Sicurezza Documentale a.a. 2017/2018

DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ

Minacce Software

Malware

- abbreviazione per **malicious software -** *software malintenzionato* - di solito tradotto come *software dannoso*
- qualsiasi software che si comporta in modo illecito o malevolo nei confronti dell'utente
  - disturbare le operazioni svolte da un computer
  - rubare informazioni sensibili
  - accedere a sistemi informatici privati
  - mostrare pubblicità indesiderata
- tipicamente associati a un meccanismo di diffusione
- moltissime tipologie e varianti
  - più che una classificazione del software si classificano le tipologie di "comportamento"
    - virus, trojan, worm, ecc.
    - es. un malware può essere contemporaneamente trojan e virus

Minacce Software

Virus

- un virus è codice eseguibile in grado di infettare (copiarsi all'interno di) altro codice eseguibile
  - una volta eseguito, infetta dei file in modo da fare copie di se stesso
- cioè è in grado di riprodursi e diffondersi automaticamente all'interno di un sistema
- sono più diffusi nei sistemi Windows dove il confinamento è tradizionalmente meno stretto

Minacce Software

Virus – Ciclo di vita

- *creazione*: è la fase in cui lo sviluppatore progetta, programma e diffonde il virus. Di solito i cracker per la realizzazione di virus utilizzano linguaggi di programmazione a basso livello. La diffusione di pacchetti software che permettono anche ad utenti inesperti di creare virus pericolosissimi ha reso accessibile il procedimento di creazione anche a persone senza competenze.
- *incubazione*: il virus è presente sul computer da colpire ma non compie alcuna attività.
- *infezione*: il virus infetta il file e di conseguenza il sistema.
- *attivazione*: al verificarsi delle condizioni prestabilite dal cracker, il virus inizia l'azione dannosa.
- *propagazione*: il virus propaga l'infezione, riproducendosi e infettando sia file nella stessa macchina che altri sistemi.
- *riconoscimento*: l'antivirus riconosce un certo file come infetto.
- *estirpazione*: è l'ultima fase del ciclo vitale del virus. Il virus viene eliminato dal sistema.

Minacce Software

Virus – capacitá distruttive

- *innocui*: se comportano solo una diminuzione dello spazio libero sul disco senza nessun'altra alterazione delle operazioni del computer;
- *non dannosi*: se comportano solo diminuzione dello spazio libero sul disco, emostrano grafici, suoni o altri effetti multimediali.
- *dannosi*: possono provocare problemi alle normali operazioni del computer (ad esempio, cancellazione di alcune parti dei file, modifica di file o apertura di applicazioni);
- *molto dannosi*: Causano danni difficilmente recuperabili come la cancellazione di informazioni fondamentali per il sistema (formattazione di porzioni del disco, modifica dei parametri di sicurezza del sistema operativo, ...).

Minacce Software

Virus – Sintomi più frequenti di infezione

- *Rallentamento del computer*: il computer lavora molto più lentamente del solito. Impiega molto tempo ad aprire applicazioni o programmi. Il sistema operativo impiega molto tempo ad eseguire semplici operazioni che solitamente non richiedono molto tempo.
- *Impossibilità di eseguire un determinato programma o aprire uno specifico file*;
- *Scomparsa di file e cartelle*;
- *Messaggi di errore inattesi o insoliti*: visualizzazione di finestre di dialogo contenenti messaggi assurdi, buffi o aggressivi;
- *Riduzione di spazio nella memoria e nell'hard disk*: riduzione significativa dello spazio libero nell'hard disk;
- *Ridenominazione di file;*
- *Problemi di avvio del computer;*

Minacce Software

Virus – Sintomi più frequenti di infezione

- *Interruzione del programma in esecuzione*
- *Tastiera e/o mouse non funzionanti correttamente*: la tastiera non scrive ciò che è digitato dall'utente o esegue operazioni non corrispondenti ai tasti premuti. Il puntatore del mouse si muove da solo o indipendentemente dal movimento richiesto dall'utente;
- *Scomparsa di sezioni di finestre*: determinate sezioni (pulsanti, menu, testi etc…) che dovrebbero apparire in una particolare finestra sono scomparse o non vengono visualizzate.
- *Antivirus disattivato automaticamente*: Può capitare che un virus disattivi forzatamente un antivirus per poter essere eseguito senza correre il rischio di essere rilevato;
- *Lentezza della connessione Internet*: il virus potrebbe usare la connessione per propagare l'infezione, o inviare dati a chi ha scritto il virus;
- *Limitazioni nella visualizzazione di alcuni siti Internet*, soprattutto quelli dei produttori di antivirus: è un meccanismo di protezione da parte del virus, che in questo modo impedisce di adottare contromisure dopo l'infezione.

Minacce Software

Virus

- alcuni sono dei semplici scherzi, altri danneggiano irreparabilmente il sistema
- usavano mezzi “sociali” per la diffusione
  - una volta erano i floppy disk (larga diffusione con l'MS-DOS)
  - ora è sopratutto l'email e lo spam, ma anche il web (vulnerabilità dei browser).

Minacce Software

Trojan

- L'etimologia della parola deriva da Cavallo di Troia ed indica il modo in cui il programma penetra le difese: apparendo come un software utile o apparentemente sicuro, l'utente lo esegue di sua spontanea volontà facendo avviare anche il virus in background.
- un eseguibile che si spaccia per innocuo ma esegue attività malevole
- il codice malevolo contenuto è detto payload
- I trojan non si diffondono autonomamente come i virus e non sono in grado di replicare se stessi. Quindi richiedono un intervento diretto dell'aggressore per far giungere l'eseguibile maligno alla vittima.
  - la diffusione è tipicamente via email

Minacce Software

Trojan – come evitare di essere infettati

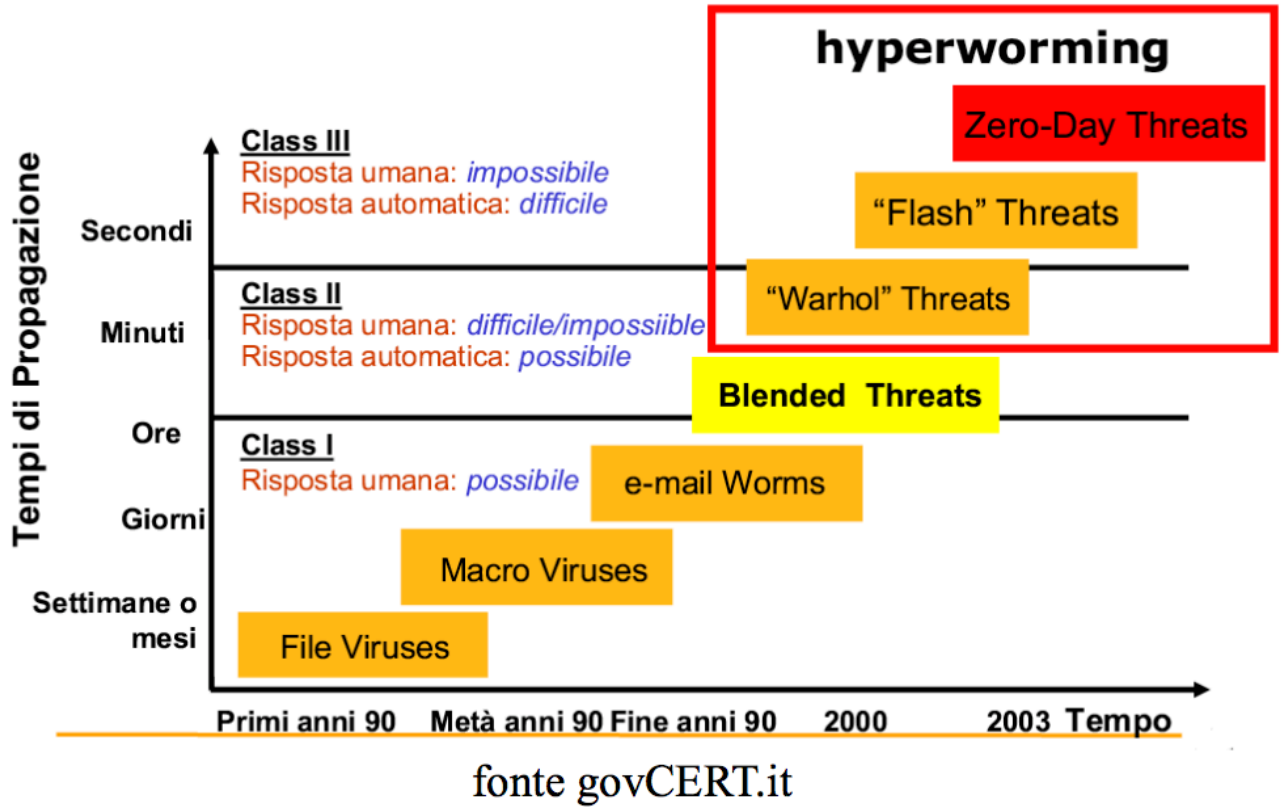
- Conoscere la sorgente da dove si scarica il file e controllare se sia affidabile.
- Controllare se il file che si vuole scaricare corrisponda effettivamente a quello che si sta scaricando.
- Controllare che non vengano scaricati altri file insieme al file che si vuole effettivamente scaricare.
- Controllare che il file scaricato abbia senso sia come formato che come nome, ad esempio se volevo scaricare una immagine controllare che non sia un file excel o eseguibile.
- In ogni caso una volta scaricato il file controllare l'eventuale presenza di virus o trojan tramite un antivirus.

Minacce Software

Worm - *verme*

- sono una evoluzione dei virus
  - a differenza di questo, non necessita di legarsi ad altri programmi eseguibili per diffondersi
- si diffondono attraverso la rete sfruttando tecniche di vulnerabilità note
- il sistema vulnerabile viene attaccato e quindi infettato
- la velocità di diffusione è enorme, solitamente infettano tutti i sistemi vulnerabili nell'arco di 15 minuti

Minacce Software



fonte govCERT.it

Minacce Software

Rootkit

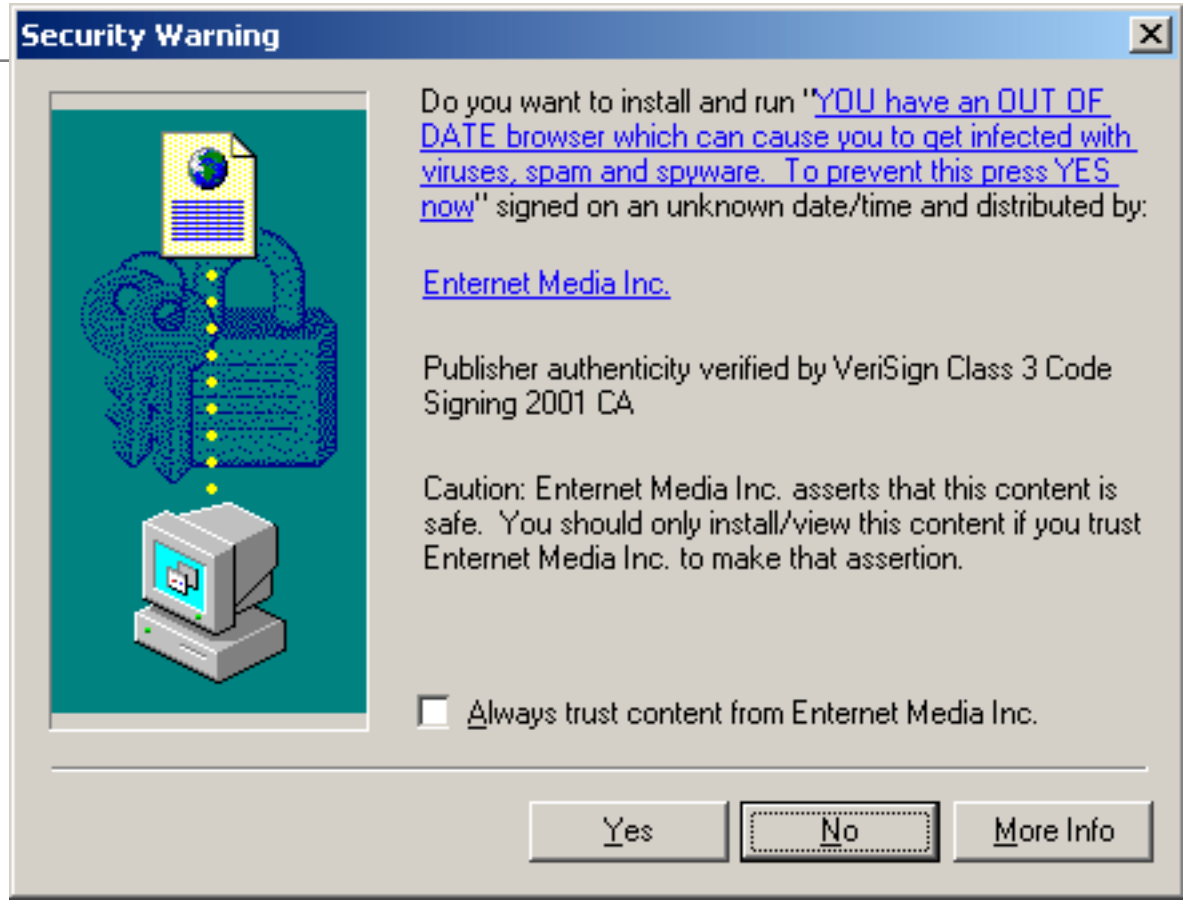
- suite di software malevoli che permette ad un hacker penetrato in un sistema di modificarlo in modo che...
  - il sistema sia sotto il controllo del‘hacker
  - sia molto difficile accorgersi dell'intrusione
- Il termine inglese "Rootkit" deriva dalla concatenazione di due termini: "root" (che indica, tradizionalmente, l'utente con i maggiori permessi nei sistemi) e "kit" (che si riferisce al software che implementa lo strumento)

Minacce Software

SpyWare

- Software che raccolgono informazioni su ciò che l'utente fa o ha installato sul pc e la trasmette ad altri
  - che applicazioni ho installato? che siti visito? che password ho nella mia cache? che carte di credito sto usando?
- si nascondono in applicazioni free di uso comune (approccio trojan)
- è legale distribuirli se la licenza d'uso dichiara l'attività di monitoraggio.
  - quasi mai la licenza d'uso è letta con attenzione


Microsoft Internet Explorer
If your computer is slowing down or crashing, get a free scan of your computer to make sure it is not infected. Scan now and get a fully functional spam blocker for free!
Click OK to start installation.
Advertisement.
OK
Cancel

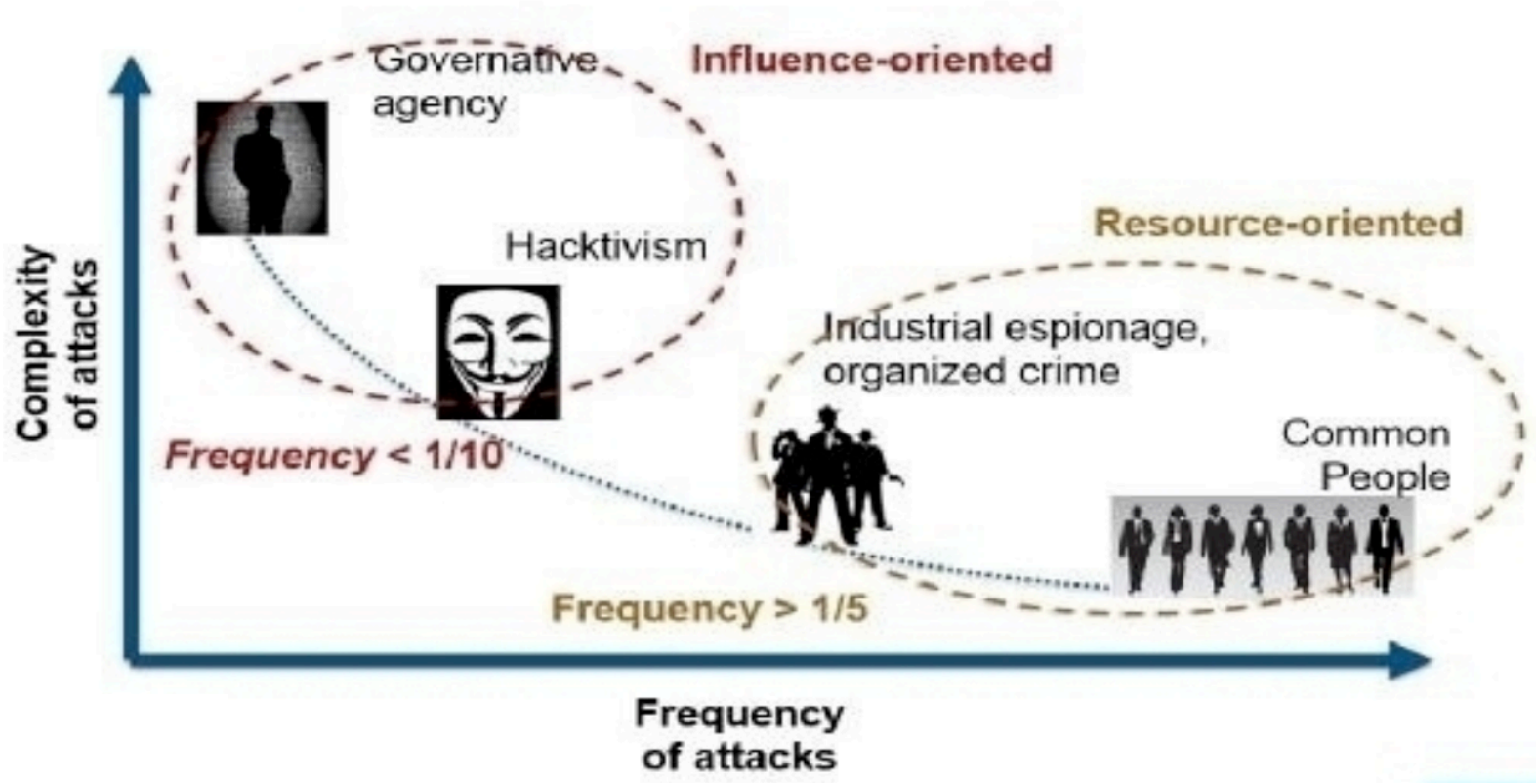

Security Warning
Do you want to install and run "YOU have an OUT OF DATE browser which can cause you to get infected with viruses, spam and spyware. To prevent this press YES now" signed on an unknown date/time and distributed by:
Enternet Media Inc.
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA
Caution: Enternet Media Inc. asserts that this content is safe. You should only install/view this content if you trust Enternet Media Inc. to make that assertion.
Always trust content from Enternet Media Inc.
Yes
No
More Info

Minacce Software

AdWare

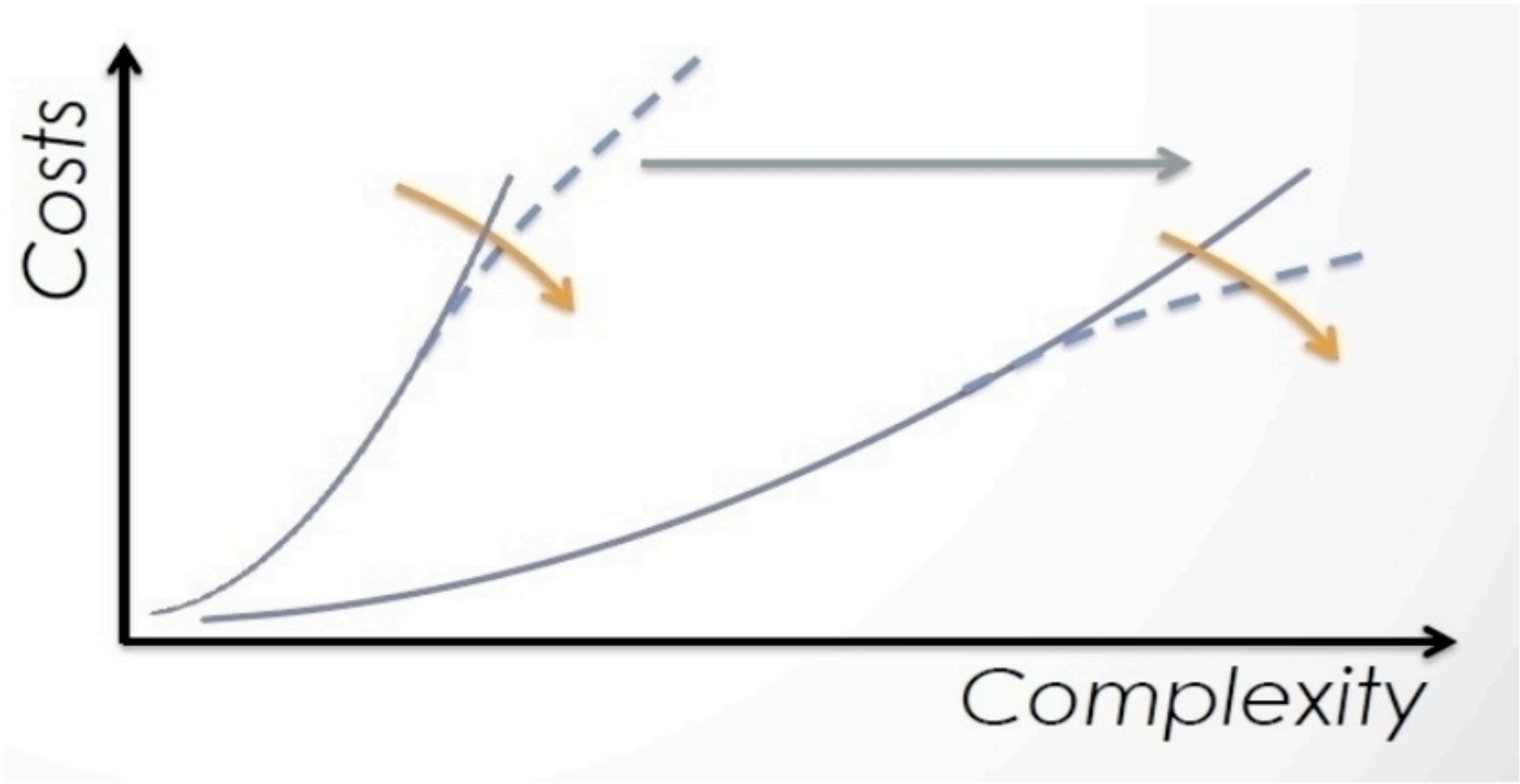
- Una forma di spyware che raccoglie informazioni sull'utente per visualizzare le pubblicità nel browser Web sulla base alle informazioni raccolte

Lo scenario dei rischi

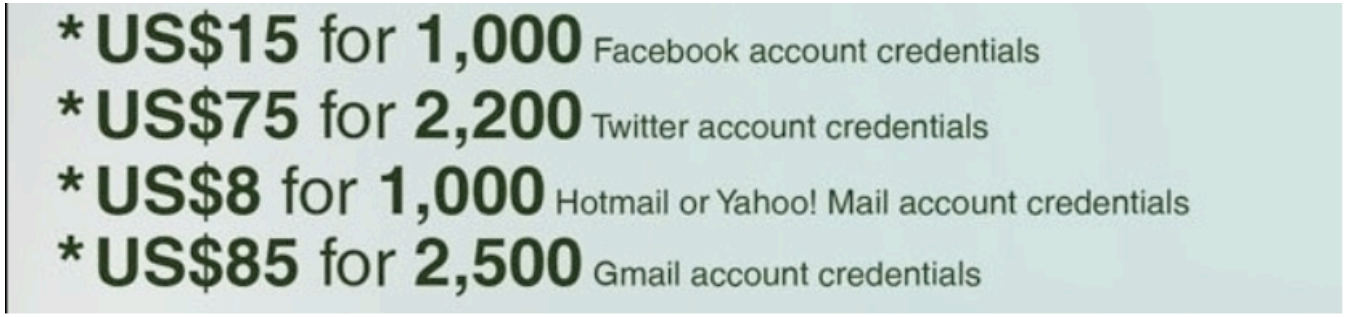


Analisi dei rischi e bilancio dei costi

Miglioramenti tecnologici ed organizzativi



Quanti soldi si guadagnano con i dati rubati?



Quanti soldi si guadagnano con i dati

Estimate of Prices (without PIN, with PIN, PIN and good balance)

Dumps	US			EU			CA, AU		Asia	
Visa Classic	$15	$80		$40	$150		$25	$150	$50	$150
Master Card Standard		$90			$140			$150		$140
Visa Gold/Premier	$25	$100	$200	$45	$160	$250	$30	$160	$55	$150
Visa Platinum	$30	$110		$50	$170		$35	$170	$60	$170
Business/Corporate	$40	$130		$60	$170		$45	$175	$70	$170
Purchasing/Signature	$50	$120		$70			$55		$80	
Infinite				$130	$190		$60	$200		$190
Master Card World		$140								
AMEX	$40			$60			$45		$70	
AMEX Gold	$70			$90			$75		$100	
AMEX Platinum	$50									

Quanti soldi si guadagnano con i dati rubati?

In informatica si definisce **0-day** qualsiasi vulnerabilità di sicurezza non pubblicamente nota e il programma (exploit) che sfrutta questa vulnerabilità per eseguire azioni non normalmente permesse nel sistema in questione. Vengono chiamati 0-day proprio perché lo sviluppatore ha zero giorni per riparare la falla nel programma prima che qualcuno la possa sfruttare

Prices for zero-day vulnerabilities.

Adobe Reader	$5,000–$30,000
Mac OS X	$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

Soluzioni?

Antivirus

- suite software che...
  - verificano che non vi sia traccia di virus negli eseguibili del sistema (approccio reattivo)
  - verificano che non vi sia traccia di virus negli eseguibili che state per eseguire (approccio proattivo)
  - sono in grado di rimuovere virus scoperti
  - contengono un DB di firme di virus noti
  - sono in grado di aggiornare (update) il DB automaticamente via rete

Soluzioni?

Antivirus

- inizialmente gli antivirus erano basati sul riconoscimento di sequenze
- virus mutanti rendono molto più difficile l'intercettazione
- euristiche

Soluzioni?

Antivirus - drawbacks

- F.B. Cohen ,1987, antivirus
  - non esiste un algoritmo per rilevare un qualsiasi virus
- D.M. Chess and S.R. White 2000
  - esistono virus non rilevabili da alcun antivirus

Social Engineering

- l'insieme di tecniche "sociali" che hanno l'obiettivo di manipolare le persone inducendole a...
  - divulgare informazioni confidenziali
  - fare cose contro la politica di sicurezza

Minacce Software

hoax

- email che raggirano l'utente convincendolo a fare cose a suo svantaggio
- Esempio:
  - SULFNBK.EXE è però un programma che è regolarmente parte di Windows!

```
Subject: BAD virus - act quickly!!
Date: Tue, 29 May 2001 21:57:22 -0400

Subject: Please Act Urgently
VIRUS COULD BE IN YOUR COMPUTER
It will become activate on June 1st and will delete all files and folders
   on
the hard drive.
No Anti-Virus software can detect it because it doesn't become a VIRUS
until 1/6/2001.
It travels through the e-mail and migrate to your computer.
To find it please follow the following directions:
Go To "START" button
Go to "Find" or "Search"
Go to files and folders
Make sure to search in drive C
Type in; SULFNBK.EXE
Begin Search
If it finds it, highlight it and delete it
Close the dialogue box
…..
```

Hotmail®

ninemsn part of the Microsoft Network

Urgent Message to all Hotmail® Users

Dear Hotmail®User.

We have been aware of a major increase of users signing up to Hotmail® over the past few months.

We are needing to upgrade our servers to handle this massive internet traffic.

We have also discovered that there are many Hotmail® accounts being unused.

We are asking for your co-operation to "sort through" all Hotmail® email address's and close all of the unused accounts.
Please read the following:

What you need to do to tell us you are using this email account:

When you receive this mail, click on the FORWARD button. **YOU MUST DO THIS NO LONGER THAN 1 DAY OF RECEIVING THIS EMAIL.**
Now, enter **AT LEAST 15 HOTMAIL® EMAIL ADDRESS'S** (so this message can be spread).
Now, **YOU MUST ENSURE THE SUBJECT LINE READS EXACTLY:**

my account is active

Now, click the **SEND** button.

After you have completed this, your email address will be secured.

HOTMAIL®, NINE MSN®, AND THE MICROSOFT CORPORATION®ENSURES YOU THAT THIS ISN'T A 'CHAIN LETTER'.

This process is **NECESSARY FOR THE PROTECTION OF YOUR HOTMAIL® ACCOUNT.**

Queries? Questions? **CONTACT US.** Email support@msn.com, or visit http://help.msn.com

NETFLIX

We're sorry to say goodbye

We've cancelled your Netflix Account. This change will be effective Tuesday, November 8, 2016.

If you've changed your mind and you would like to continue, simply click here : https://www.netflix.com/RestartMembership to enjoy TV shows & movies without interruption.

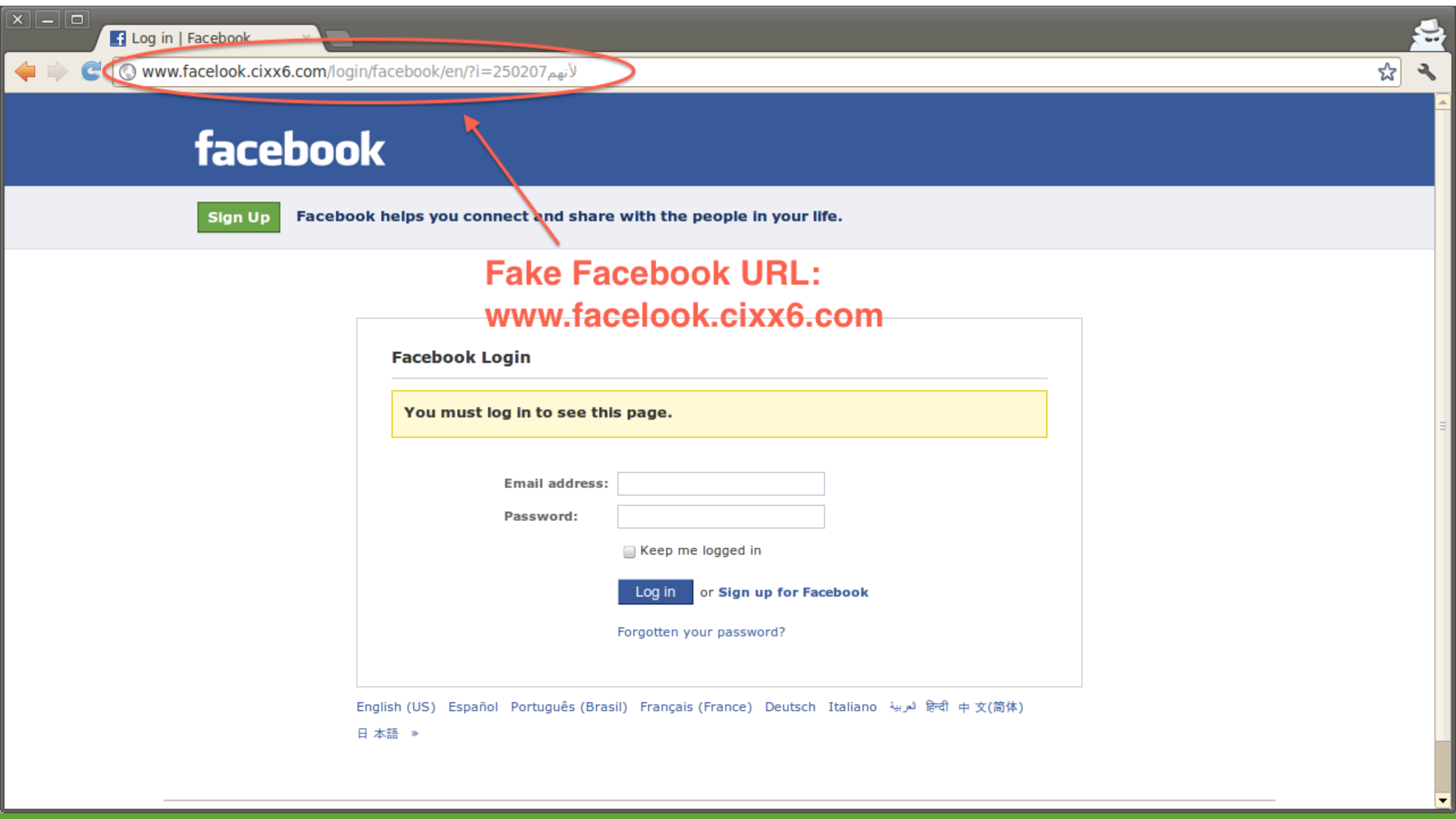
We hope you enjoyed the service – and we'd love to have you back someday.

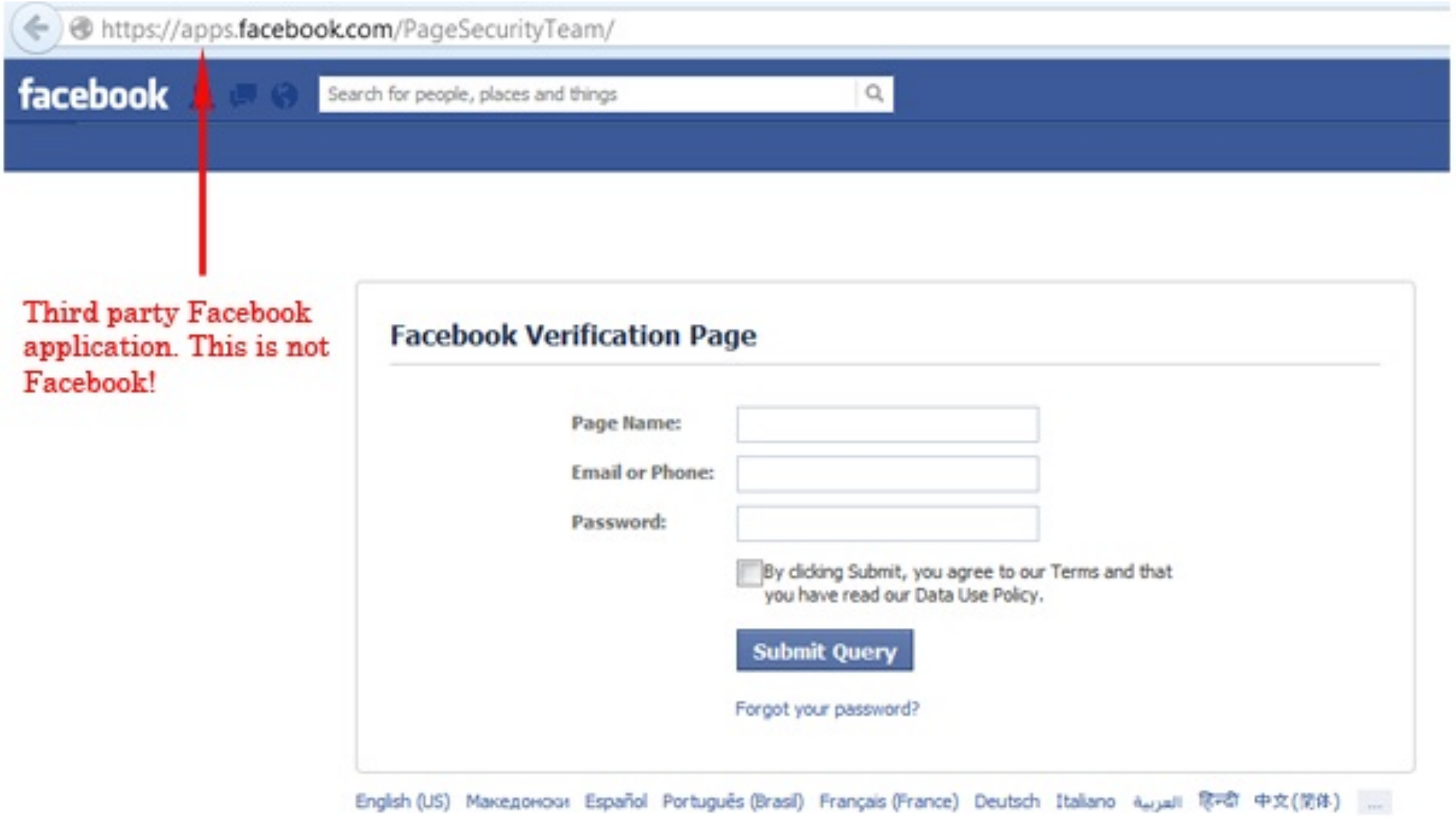
–The Netflix Team

Minacce Software

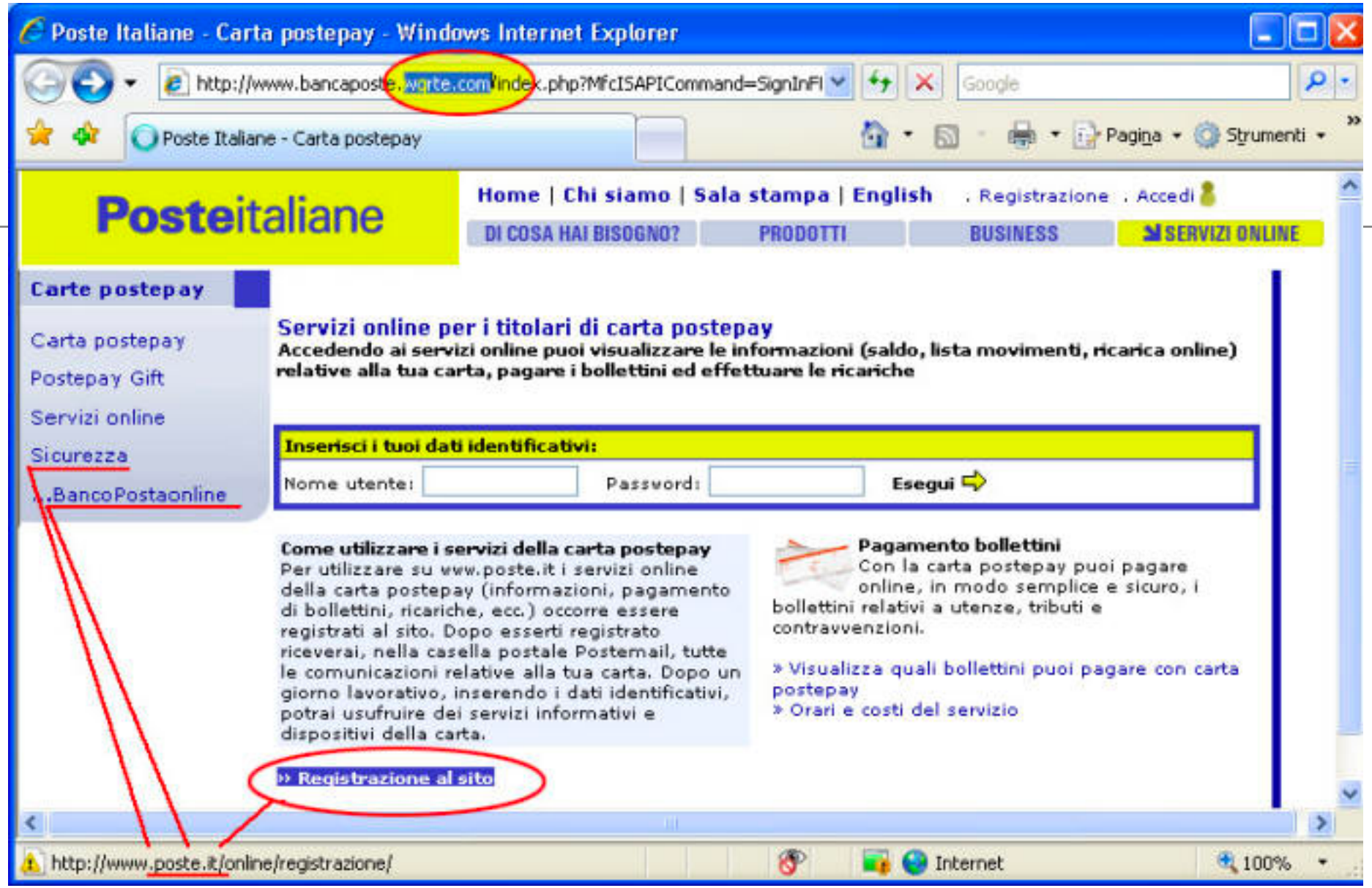
phishing

- acquisizione illegale di informazioni confidenziali (es. passwords) ottenuto “impersonando” una entità fidata
  - la vittima è adescata tipicamente via email
    - ma anche telefonicamente
- l’entità fidata viene spesso impersonata tramite clonazione del sito web
  - con url simili


Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207لأنهم
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Fake Facebook URL:
www.facelook.cixx6.com
Facebook Login
You must log in to see this page.
Email address:
Password:
Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
日本語 »


https://apps.facebook.com/PageSecurityTeam/
facebook
Search for people, places and things
Third party Facebook application. This is not Facebook!
Facebook Verification Page
Page Name:
Email or Phone:
Password:
By clicking Submit, you agree to our Terms and that you have read our Data Use Policy.
Submit Query
Forgot your password?
English (US) Македонски Español Português (Brasil) Français (France) Deutsch Italiano العربية 中文(简体)


From:
on behalf of
Amazon <management@mazoncanada.ca>
not an Amazon email address
(note the missing A in Amazon)
To:
@sheridanc.on.ca
Cc:
Subject: Suspension
amazon.com
Dear Client,
Generic non-personalized greeting
We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.
To confirm your identity with us click the link bellow:
https://www.amazon.com/exec/obidos/sign-in.html
Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"
Sincerely,
The Amazon Associates Team
© 1996-2013, Amazon.com, Inc. or its affiliates


Poste Italiane - Carta postepay - Windows Internet Explorer
http://www.bancaposte.wqrte.com/index.php?MfcISAPICommand=SignInFl
Google
Poste Italiane - Carta postepay
Pagina
Strumenti
Posteitaliane
Home | Chi siamo | Sala stampa | English
. Registrazione . Accedi
DI COSA HAI BISOGNO?
PRODOTTI
BUSINESS
SERVIZI ONLINE
Carte postepay
Carta postepay
Postepay Gift
Servizi online
Sicurezza
..BancoPostaonline
Servizi online per i titolari di carta postepay
Accedendo ai servizi online puoi visualizzare le informazioni (saldo, lista movimenti, ricarica online) relative alla tua carta, pagare i bollettini ed effettuare le ricariche
Inserisci i tuoi dati identificativi:
Nome utente:
Password:
Esegui
Come utilizzare i servizi della carta postepay
Per utilizzare su www.poste.it i servizi online della carta postepay (informazioni, pagamento di bollettini, ricariche, ecc.) occorre essere registrati al sito. Dopo esserti registrato riceverai, nella casella postale Postemail, tutte le comunicazioni relative alla tua carta. Dopo un giorno lavorativo, inserendo i dati identificativi, potrai usufruire dei servizi informativi e dispositivi della carta.
» Registrazione al sito
Pagamento bollettini
Con la carta postepay puoi pagare online, in modo semplice e sicuro, i bollettini relativi a utenze, tributi e contravvenzioni.
» Visualizza quali bollettini puoi pagare con carta postepay
» Orari e costi del servizio
http://www.poste.it/online/registrazione/
Internet
100%