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

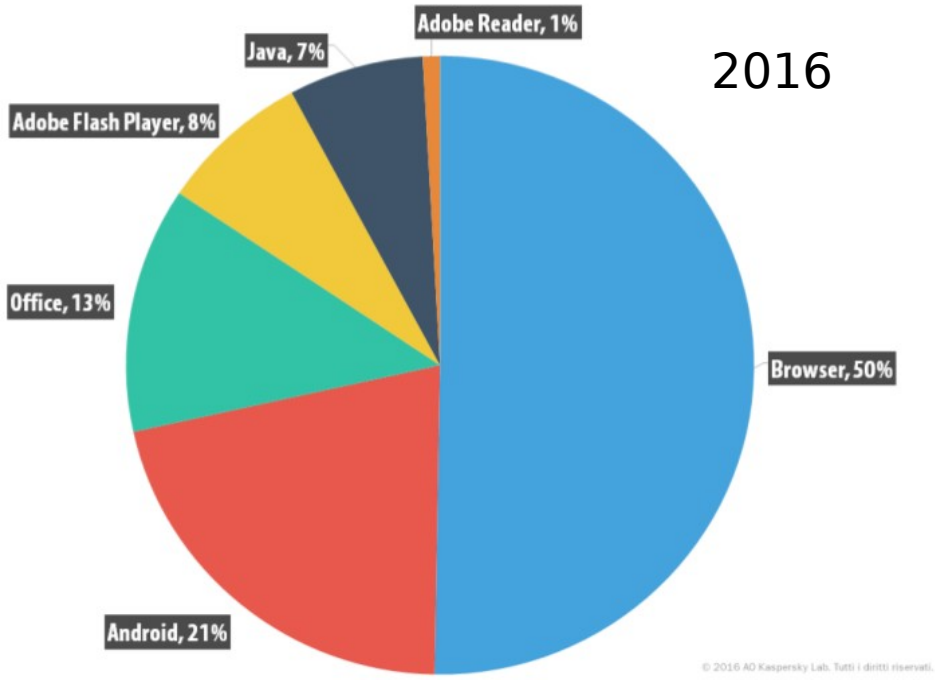
Rischi digitali e misure di sicurezza

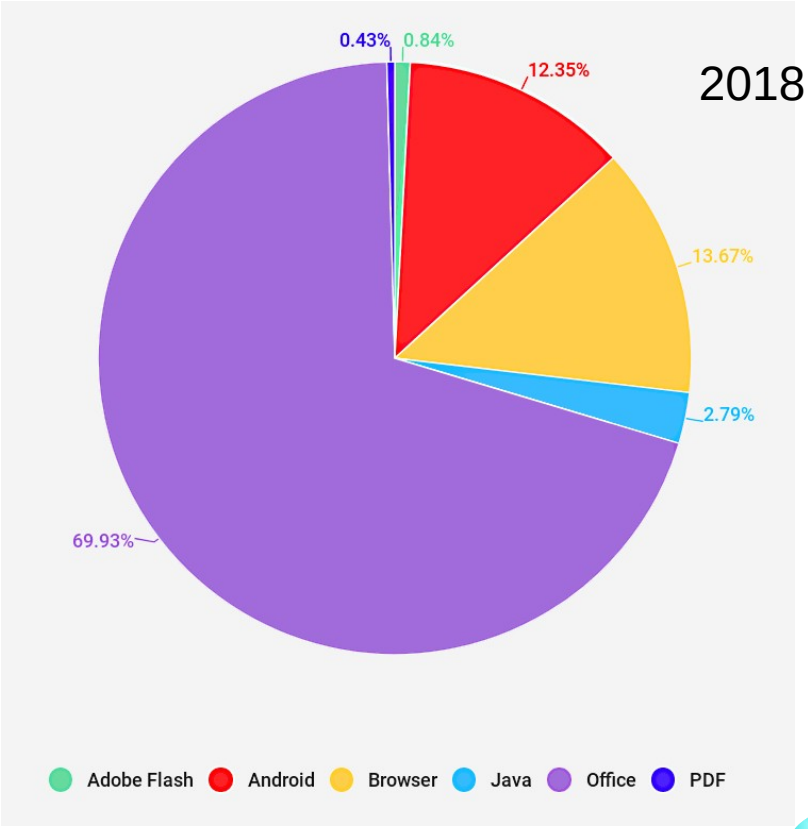
Roberto Cecchini

Riunione esperti qualificati INFN
Presidenza, 12 aprile 2019

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

Metodi di attacco, l'evoluzione





Fonte: Kasperski

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

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).

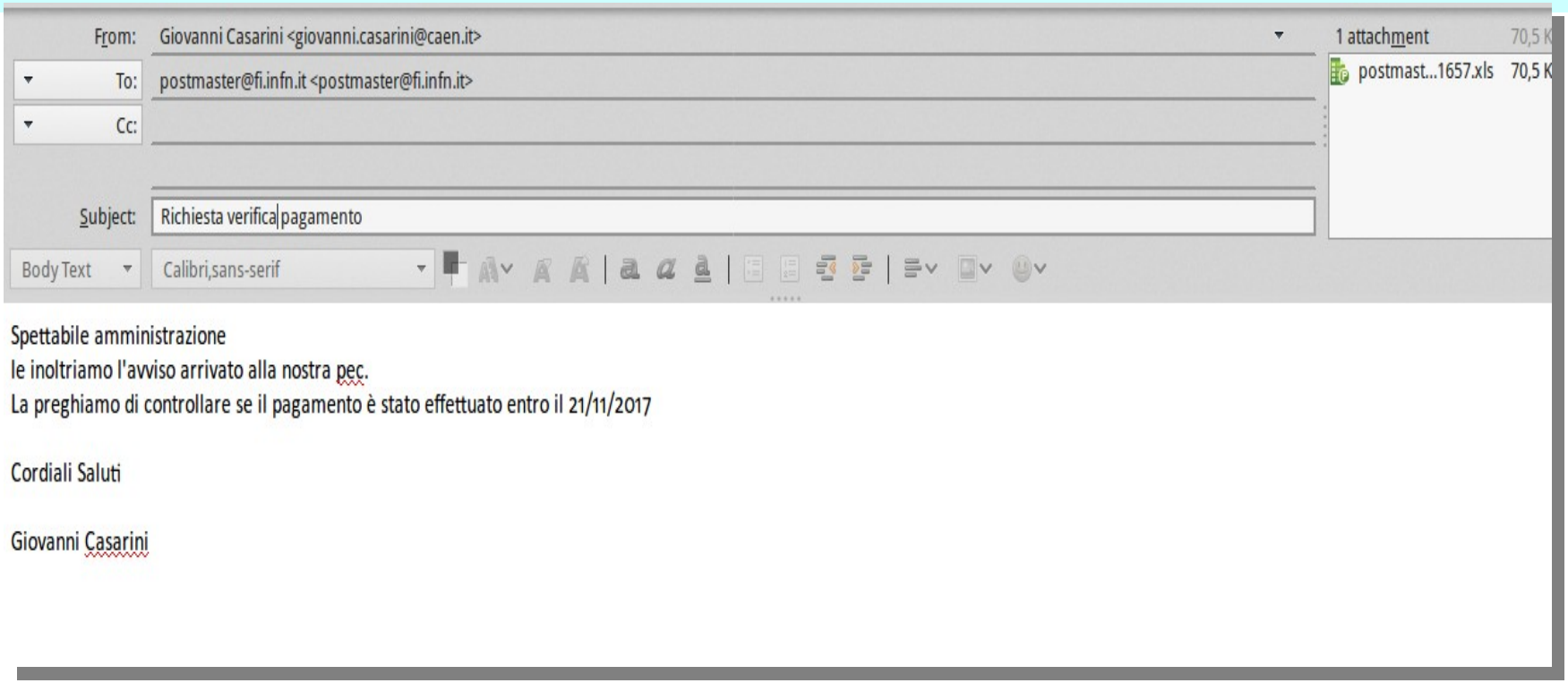
Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

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.)

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

Phishing (1)

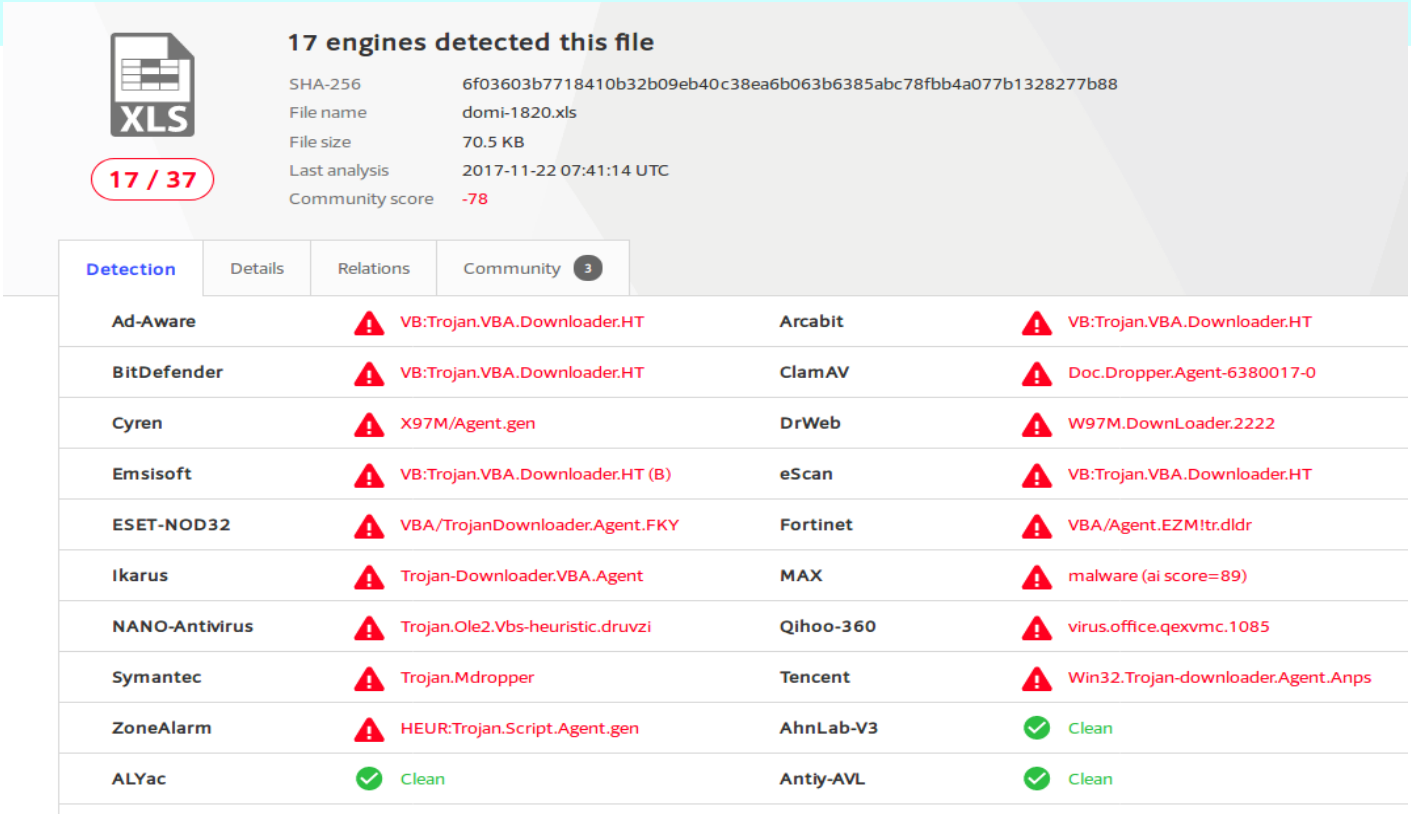


Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Analisi file sospetti

Se avete dubbi su di un file (anche se il vostro antivirus tace) potete farlo esaminare da uno dei tanti servizi disponibili in rete ad esempio:
virustotal.com

virustotal.com: esempio di analisi



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

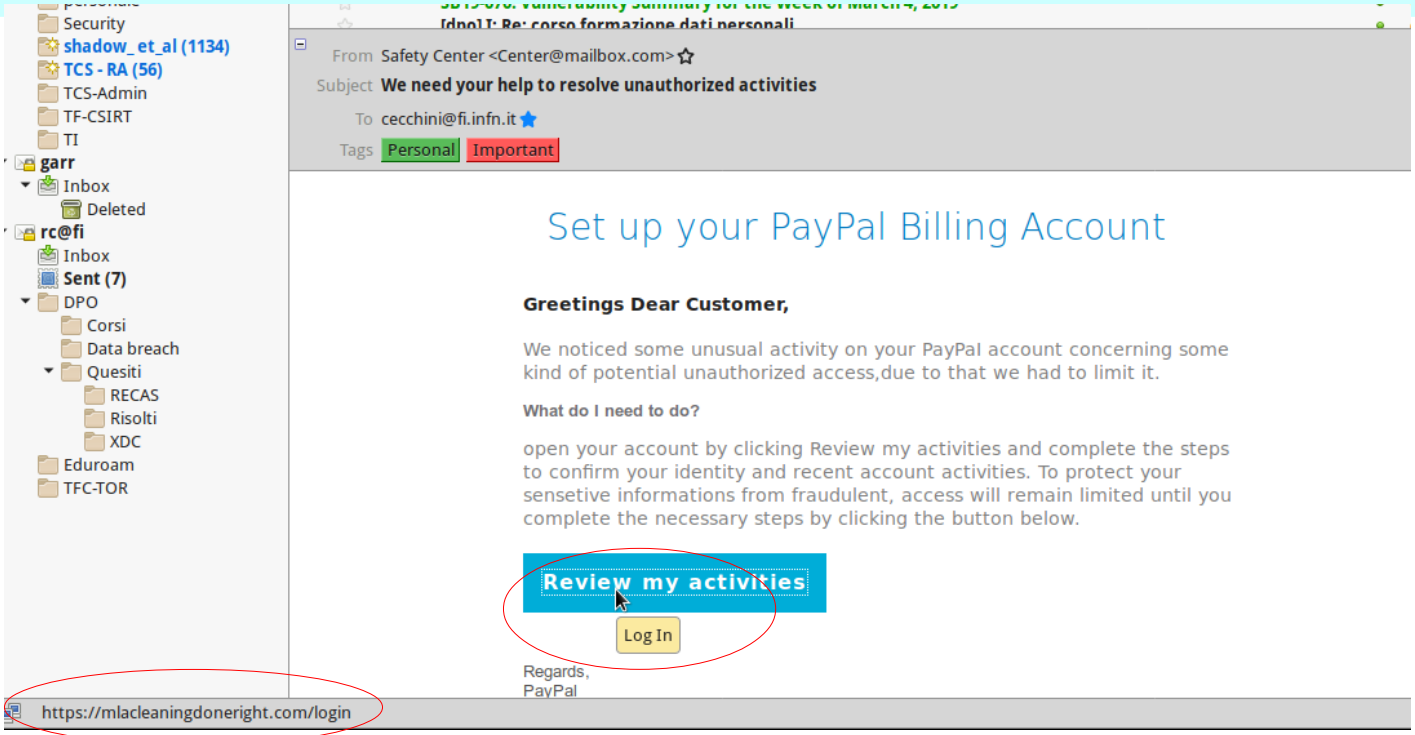
17 / 37

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 (2)

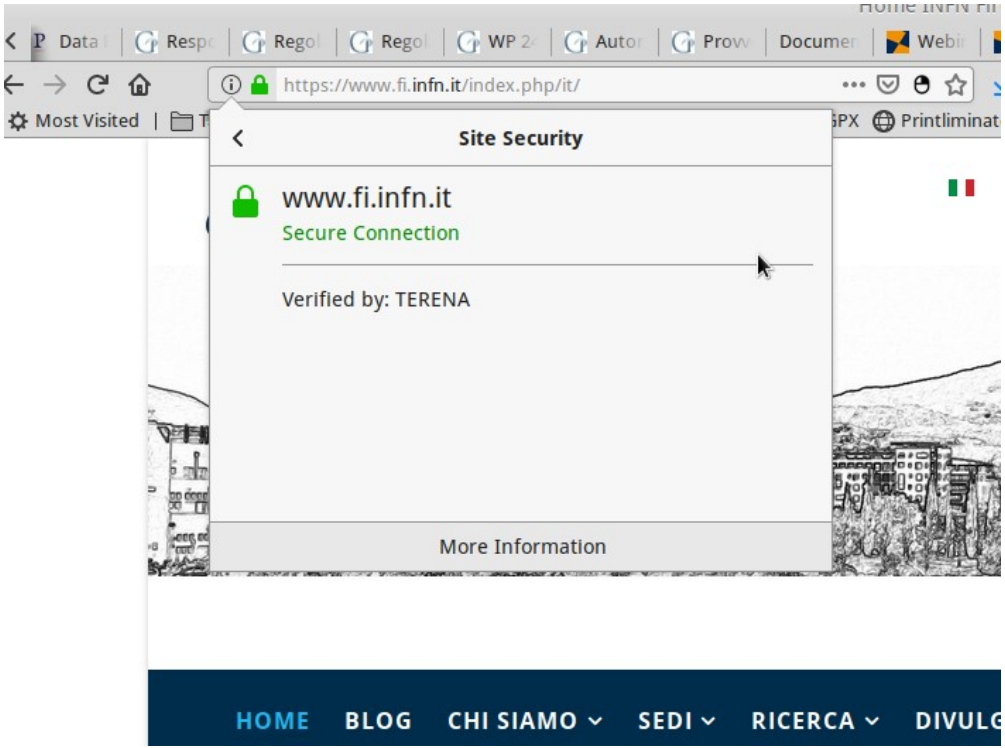


Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

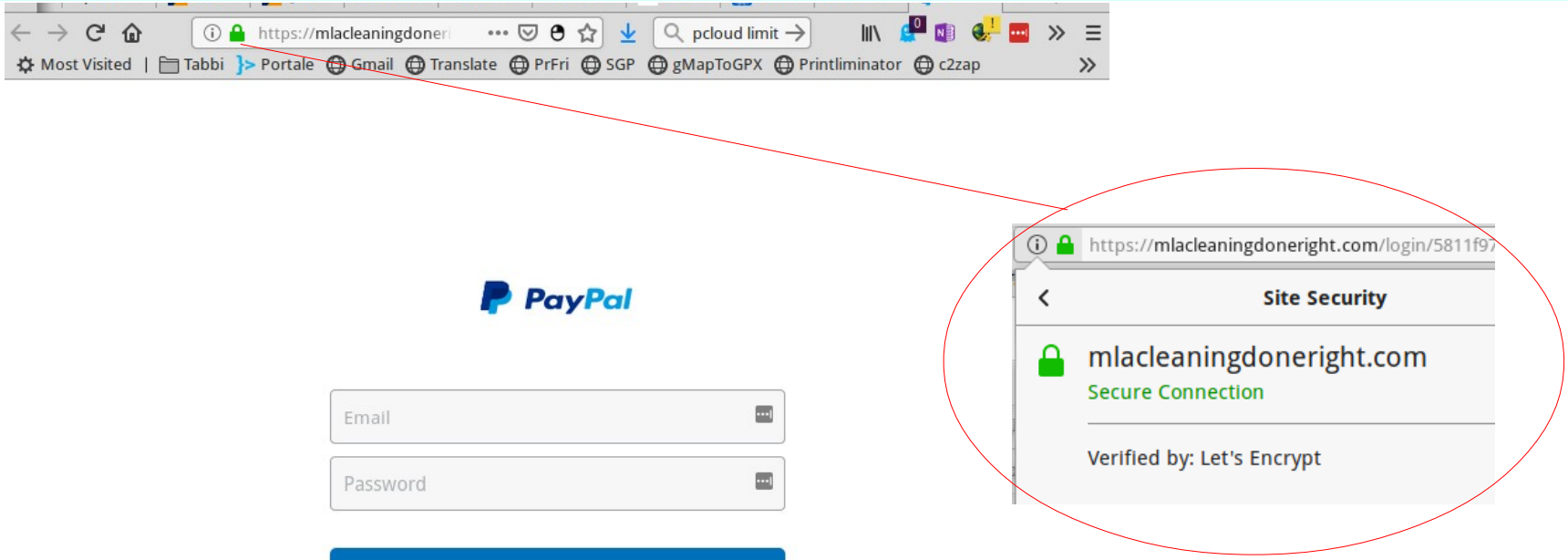
Connessioni web

Usare solo connessioni “sicure” (**https://...**), cioè “garantite” da un certificato digitale:

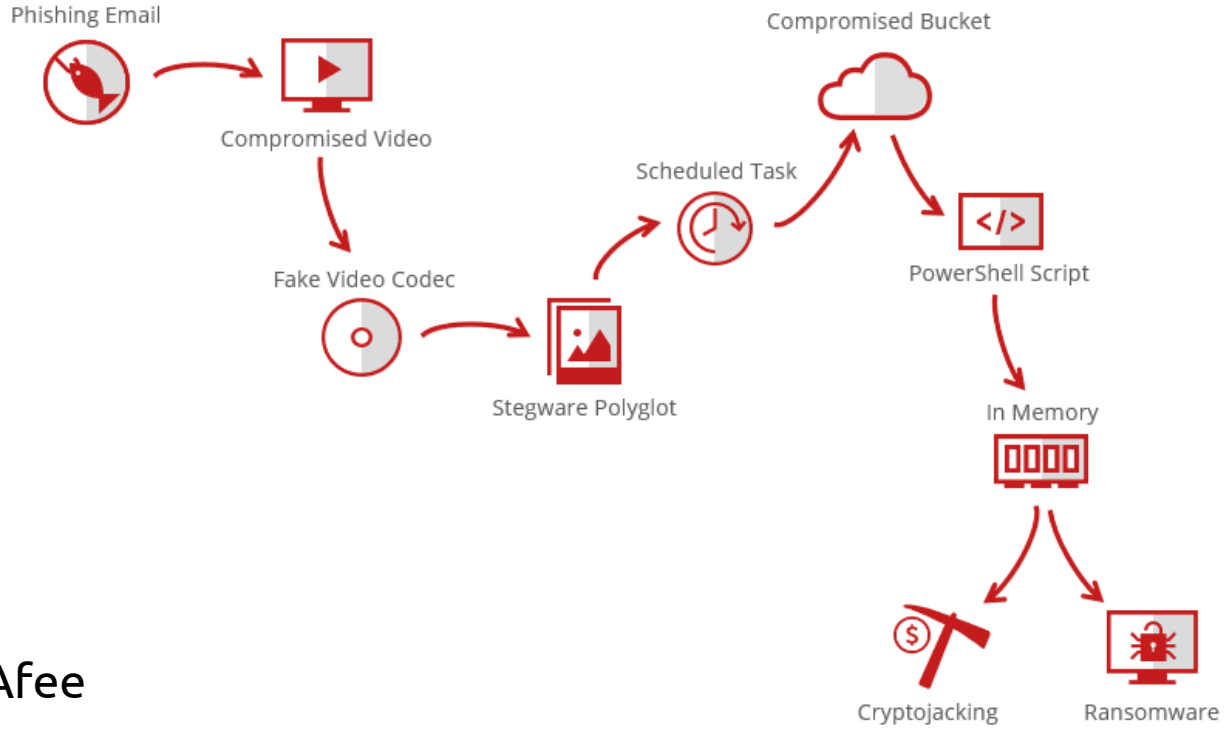
- segnalate nel browser da un lucchetto
- il traffico è cifrato
- c'è una certa garanzia sull'identità del server



Phishing (2, segue)



Uno scenario di phishing



da MacAfee

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, rendere illeggibile il contenuto.

Norme d'uso: punti principali (1/4)

- Non utilizzare indirizzi IP arbitrari.
- Se possibile, usare un filesystem cifrato.
- Configurare lo sharing (se necessario) permettendolo solo al gruppo di persone che ne dovranno fare uso e impostando gli opportuni permessi (read/write, read...).
- L'accesso da remoto al sistema deve avvenire solo tramite RDP, specificando gli account abilitati.
- Il sistema operativo e tutto il software impiegato deve esser mantenuto costantemente aggiornato, applicando tutte le patch di sicurezza non appena disponibili (eccezioni sono possibili, ma solo in casi particolari).

Norme d'uso: punti principali (2/4)

- A seguito di modifiche significative del sistema, concordare con il Servizio Calcolo l'esecuzione di una scansione di sicurezza.
- Deve essere installato l'antivirus messo a disposizione dall'INFN, impostando l'aggiornamento automatico e l'esecuzione delle scansioni anti-malware dei supporti rimovibili al momento della loro connessione.
- Attivare il firewall personale.
- Limitare al massimo l'uso di dispositivi esterni.

Norme d'uso: punti principali (3/4)

- Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimovibili.
- Disattivare l'esecuzione automatica dei contenuti dinamici (p.e. macro) presenti nei file.
- Disattivare l'anteprima automatica dei contenuti dei file e dei messaggi di posta.

Norme d'uso: punti principali (4/4)

- Eseguire almeno settimanalmente una copia di salvataggio delle informazioni necessarie per il completo ripristino del sistema.
- Cifrare le copie di salvataggio.
- In caso di compromissione del sistema informare immediatamente il Servizio Calcolo e Reti e concordare la procedura di ripristino.

Il *data breach*

- Una 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 sospettato).

Data breach: qualche esempio

- Perdita di un portatile o chiavetta usb (cifrati o no)
  - confidenzialità e/o disponibilità.
- 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.

Domande?