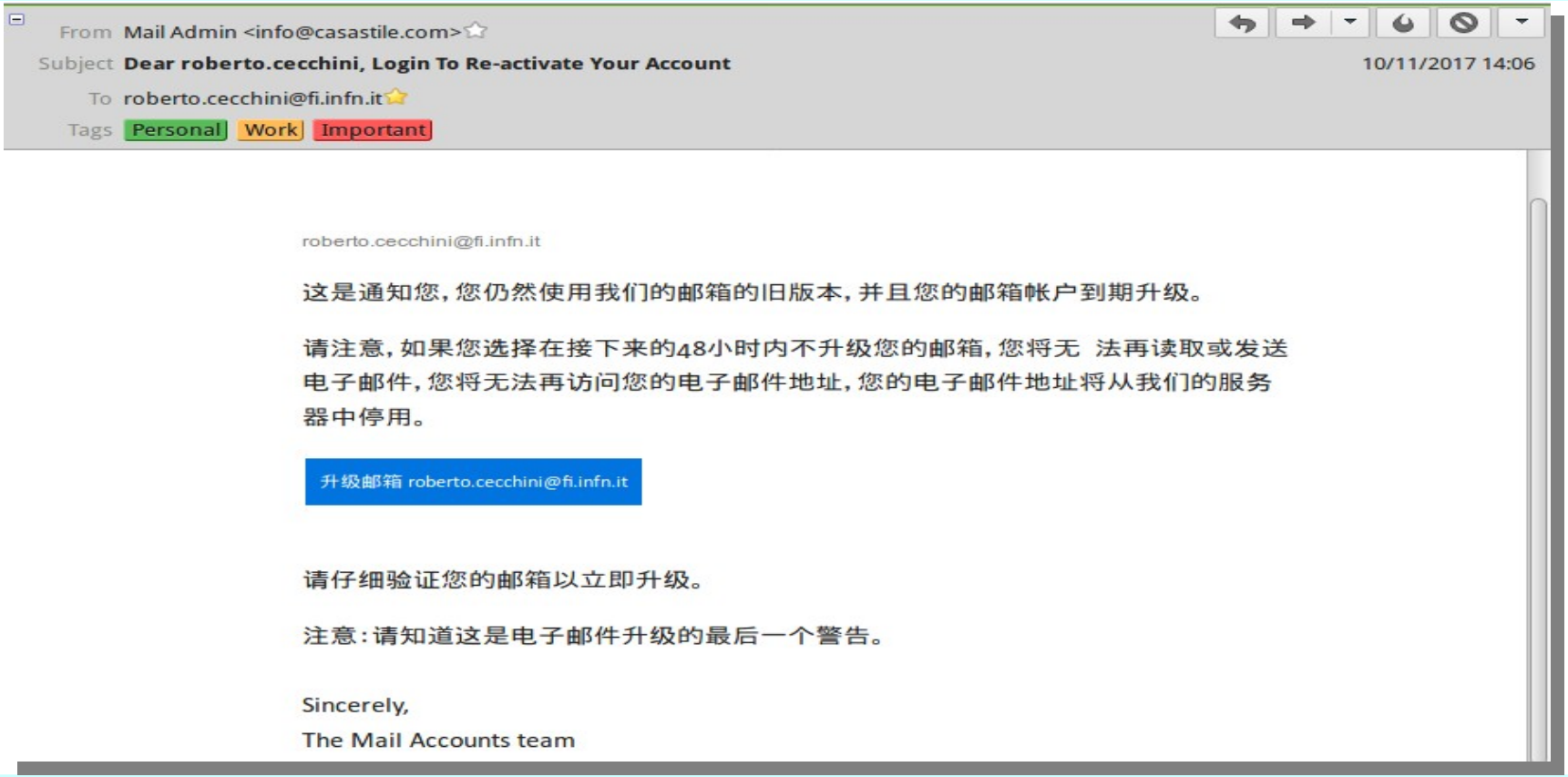
Phishing?

- Link non corrispondente a quello visualizzato
- Analizzare il dominio a cui si chiede di accedere: ad esempio login.bancaintesa.web.com/credenziali
- Messaggio sgrammaticato o in inglese
- Richiesta di azioni urgenti
- Richiesta di informazioni personali. Diffidate di messaggi in cui vi si chiede di accedere al sito per motivi di “aggiornamento” o “operazioni da confermare”.
- Offerte molto interessanti
- Richiesta di soldi
- Lettera minacciosa di un avvocato
- Agenzia governativa: Equitalia, Agenzia delle Entrate e tutte le altre
- Richieste dal Servizio Calcolo (casella postale piena, account in scadenza, ecc. ecc.)

Proteggetevi!

- Non rispondete mai a richieste di password, codici di sicurezza, PIN ecc.
- Fate molta attenzione agli allegati
- Elementi sospetti
  - email che sollecitano azioni urgenti.
  - email con formule generiche quali “Caro cliente” o “Gentile Signora/Egregio Signore”.
  - email con errori di grammatica o ortografia.
- Se c'è un link, fateci passare sopra il puntatore e controllate la vera destinazione che apparirà nella barra degli indirizzi.

Phishing: esempio 1



From Mail Admin <info@casastile.com>
Subject **Dear roberto.cecchini, Login To Re-activate Your Account**
10/11/2017 14:06
To roberto.cecchini@fi.infn.it
Tags Personal Work Important

roberto.cecchini@fi.infn.it

这是通知您，您仍然使用我们的邮箱的旧版本，并且您的邮箱帐户到期升级。

请注意，如果您选择在接下来的48小时内不升级您的邮箱，您将无 法再读取或发送电子邮件，您将无法再访问您的电子邮件地址，您的电子邮件地址将从我们的服务器中停用。

升级邮箱 roberto.cecchini@fi.infn.it

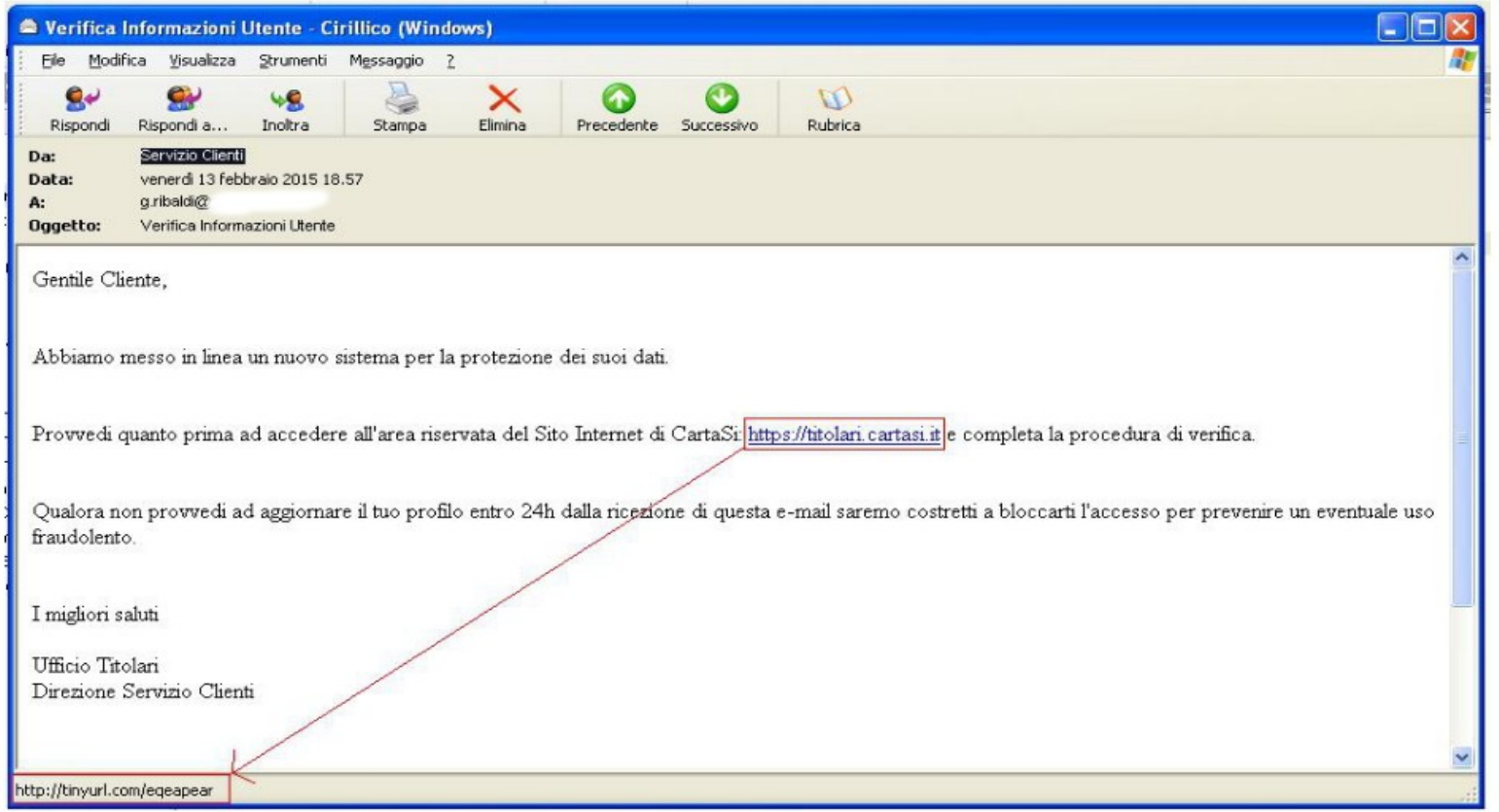
请仔细验证您的邮箱以立即升级。

注意：请知道这是电子邮件升级的最后一个警告。

Sincerely,
The Mail Accounts team

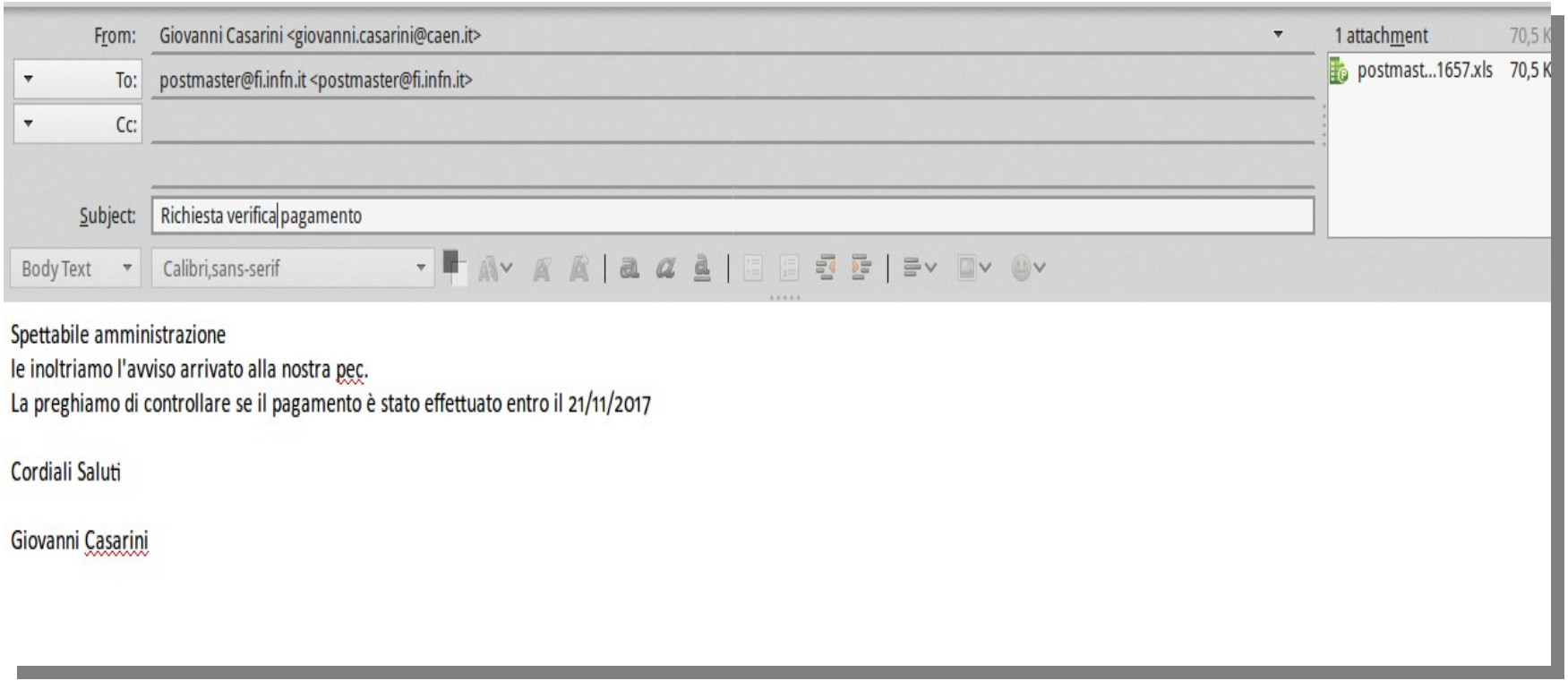
Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Phishing: esempio 2



Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Phishing: esempio 2



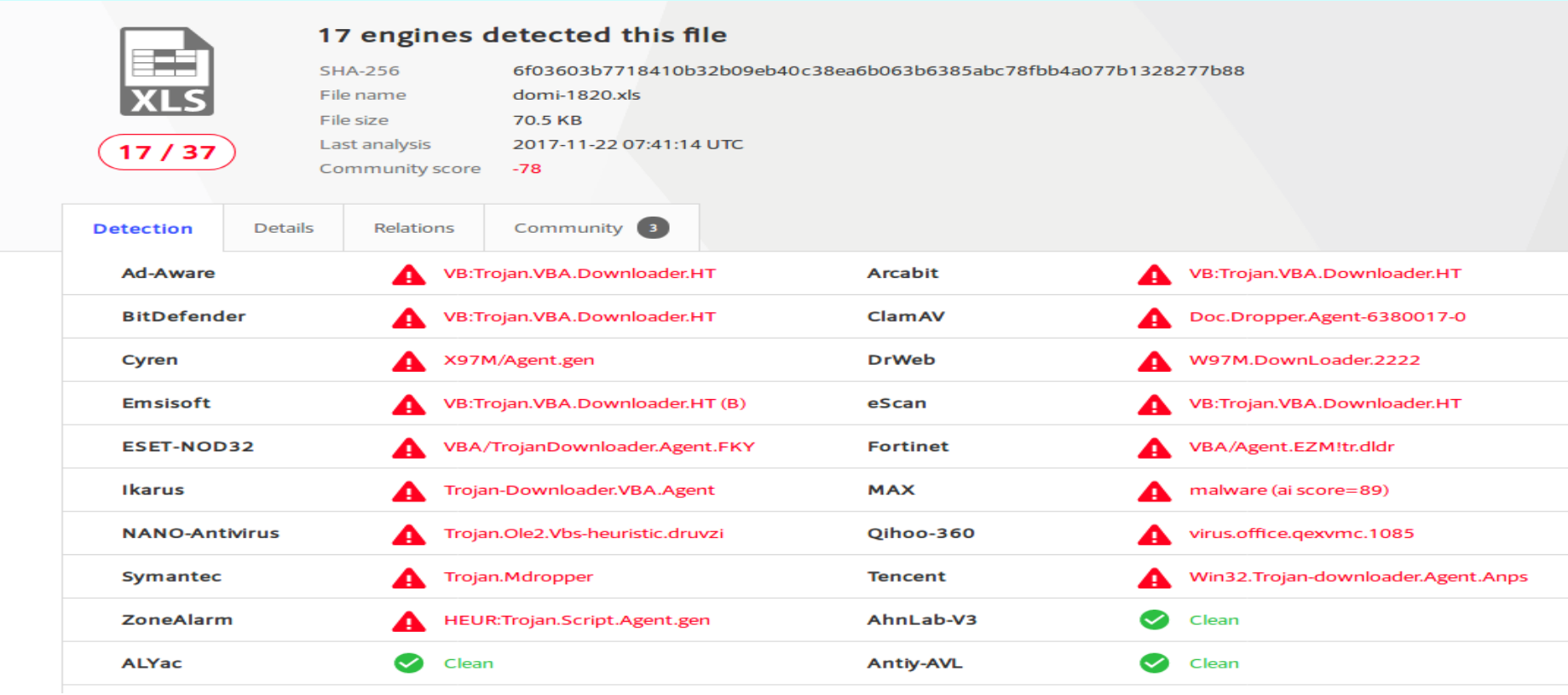
From: Giovanni Casarini <giovanni.casarini@caen.it>
1 attachment 70,5 K
To: postmaster@fi.infn.it <postmaster@fi.infn.it>
postmast...1657.xls 70,5 K
Cc:
Subject: Richiesta verifica pagamento
Body Text Calibri,sans-serif

Spettabile amministrazione
le inoltriamo l'avviso arrivato alla nostra pec.
La preghiamo di controllare se il pagamento è stato effettuato entro il 21/11/2017

Cordiali Saluti

Giovanni Casarini

virustotal.com



17 / 37

17 engines detected this file

SHA-256	6f03603b7718410b32b09eb40c38ea6b063b6385abc78fbb4a077b1328277b88
File name	domi-1820.xls
File size	70.5 KB
Last analysis	2017-11-22 07:41:14 UTC
Community score	-78

Detection | Details | Relations | Community 3

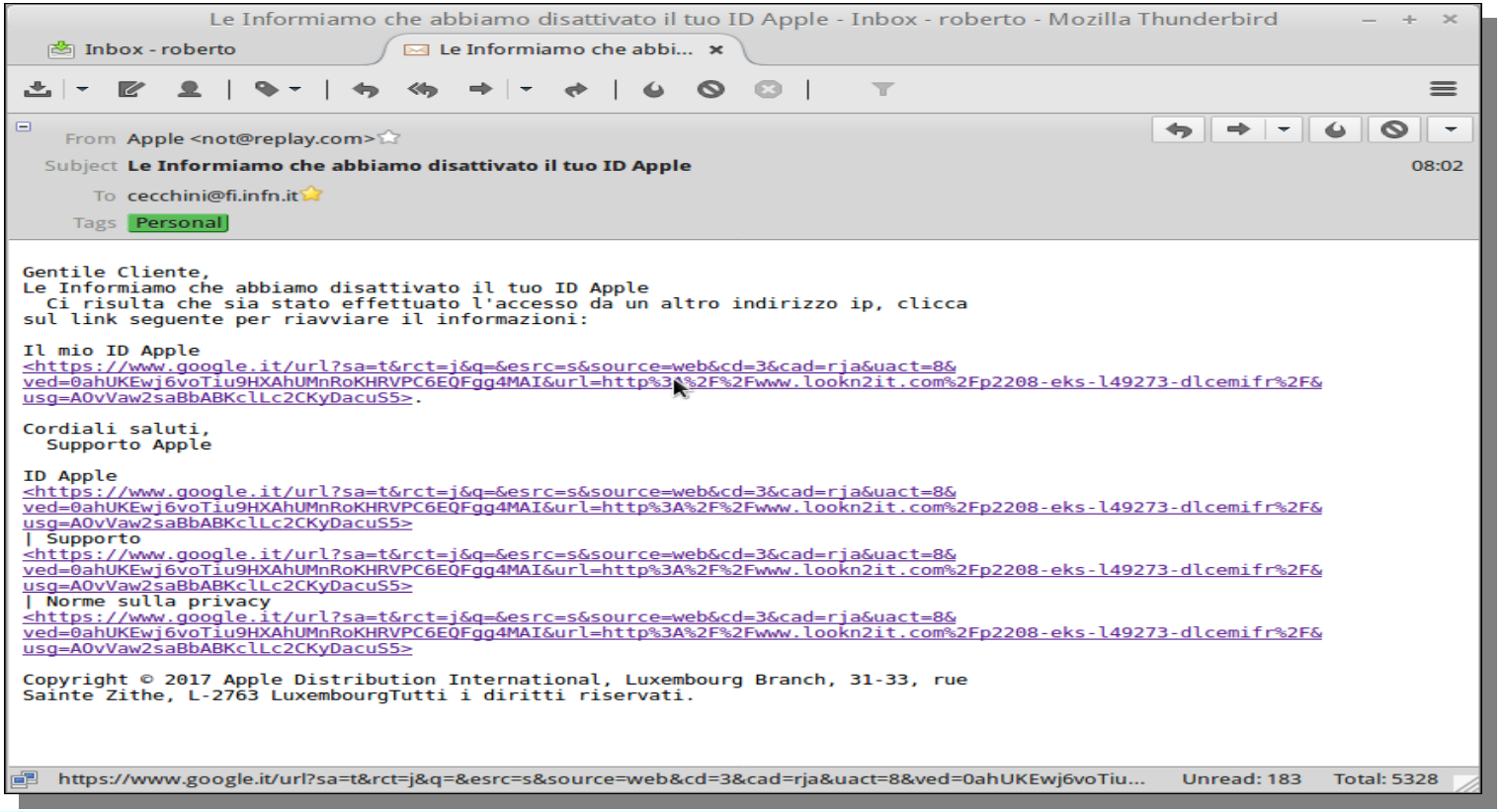
Ad-Aware	VB:Trojan.VBA.Downloader.HT	Arcabit	VB:Trojan.VBA.Downloader.HT
BitDefender	VB:Trojan.VBA.Downloader.HT	ClamAV	Doc.Dropper.Agent-6380017-0
Cyren	X97M/Agent.gen	DrWeb	W97M.DownLoader.2222
Emsisoft	VB:Trojan.VBA.Downloader.HT (B)	eScan	VB:Trojan.VBA.Downloader.HT
ESET-NOD32	VBA/TrojanDownloader.Agent.FKY	Fortinet	VBA/Agent.EZM!tr.dldr
Ikarus	Trojan-Downloader.VBA.Agent	MAX	malware (ai score=89)
NANO-Antivirus	Trojan.Ole2.Vbs-heuristic.druvzi	Qihoo-360	virus.office.qexvmc.1085
Symantec	Trojan.Mdropper	Tencent	Win32.Trojan-downloader.Agent.Anps
ZoneAlarm	HEUR:Trojan.Script.Agent.gen	AhnLab-V3	Clean
ALYac	Clean	Antiy-AVL	Clean

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Phishing: esempio 3

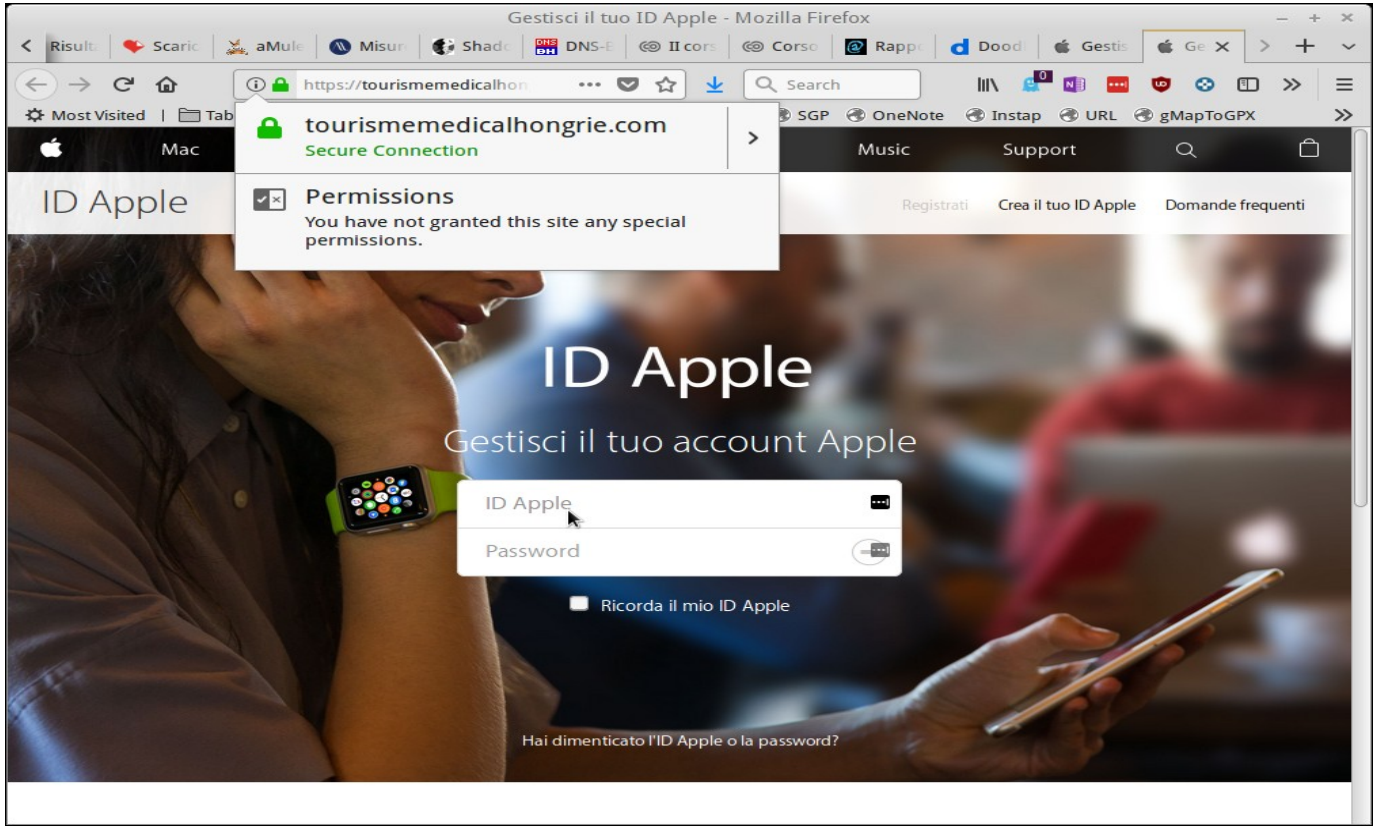
Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Phishing: esempio 3 segue



Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Phishing: esempio 3 segue



Le “bufale” (Hoax)

- Non sono un'invenzione recente, ma internet le rende particolarmente pericolose.
- Notizie false:
  - aumentano le e-mail inutili in circolazione,
  - diffondono indirizzi di e-mail,
  - effetti simili a quelli di un virus.
- Frasi tipiche:
  - “Nuovo virus pericolosissimo”
  - “Notizia proveniente da Microsoft”
  - “Bambina in fin di vita”
  - “Diffondete la notizia quanto più possibile”

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Le “bufale” (Hoax) segue

- Prima di ridiffondere la notizia, controllatene l’autenticità:
  - CICAP, bufalopedia, ecc. ecc.
- Anche se la notizia è vera (e anche se per una nobile causa) valutate attentamente l’opportunità della sua diffusione via la rete GARR.
- **In ogni caso, mettete i destinatari in BCC:**

Misure elementari di sicurezza

Sicurezza “base”

- Non lasciare documenti incustoditi sulla scrivania;
- utilizzare il salvaschermo con password;
- chiudere a chiave l’ufficio;
- attenzione alle stampanti e fotocopiatrici in luoghi pubblici;
- utilizzare solo i servizi cloud approvati dall’INFN;
- evitare per quanto possibile di trasferire dati personali su supporti rimovibili e comunque cancellarli appena non più necessari;
- prima di rottamare un’apparecchiatura elettronica, aver cura di rendere illeggibile il contenuto.

Nel proprio sistema

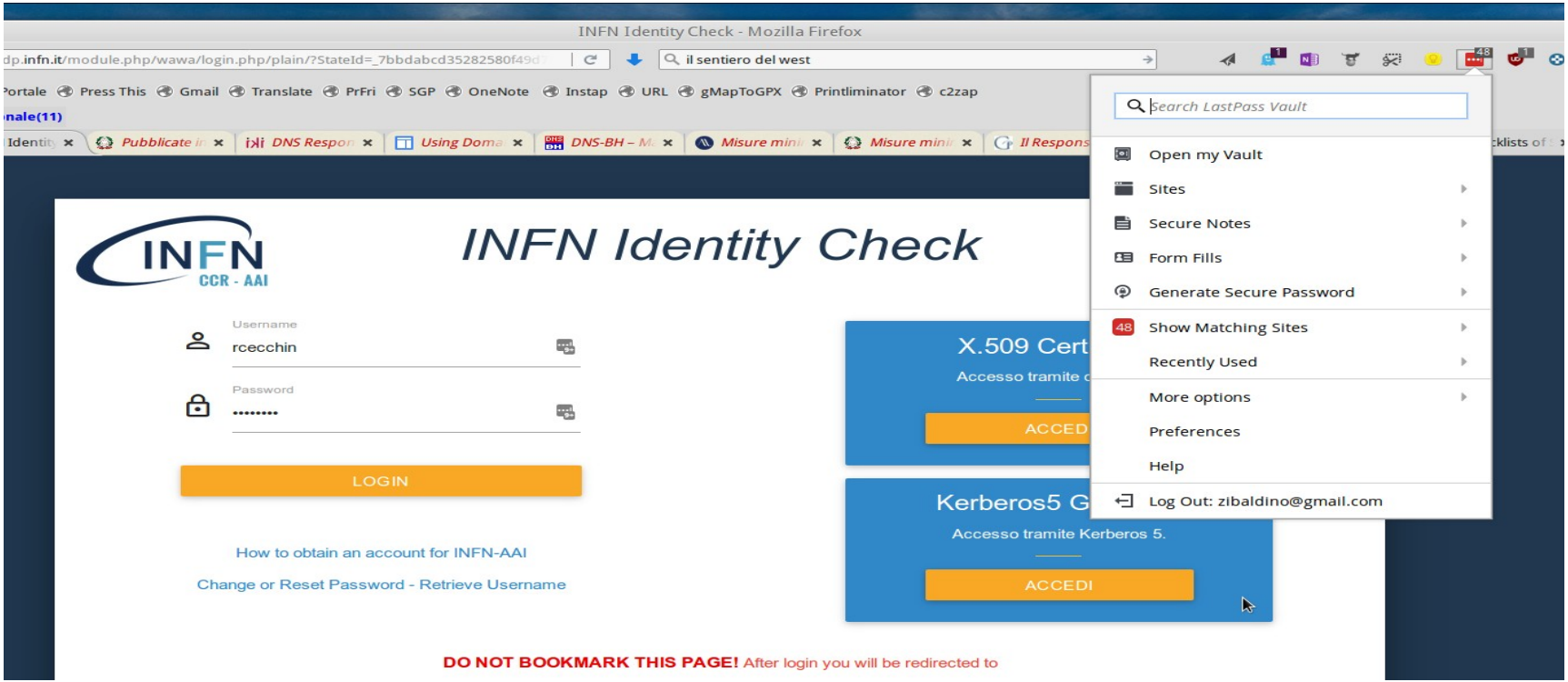
- Non modificare la configurazione rilasciata dal Servizio Calcolo!
  - non abilitare l'esecuzione automatica dei contenuti dei device rimovibili (stuxnet!)
  - attivare le macro Office solo caso per caso
  - non disattivare la scansione automatica dei device esterni al loro collegamento
  - non attivare il preview automatico delle e-mail
- Seguire le indicazioni del Servizio Calcolo per i backup

Password

- **Personale e non cedibile**
- Da proteggere con la massima cura
- Da non conservare in chiaro
- Da non riciclare

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Password manager: LastPass



Antivirus

- È **obbligatorio** installare un antivirus
  - Il Servizio di Calcolo dispone di software e licenze e può prestare consulenza al riguardo
- In ogni caso:
  - non aprite allegati di e-mail di cui non siete sicuri, **anche se il mittente è una persona di cui vi fidate**;
    - il campo From: **non è mai attendibile**
  - usate solo programmi provenienti da fonti fidate

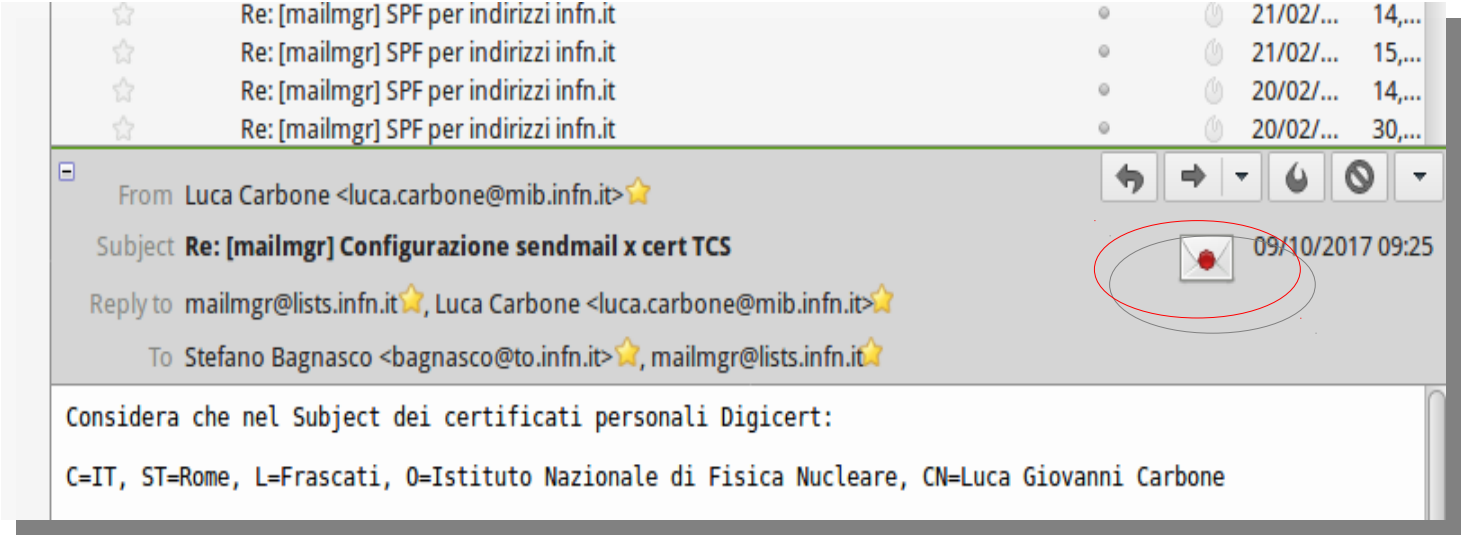
Crittografia

- I dati (mail, file, database, cartelle) possono venire cifrati:
  - “impossibili” da capire tranne che per i possessori della chiave di cifratura;
  - la chiave può essere di tipo hardware (ad es. smart card) o software (passphrase);
  - se la chiave viene persa, i dati sono irrecuperabili.

Posta: firmare e cifrare

- Un messaggio “firmato” con un certificato digitale garantisce l'identità del mittente
  - tutti possono firmare i propri messaggi (dopo aver ottenuto un certificato digitale)
- Un messaggio cifrato impedisce la lettura a chi non è tra i destinatari
  - è necessario che anche i riceventi abbiano un certificato digitale
- I certificati digitali sono disponibili per chiunque abbia un account AAI INFN

Posta firmata



Il “data breach”

- La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
- Deve essere segnalato **immediatamente** (anche se solo un sospetto)

Statistiche

www.breachlevelindex.com

Data breach: qualche esempio

- Perdita di un portatile o chiavetta usb (cifrati o no)
  - confidenzialità e/o disponiblità
- Attacco *ransomware*
- Invio di un file con dati personali a un destinatario sbagliato
  - attenzione al meccanismo di autocompletamento!
- Infezione da un virus che cattura i dati personali sul vostro pc

Cosa non fare

- Non far nulla e sperare
- Aspettare mesi
- Negare, negare, negare

In ogni caso…

- Il Servizio Calcolo, anche se spesso non ha risorse sufficienti, va comunque sempre interpellato.
- Il System Manager è il vostro miglior amico!

Domande?