

Social Engineering - Vettori di attacco

Paolo PRINETTO

Direttore

CINI Cybersecurity
National Laboratory



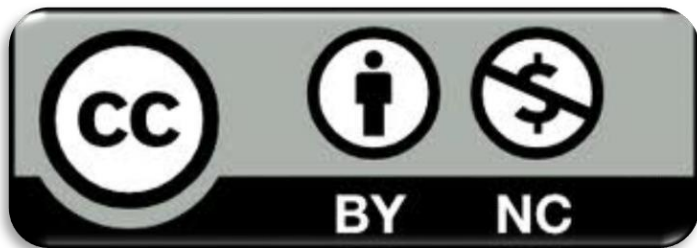
<https://cybersecnatlab.it>

License & Disclaimer

2

License Information

This presentation is licensed under the
Creative Commons BY-NC License



To view a copy of the license, visit:

<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Obiettivo della presentazione

3

- Introdurre il concetto di social engineering
- Analizzare nel dettaglio i vettori di attacco più utilizzati nell'ambito della social engineering
- Proporre, di volta in volta, adeguate contromisure

Prerequisiti

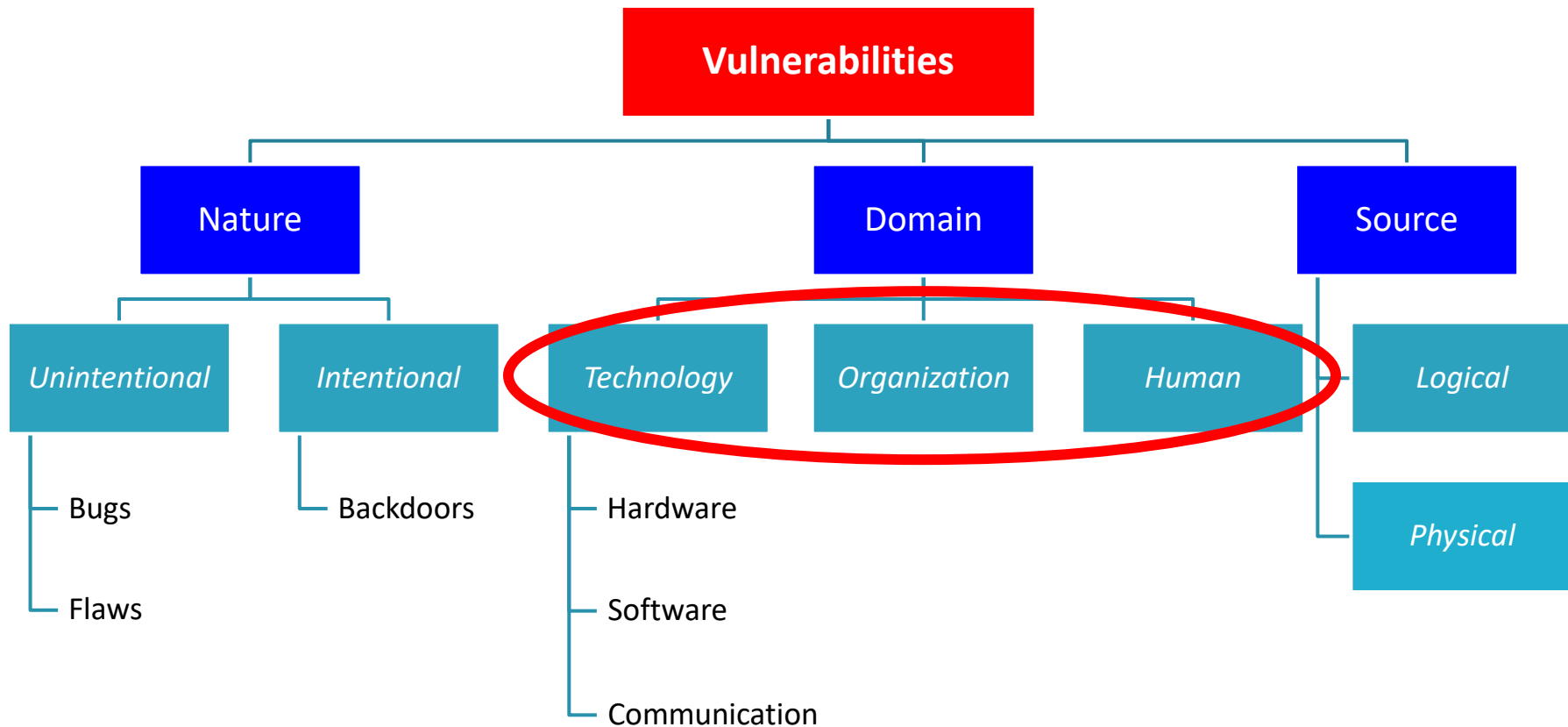
4

➤ Nessuno

Approfondimenti

5

- Alla lezione, dopo l'ultima slide, sono state aggiunte delle slide che presentano degli *Approfondimenti* relativi ad alcuni degli argomenti trattati.



Classifica

7

- Come classificare queste vulnerabilità in base alla loro “pericolosità” nei confronti della security?

Classifica

8



Classifica

9



Aspetti
tecnologici
(HW/SW)

Classifica

10

Aspetti
organizzativi



Aspetti
tecnologici
(HW/SW)

Classifica

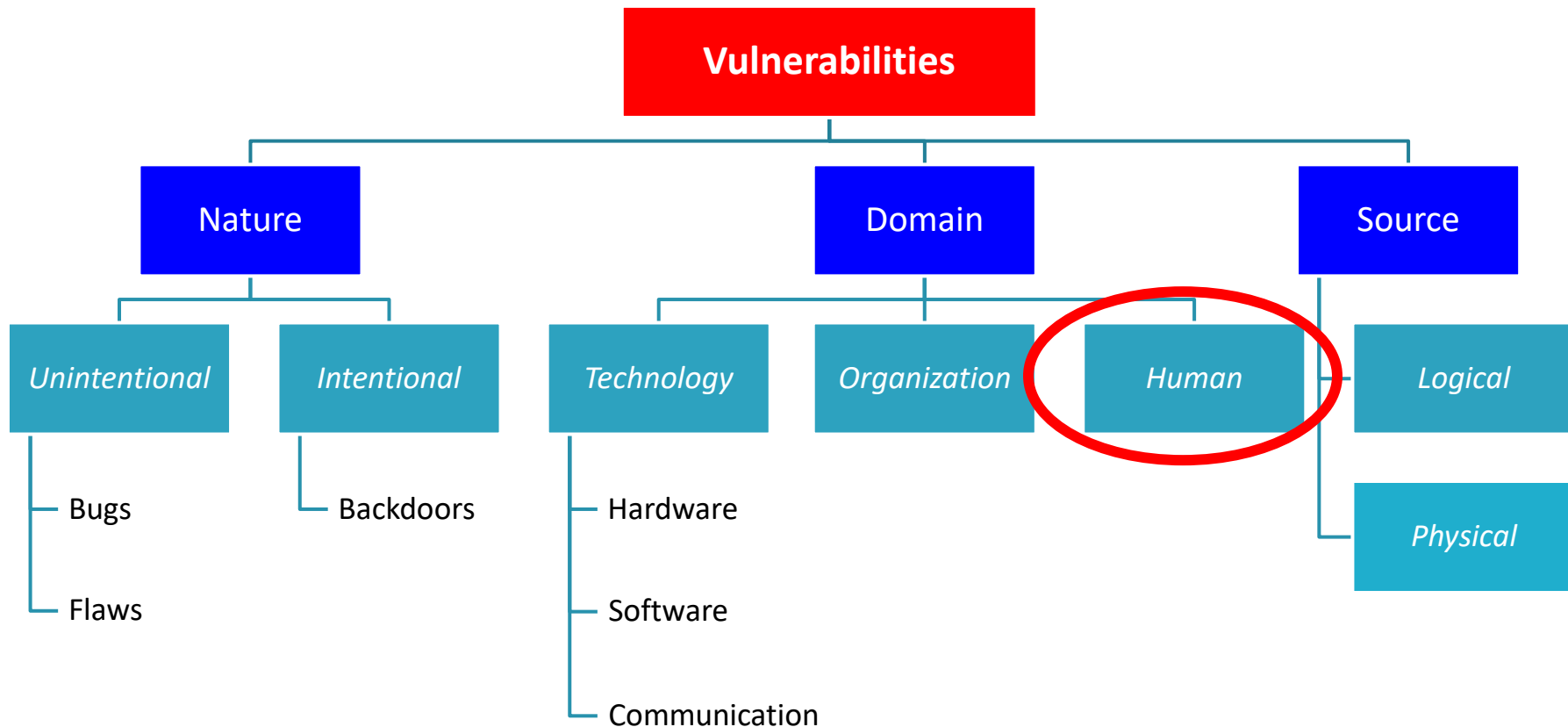
11

Fattore
umano

Aspetti
organizzativi

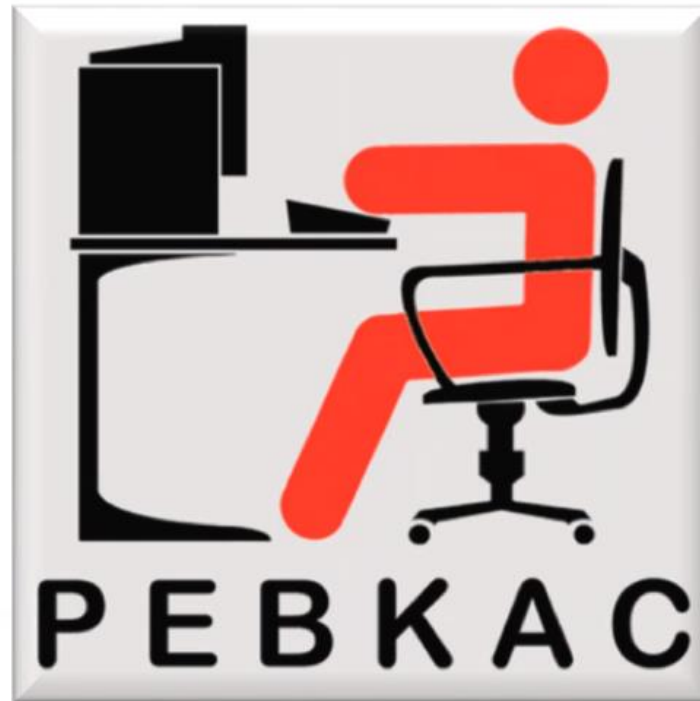
Aspetti
tecnologici
(HW/SW)





L'uomo è sempre l'anello debole !!

13



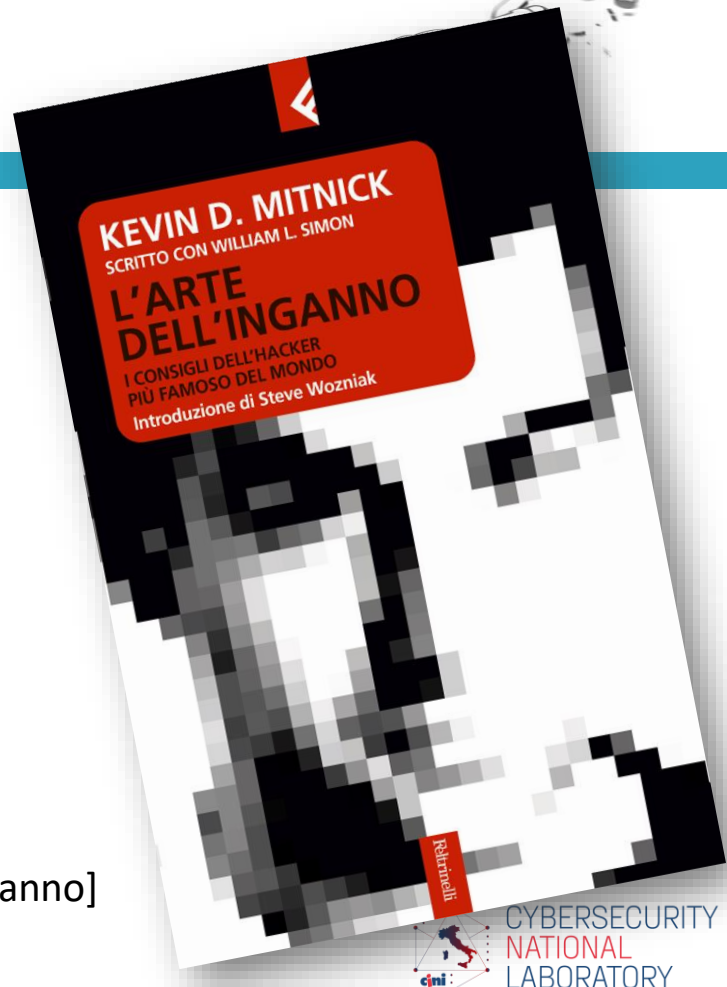
Problem Exist Between Keyboard And Chair

L'anello debole

14

*“Non importa quanto siano forti i vostri firewall, i sistemi di rilevamento delle intrusioni, la crittografia, gli antivirus, voi siete sempre l'anello debole della sicurezza informatica!
Le persone sono più vulnerabili dei computer”*

[Kevin D. Mitnick & William L. Simon – L'Arte dell'Inganno]



Vulnerabilità a livello umano

15

- Scarsa consapevolezza e cultura da parte di TUTTE le persone coinvolte
- Errata percezione dei rischi
- *Ingegneria sociale*

Social Engineering



16

- L'arte e la scienza del far fare alle persone quel che si desidera

[Harl - People Hacking: The Psychology of Social Engineering]

Social Engineering



17

- Combinazione di tecniche sociologiche, psicologiche e di raccolta di informazioni utilizzate per manipolare le persone con l'obiettivo finale di
 - convincerle a rilasciare informazioni sensibili
 - compiere azioni che non rispettano le normali misure di sicurezza
 - farle agire in maniera tale da consentire l'accesso o l'uso non autorizzato di sistemi, reti, dati, informazioni

Social Engineering

18

- *“L’uso del proprio ascendente e delle capacità di persuasione per ingannare o manipolare gli altri convincendoli che l’ingegnere sociale sia quello che non è.”*

[Kevin D. Mitnick & William L. Simon – L’Arte dell’Inganno]



Social Engineering – Come è possibile?

19

Analisi del *Fattore Umano*

20

- Gli esseri umani:
 - sono sistemi “complessi”
 - hanno delle vulnerabilità prevalentemente basate su:
 - tratti comportamentali
 - *buona fede* esercitata dagli individui nei rapporti sociali
 - *bias cognitivi*

Alcuni bias cognitivi

21

- L'ego
- La fiducia nell'autorità
- La voglia di rendersi utile
- La paura di perdere
- La pigrizia o l'ignoranza
- La tendenza a fidarsi
- La non consapevolezza del valore delle informazioni
- L'entusiasmo nel ricevere un vantaggio o una ricompensa

Video interessante

22

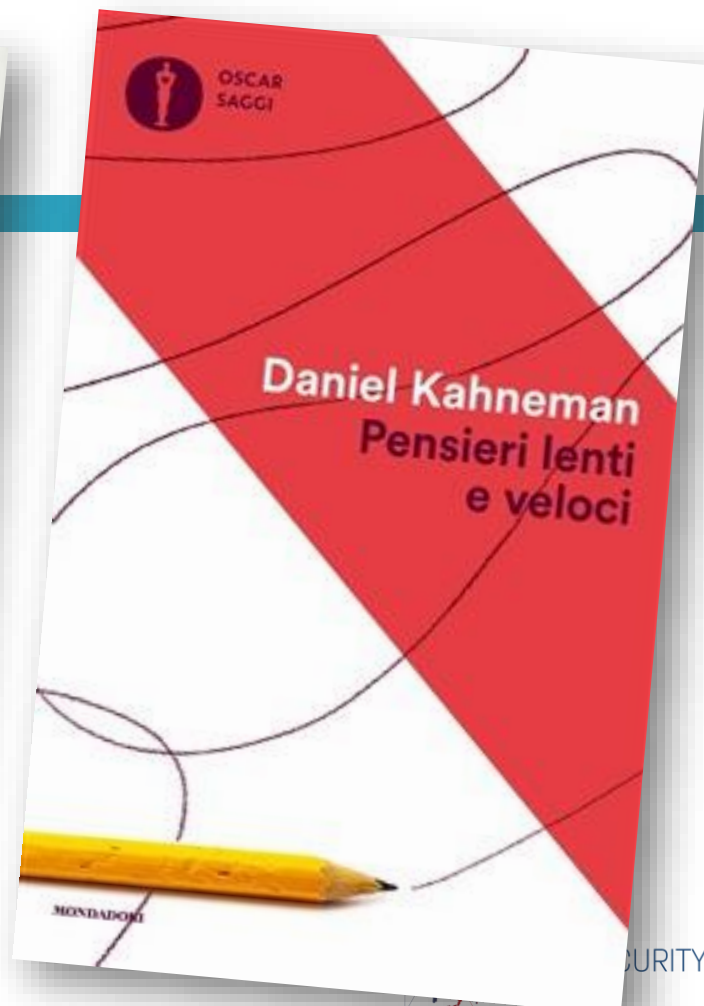
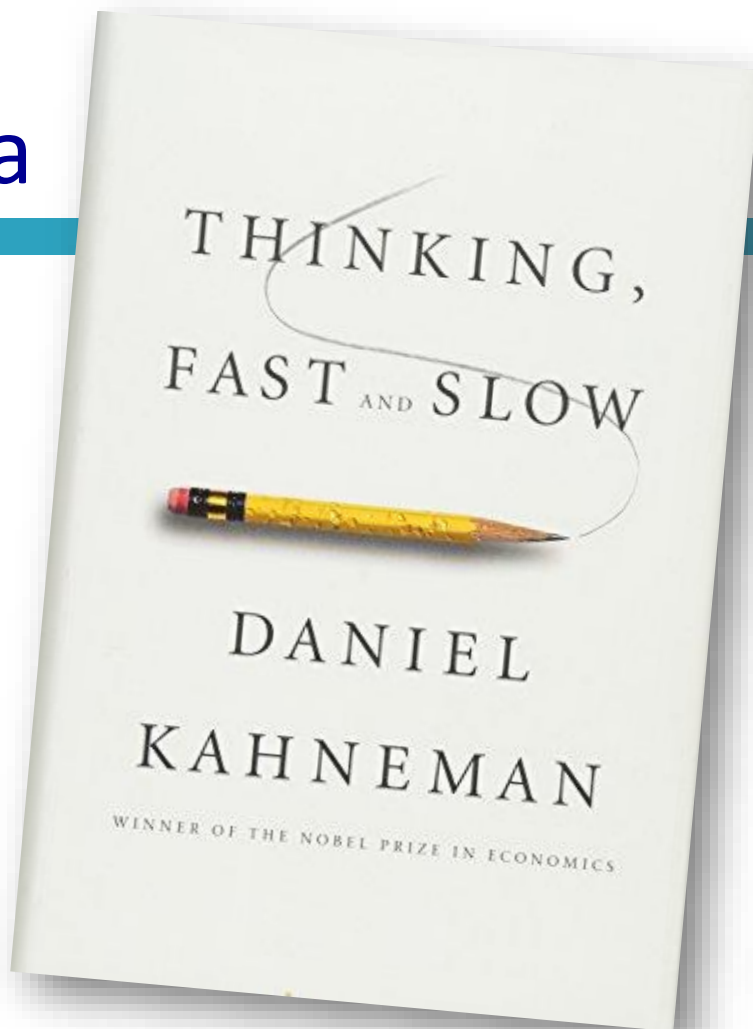
➤ <https://www.facebook.com/Mensaltalia/videos/>

BIAS

COGNITIVI

Lettura consigliata

24



Social Engineering - Target

25

- Ciascuno di noi può essere la vittima prescelta
- Target primario è spesso il personale di help desk, segretariale o di supporto

Social Engineering - Target

26

- Ciascuno di noi può essere la vittima prescelta
- Target primario è spesso il personale di help desk, segretariale o di supporto
- Perché spendere tempo nel cercare le vulnerabilità di un sistema, quando con l'inganno se ne può ottenere la password?

Social Engineering – I vettori di attacco

27

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Social Engineering – I vettori di attacco

28

➤ Varie tipologie di *pesca*:

➤ Phishing

- Spear Phishing
- Whaling

➤ Vishing

➤ Via social

- OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Social Engineering – I vettori di attacco

29

➤ Varie tipologie di *pesca*:

➤ Phishing

- Spear Phishing
- Whaling

➤ Vishing

➤ Via social

- OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

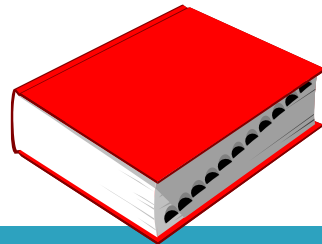
➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Phishing



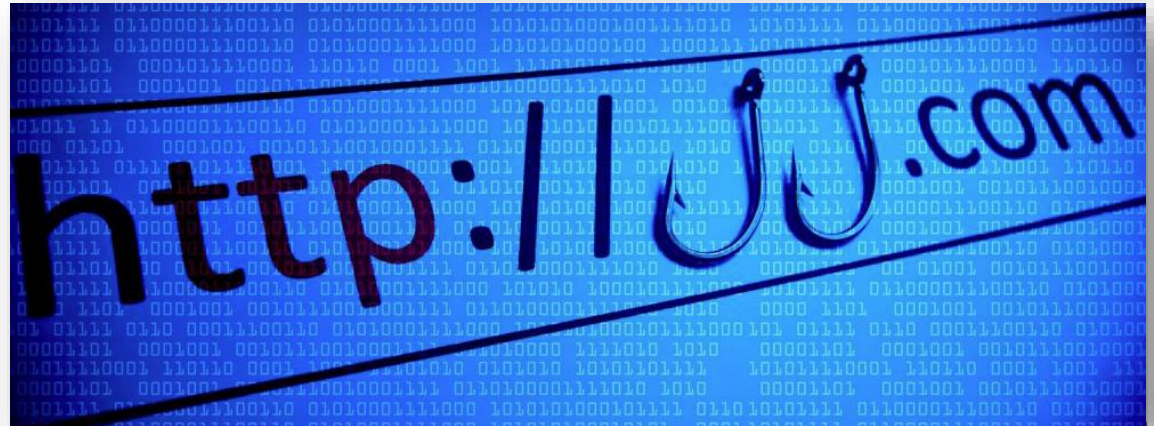
30

- Truffa *via Internet* in cui l'aggressore cerca di ingannare la vittima inducendola a:
 - Fornire informazioni personali, come credenziali d'accesso, dettagli sul conto corrente bancario e sulle carte di credito;
 - Aprire allegati che contengono malware.

Phishing – Come si realizza

31

- Tipicamente tramite l'invio, più o meno mirato, di e-mail che imitano nella grafica e nelle impostazioni siti bancari o postali con le quali si richiede di inviare dati personali.



Phishing – Esempio *banale*

32

PoliTO

Your PoliTO eMAIL Has Expired

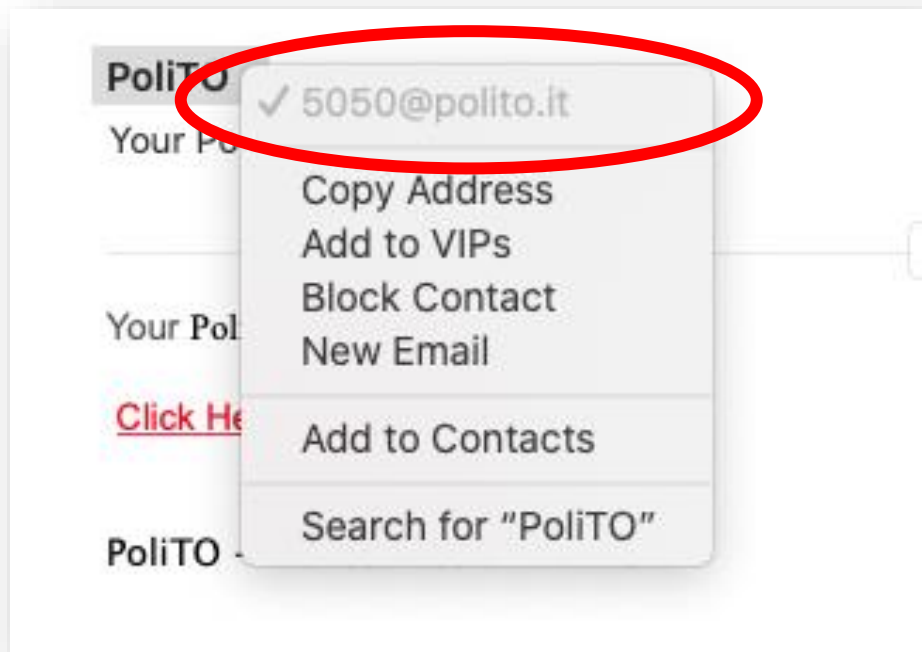
Your PoliTO eMAIL Has Expired

[Click Here To Renew](#)

PoliTO – Politecnico di Torino

Phishing – Esempio *banale*

33



Phishing – Esempio *banale*

34

PoliTO

Your PoliTO eMAIL Has Expired

Your PoliTO eMAIL Has Expired

[Click Here To Renew](#)

[https://templatesbazaar.com/fatwaonline/test/
mail.polito.it.html](https://templatesbazaar.com/fatwaonline/test/mail.polito.it.html)

PoliTO – Politecnico di Torino

Phishing

35

➤ Esempio *molto meno banale*

Aruba.it

Inbox - ...to@polito.it 20 April 2020 at 08:41

A

Problema di pagamento

To: Paolo PRINETTO,

Reply-To: Aruba.it

aruba.it

Gentile cliente

ti informiamo che le tue informazioni di pagamento non sono valide.
ti informiamo che il dominio [ARUBA.it](https://www.aruba.it), a cui risulta collegato questo account di posta, scadrà il giorno **21/04/2020**
Desideriamo ricordare che, qualora il dominio non venga rinnovato entro tale data, questi e tutti i servizi associati, comprese le caselle di posta verranno disattivate e non potranno più essere utilizzate per l'invio e la ricezione.

COME RINNOVARE IL DOMINIO?

L'operazione di rinnovo è semplice e veloce: è sufficiente effettuare l'ordine online e relativo pagamento.

RINNOVA ORA CON UN CLICK

Per visualizzare il riepilogo dell'ordine e l'importo da pagare, puoi procedere al rinnovo da questa pagina.

Se il tuo stato non viene risolto entro 48 ore, sospenderemo definitivamente i tuoi servizi.

Grazie per la collaborazione

Cordiali saluti

Customer Care Aruba S.p.a.

www.aruba.it

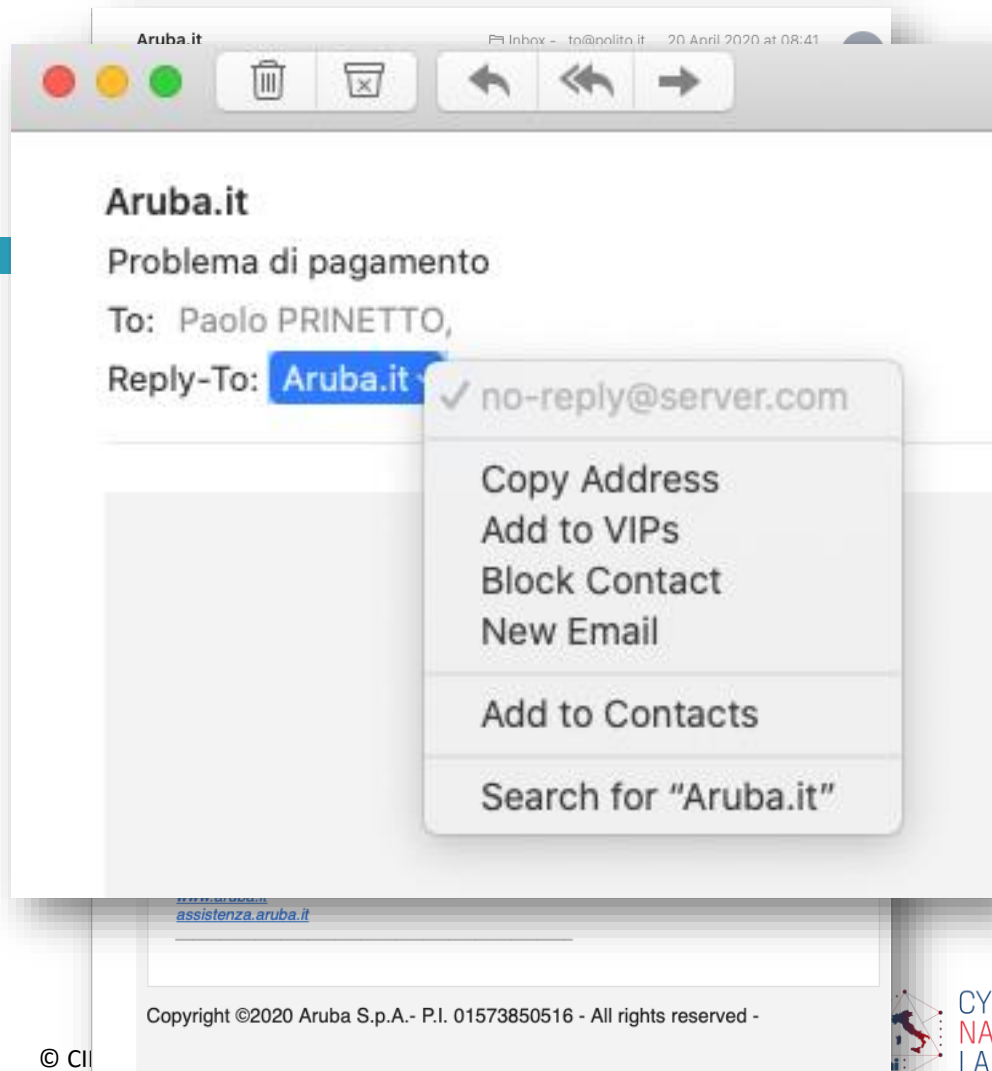
assistenza.aruba.it

Copyright ©2020 Aruba S.p.A.- P.I. 01573850516 - All rights reserved -

Phishing

36

- Esempio *molto meno banale*



Phishing

37

➤ Esempio *molto meno banale*

Aruba.it

Inbox - ...to@polito.it 20 April 2020 at 08:41

A

Problema di pagamento

To: Paolo PRINETTO,

Reply-To: Aruba.it

aruba.it

Gentile cliente

ti informiamo che le tue informazioni di pagamento non sono valide.
ti informiamo che il dominio [ARUBA.it](http://aruba.it), a cui risulta collegato questo account di posta, scadrà il giorno **21/04/2020**
Desideriamo ricordare che, qualora il dominio non venga rinnovato entro tale data, questi e tutti i servizi associati, comprese le caselle di posta verranno disattivate e non potranno più essere utilizzate per l'invio e la ricezione.

COME RINNOVARE IL DOMINIO?

L'operazione di rinnovo è semplice e veloce: è sufficiente effettuare l'ordine online e relativo pagamento.

RINNOVA ORA CON UN CLICK

<http://rangapselari.com/A85073P666X6T5/>

Per visualizzare il riepilogo dell'ordine e l'importo da pagare, puoi procedere al rinnovo da questa pagina.

Se il tuo stato non viene rinnovato entro 48 ore, perderemo definitivamente i tuoi servizi.

Grazie per la collaborazione

Cordiali saluti

Customer Care Aruba S.p.a.

www.aruba.it

assistenza.aruba.it

Copyright ©2020 Aruba S.p.A.- P.I. 01573850516 - All rights reserved -

Phishing - Contromisure

38

- Non clickate su alcun link presente in email sospette
- Non aprite né salvate mai gli allegati a email sospette, neppure se in formati che potresti ritenere sicuri (es., immagine)
- Ricorda che nessuna organizzazione seria ti chiederà mai di inviare password né di cliccare su un link incluso in una email

Phishing - Contromisure

39

- Se ricevete email sospette, inoltratele a
infected@csirt.gov.it



Presidenza del Consiglio dei Ministri - *Sistema di Informazione per la Sicurezza della Repubblica*



CSIRT

Computer Security Incident Response Team - Italia

HOME CHI SIAMO NORMATIVA SEGNALAZIONI GLOSSARIO NEWS FAQ



Cerca



Social Engineering – I vettori di attacco

40

➤ Varie tipologie di *pesca*:

➤ Phishing

➤ Spear Phishing

➤ Whaling

➤ Vishing

➤ Via social

➤ OSInt & SocMInt

➤ Spacciarsi per altri:

➤ Impersonation

➤ Do ut des

➤ Quid pro Quo

➤ Attacchi *fisici*:

➤ Baiting

➤ Dumpster Diving

➤ Piggybacking o Shoulder Surfing

➤ Physical Access

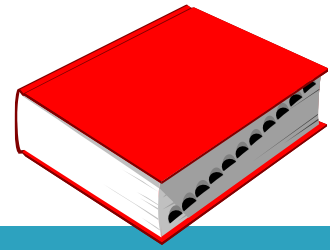
➤ *Bufale*:

➤ Hoaxing

➤ Fake news

➤ Fake software – Trojan

Spear Phishing



41

- È una forma mirata di phishing orientata a colpire una vittima accuratamente selezionata.
- Il mezzo tecnico dell'attacco, e-mail o sito web, sarà costruito appositamente per risultare credibile nei confronti della vittima prescelta, ed essere così più efficace al fine di ottenere delle particolari informazioni a cui l'attaccante intende arrivare.

Spear Phishing - Contromisure

42

- Magari la email che ricevi cita il nome di un collega, si riferisce alle attività che svolgi, o ai tuoi interessi, hobby, parenti, contiene gli auguri per il tuo compleanno, etc.
- Sospetta sempre delle email che ti destano anche minima sorpresa, quindi non già sollecitate o attese.
- Verifica sempre con mezzi alternativi (es. telefono) il contenuto di email che comunicano modifiche di modalità di comunicazione.

Social Engineering – I vettori di attacco

43

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Whaling



44

- Attacchi di spear phishing diretti specificamente verso senior executive e altre persone di elevato profilo nell'ambito di una organizzazione.

Whaling

45

- Attacchi di spear phishing diretti specificamente verso senior executive e altre persone di elevato profilo nell'ambito di una organizzazione.
- Il termine whaling (da whale - balena) è stato coniato per questi tipi di attacco per evidenziare la “grandezza” e l'importanza degli obiettivi

Whaling ??

46



Approfondimento Rai

Ecco la strana storia della tentata truffa alla Rai di Marcello Foa

true

09 MAGGIO 2020

Un anno fa la mail di un sedicente ministro Tria convince il presidente ad autorizzare una operazione da un milione di euro. La truffa è sventata ma svela una trama internazionale che porta in Israele

Rai, un falso ministro Tria cerca di truffare il presidente Foa

Al dirigente di Viale Mazzini è arrivata in primavera una e-mail firmata dall'allora ministro dell'Economia con una richiesta di fondi per un progetto internazionale. D'accordo con l'ad Salini è partita la denuncia. Ma il dem Anzaldi contesta la ricostruzione dell'azienda: "Fatti gravissimi"

14 dicembre 2019

ABBONATI A

Rep:



Commenti



Tentata truffa alla Rai e al presidente del Cda Marcello Foa che ha ricevuto una e-mail firmata Giovanni Tria, all'epoca ministro dell'Economia, con la richiesta di fondi per sviluppare un progetto all'estero. L'incredibile vicenda - ricostruita dall'AdnKronos che ricorda come anche Repubblica si fosse occupata della vicenda - è iniziata prima dell'estate, quando nella casella postale del presidente della Rai si è

materializzata la e-mail con la richiesta di soldi firmata Giovanni Tria e il numero di conto corrente su cui accreditare la somma. Foa ha parlato della



ria della tentata truffa alla
a

ministro Tria convince il presidente ad autorizzare
La truffa è sventata ma svela una trama

Social Engineering – I vettori di attacco

48

➤ Varie tipologie di *pesca*:

➤ Phishing

➤ Spear Phishing

➤ Whaling

➤ Vishing

➤ Via social

➤ OSInt & SocMInt

➤ Spacciarsi per altri:

➤ Impersonation

➤ Do ut des

➤ Quid pro Quo

➤ Attacchi *fisici*:

➤ Baiting

➤ Dumpster Diving

➤ Piggybacking o Shoulder Surfing

➤ Physical Access

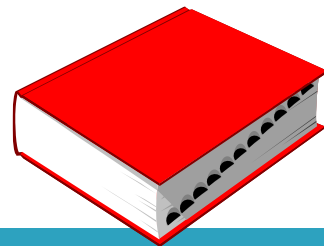
➤ *Bufale*:

➤ Hoaxing

➤ Fake news

➤ Fake software – Trojan

Vishing



49

- È una tecnica di phishing realizzata tramite chiamate telefoniche.

Vishing

50

- Sfrutta la fiducia dell'attaccato nei confronti di un'istituzione, quale una banca o una compagnia telefonica, per richiedere informazioni sensibili.
- L'attaccante può dotarsi di strumentazione IVR - Interactive Voice Response per simulare sistemi di interazione e comunicazione automatizzata come quelli in dotazione a molti call center.

Esempio

51

➤ <https://www.youtube.com/watch?v=lc7scxvKQOo>

**WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES**

Vishing - Contromisure

53

- Siamo sicuri che chi sta chiamando sia veramente il tecnico IT, l'amministratore di rete o la segretaria del Direttore?

Social Engineering – I vettori di attacco

54

➤ Varie tipologie di *pesca*:

➤ Phishing

- Spear Phishing
- Whaling

➤ Vishing

➤ Via social

- OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Via Social

55

- Le campagne di spear phishing sono realizzate raccogliendo dapprima informazioni sulla vittima (*information gathering*)
- I social network sono lo strumento preferito dagli attaccanti per la raccolta di informazioni

Le conseguenze ...

56

- Due video che ho trovato particolarmente significativi:
 - <https://www.youtube.com/watch?v=84Cy5fTM0fY>

Pizzeria Google

57



Le conseguenze ...

58

- Due video che ho trovato particolarmente significativi:
 - <https://www.youtube.com/watch?v=84Cy5fTM0fY>
 - <https://www.youtube.com/watch?v=2HQg1yUGW1Q>

Suggerimento

60

- Tramite il sito del Lab. Naz. Cybersecurity:

<https://cybersecnatlab.it>

guardate i video di sensibilizzazione prodotti da Stefano Ribaldi in collaborazione con la Polizia Postale e il Lab. stesso.

Via Social - Contromisure

61

- Limita il più possibile la divulgazione via Web delle tue informazioni personali, anche se non riservate
- Verifica le richieste di amicizia prima di accettarle, pubblica il meno possibile, proteggi i tuoi dati, le tue foto, le tue informazioni
- Non postare MAI foto di minori

Via Social - Contromisure

62

- Chat di Facebook, Whatsapp, Skype, etc., anche semplici sms possono essere malevoli
- Attenzione anche al fatto che il link malevolo potrebbe contenere il tuo nome o il nome dell'account, per invogliarti a cliccare
- Ricorda sempre, il phishing non avviene solo via email!

Social Engineering – I vettori di attacco

63

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

OSInt – Open Source Intelligence

SocMInt – Social Media Intelligence

64

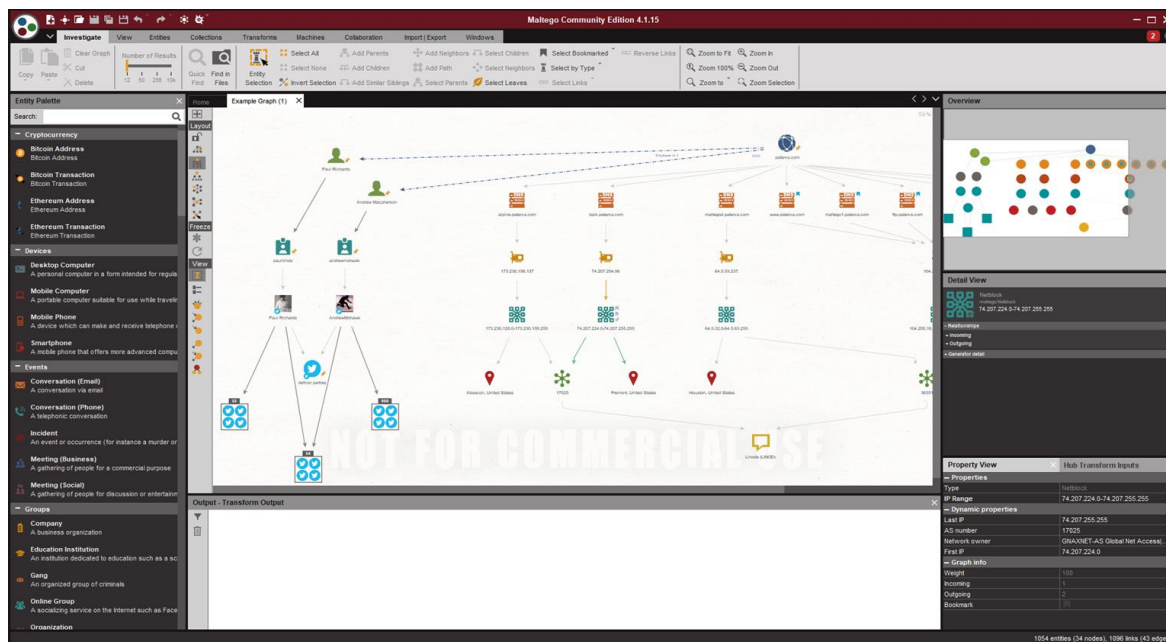
- Sfruttare i social media (SocMInt) e le informazioni personali accessibili su canali pubblici (OSInt) per raccogliere informazioni
- Molto spesso è il primo passo per strutturare un attacco di spear phishing

OSInt – Open Source Intelligence

SocMInt – Social Media Intelligence

65

➤ Usano tool sofisticati, quali Maltego



<https://www.maltego.com>

Maltego

66

- Strumento interattivo per il mining di informazioni
 - Usa pagine web, social networks, indirizzi mail, ...
- Costruisce un grafo di relazioni
 - Es. collega indirizzi mail a un sito web

Social Engineering – I vettori di attacco

67

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

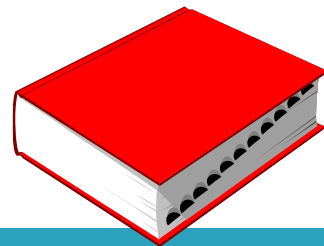
➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

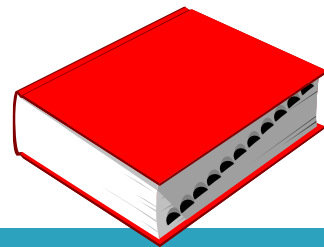
Impersonation



68

- Consiste nel fingersi qualcuno per:
 - ottenere informazioni o
 - effettuare un'operazione ostile o illecita.

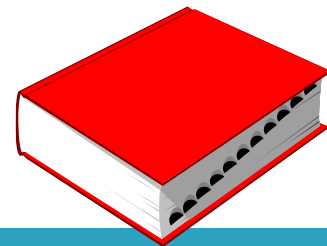
Do ut des



69

- L'attaccante offre alla vittima un regalo, un compenso o un benefit, facendo leva sulla possibilità che tali beni materiali possano attivare una dinamica di scambio reciproco di favori, rendendo la vittima più propensa a rispondere positivamente a una sua futura richiesta.

Quid pro quo



70

- L'attaccante offre alla vittima un servizio in cambio di credenziali di accesso.

Quid pro quo - Esempio

71

➤ L'attaccante:

- chiama a caso dei numeri di una azienda, spacciandosi per il supporto tecnico
- prima o poi trova qualcuno con un problema reale
- lo richiama con gentilezza e questi seguirà le sue istruzioni
- "aiuta" la vittima, ma in realtà le farà anche digitare dei comandi che gli permetteranno di installare un malware

Quid pro quo - Contromisure

72

- Sospettare di chiamate telefoniche indesiderate, visite o e-mail non richieste da parte di persone che chiedono informazioni interne
- Non fornire informazioni personali o aziendali se non dopo aver verificato l'autenticità dell'interlocutore

Social Engineering – I vettori di attacco

73

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Social Engineering – I vettori di attacco

74

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

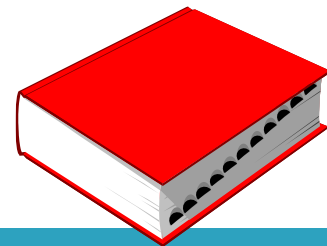
➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Baiting



75

- Prevede l'utilizzo di un'esca per attirare la vittima.

Baiting

76

- Si tratta spesso di un'esca fisica, di un supporto informatico, quale una chiavetta USB (pendrive), che viene lasciata incustodita dall'attaccante in un luogo dove possa essere presa e utilizzata dalla vittima per imprudenza o leggerezza.



Parking lot



Outside



Common room



Classroom



Hallway

Esempi

77



Esempi

78



Come è possibile?

79

- Sfruttano i cosiddetti attacchi *Human Interface Device (HID)* o *USB drive-by*

[<https://www.cyberpointllc.com/posts/cp-human-interface-device-attack.html>]

Attacchi HID

80

- Un attaccante prende:
 - una piattaforma di sviluppo embedded programmabile quale Teensy 3.2
 - un pacchetto software associato, quale Peensy o Social Engineering Toolkit (SET)



Attacchi HID

81

- Poi crea un dispositivo USB che, quando viene collegato a un computer, simula una serie predeterminata di comandi (sequenze di tasti) in grado di installare nel computer un programma malevolo (payload)
- I payload che vengono caricati ed eseguiti sono:
 - altamente configurabili
 - in grado di funzionare su Linux, Windows e Mac OS X.

Costi associati

82

- Teensy 3.2 può essere acquistato per circa 19-25 US\$:
 - https://www.amazon.com/PJRC-Teensy-3-2/dp/B015M3K5NG/ref=sr_1_1?ie=UTF8&qid=1476725192&sr=8-1&keywords=teensy+3.2
 - <https://www.pjrc.com/store/teensy32.html>

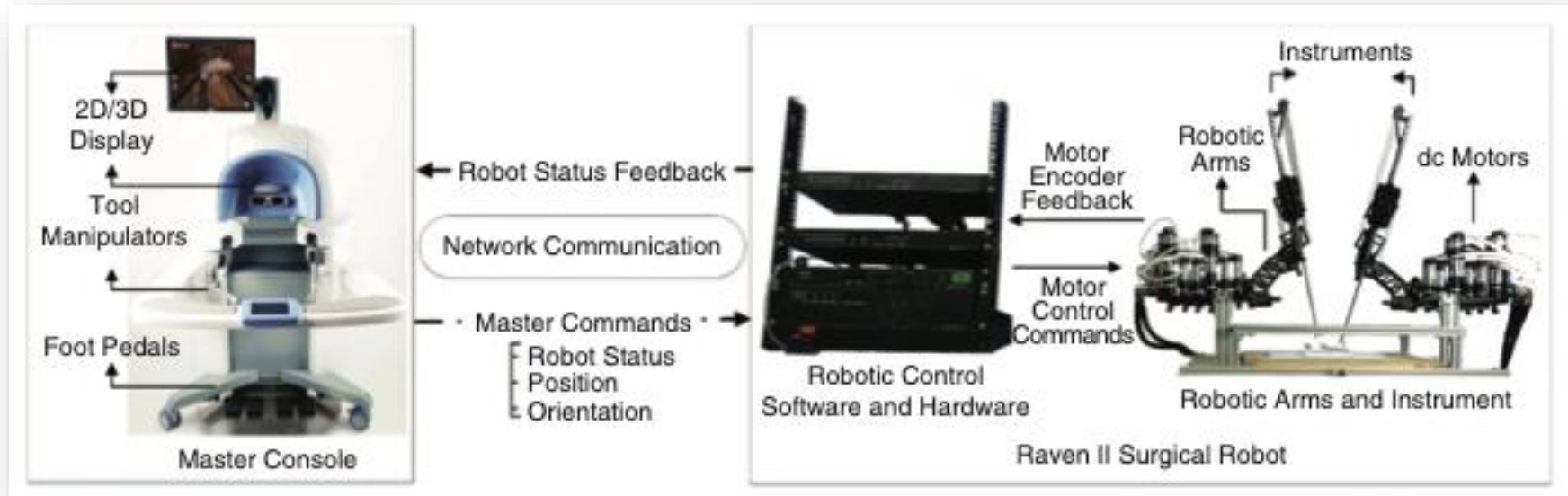
Esempi – TeamItaly

83



Esempi – Homa

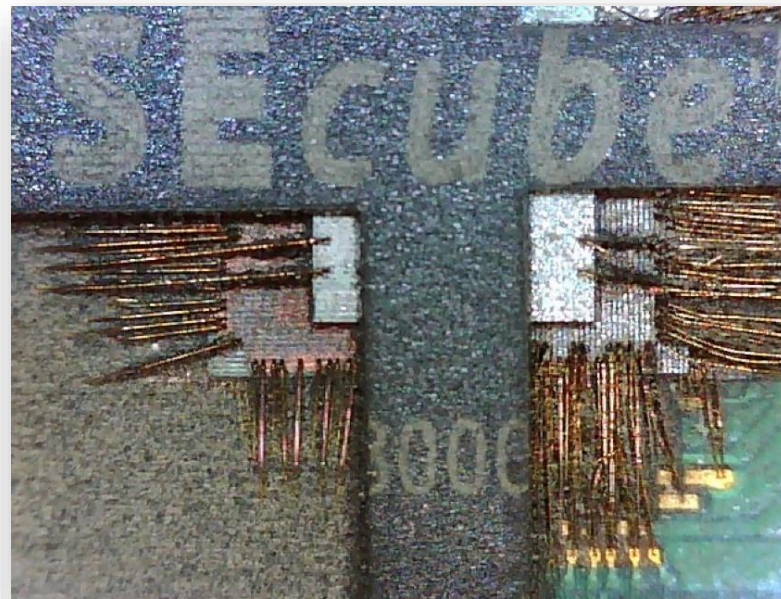
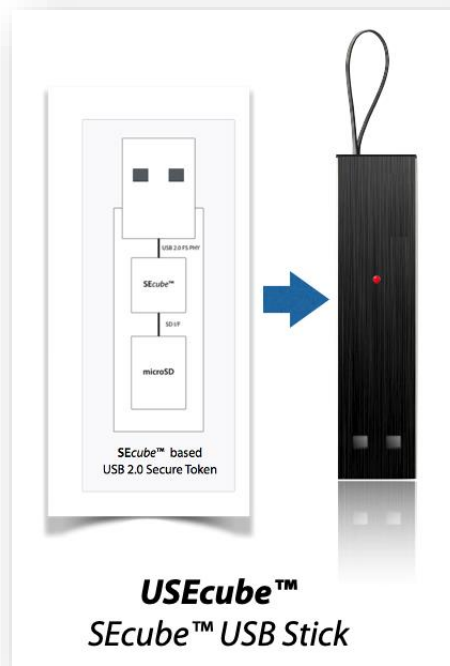
84



Caveat

85

- Non tutte le chiavette USB sono necessariamente malevoli!!

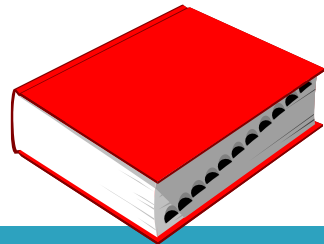


Baiting - Contromisure

86

- Accedete a chiavette USB non vostre solo attraverso *Macchine Virtuali* o *Sandbox*

Sandbox



87

- Ambiente virtuale “isolato” dal resto del computer che consente di eseguire applicazioni non certificate, scaricare file e visualizzare siti Web sospetti senza esporre a rischi e minacce il sistema su cui la sandbox è in esecuzione.

Caveat!!

88

- Non solo le pendrive, ma qualsiasi dispositivo che colleghi alla porta USB potrebbe infettare il PC, anche ciò che appare come un semplice cavetto.
- Non collegare nulla alla porta USB del tuo PC se non proveniente da fonte certa e affidabile.

E la ricarica dello smartphone?

89

- Quando usi un *charge point* pubblico o nella tua camera di hotel, collega il tuo caricatore alla presa elettrica, non inserire direttamente il cavetto nella presa USB, potresti infettare il tuo smartphone!

Social Engineering – I vettori di attacco

90

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

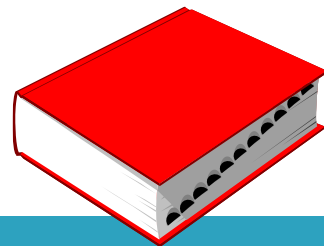
➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Dumpster Diving



91

- Prevede la raccolta e l'analisi di oggetti rottamati o dismessi dalla vittima.

Dumpster Diving - Esempi

92

- Un attaccante può trovare molti dati personali o informazioni sensibili dell'azienda su:
 - PC dismessi
 - CD
 - HD esterni
 - Stampanti dismesse
 - Agende
 - Calendari
 - Quaderni
 - Taccuini
 - ...

Problema

93

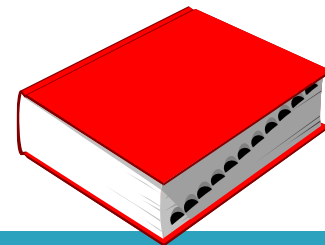
- Purtroppo, a differenza di quello che potreste pensare, in un sistema di elaborazione, quando “cancellate” un file, in realtà non cancellate fisicamente nulla, ma semplicemente chiedete al Sistema Operativo di cancellare quel file.
- Da quel momento in poi il Sistema Operativo assume che lo spazio prima occupato dal file cancellato sia disponibile e quindi, all’occorrenza, potrà “riscriverci” sopra.

Dumpster Diving - Contromisure

94

- Esegui SEMPRE delle operazioni di *sanitizzazione* (*sanitizing*) prima di dismettere qualsiasi dispositivo dotato di memoria.

Sanitizzazione (Sanitizing)



95

- Processo di rimozione dei dati sensibili da un sistema o dispositivo di archiviazione con l'intento che i dati non possano essere recuperati da alcuna tecnica conosciuta.

Sanitizzazione - Approcci

96

- Si adottano soluzioni diverse (hardware o software) in funzione di:
 - Livello di sicurezza richiesto
 - Tipo di dispositivo da sanitizzare



HDD




SSD

Sanitizzazione - Approcci

97

- Si adottano soluzioni diverse (hardware o software) in funzione di:
 - Livello di sicurezza richiesto
 - Tipo di dispositivo da sanitizzare



Alcuni esempi sono riportati
nell'Approfondimento 1

Sanitizzazione - Norme

98

- Il Regolamento (UE) 2016/679 – GDPR impone alle organizzazioni:
 - una nuova sensibilità al problema (le sanzioni sono molto severe)
 - l'implementazione di strumenti che permettano di gestire con semplicità procedure di cancellazione sicura dei dati da computer e altri dispositivi, al fine di non lasciare tracce di dati personali nel momento del riutilizzo dei sistemi o della loro alienazione (es. rivendita come usato, donazioni, smaltimento, restituzione al termine di contratti di locazione/leasing, ecc).

Sanitizzazione - Norme

99

- Il Provvedimento Garante Privacy del 13 ottobre 2008 (G.U. n.287 del 9.12.2008) intitolato *Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali* richiama l'attenzione sulla necessità di cancellare i dati personali dai dispositivi elettronici destinati a essere reimpiegati, riciclati, smaltiti.

Sanitizzazione - Standard

100

- Sono stati definiti diversi standard relativi alle procedure da seguire per la sanificazione, tra i quali:
 - ISO/IEC 17799
 - NIST Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006
 - DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM), February 2006

Social Engineering – I vettori di attacco

101

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ *Bufale*:

- Hoaxing
- Fake news
- Fake software – Trojan

Piggybacking (or Shoulder Surfing)

102

- Capacità di un attaccante di ottenere l'accesso illecito a un'area o a un'informazione riservata seguendo a breve distanza qualcuno che invece ha l'autorizzazione e la possibilità di accedervi



Piggybacking - Contromisure

103

- Se ti trovi a lavorare in luoghi affollati, proteggi i tuoi schermi tramite dei *Filtri Privacy*



Social Engineering – I vettori di attacco

104

➤ Varie tipologie di *pesca*:

- Phishing
 - Spear Phishing
 - Whaling
- Vishing
- Via social
 - OSInt & SocMInt

➤ Spacciarsi per altri:

- Impersonation
- Do ut des
- Quid pro Quo

➤ Attacchi *fisici*:

- Baiting
- Dumpster Diving
- Piggybacking o Shoulder Surfing
- Physical Access

➤ **Bufale:**

- Hoaxing
- Fake news
- Fake software – Trojan

Cultura e Spirito Critico

- Non esistono *pallottole d'argento*: serve dubitare, chiedersi a chi serve, cercare le fonti, ...

Cultura e Spirito Critico

- Non esistono *pallottole d'argento*: serve dubitare, chiedersi a chi serve, cercare le fonti, ...

Conoscenza Tecnologica

- Bisogna essere coscienti dei pericoli a cui si è esposti e ai quali si può esporre altri.

Social Engineering - Vettori di attacco

Paolo PRINETTO

Direttore
CINI Cybersecurity
National Laboratory



<https://cybersecnatlab.it>

Approfondimento 1 – Approcci alla Sanitizzazione

108

Approcci alla Sanitizzazione

109

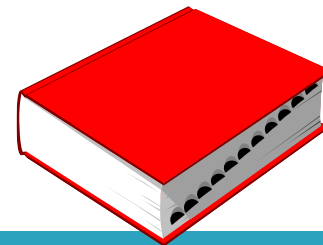
Hardware

- Degaussing

Software

- Wiping

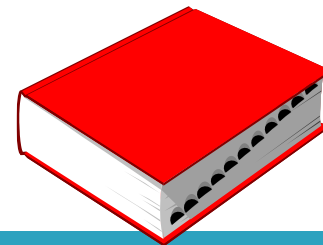
Degaussing



110

- È la rimozione o la riduzione del campo magnetico di un Hard disk utilizzando un dispositivo, chiamato *degausser*, che è stato specificamente progettato per lo specifico supporto fisico da cancellare.

Wiping



111

- *Wiping* (Pulizia), detto anche *Overwriting* (Sovrascrittura) o *Shredding* (Triturazione), prevede la scrittura ripetuta di nuovi dati su ogni blocco del file da cancellare.

Alcuni metodi di Wiping

112

- **Quick Erase:** scrive tutti 0, con una sola passata. È un metodo a bassa sicurezza visto che il disco magnetico ha una certa “memoria” di stato. Riscrivere 0 (per esempio) dove prima c’era 1 dà un valore leggermente diverso da scrivere 0 sopra 0. Si tratta di misure minime, ma che potrebbero essere rilevabili e quindi, in linea teorica, si potrebbero comunque ricostruire tutti i dati.
- **RCMP TSSIT OPS-II:** è uno standard della *Royal Canadian Mounted Police*, di media sicurezza, a 8 passate. Solitamente si scrive un byte random (o tutti 1 o tutti 0) nella prima passata, nella seconda il byte opposto della prima, e così via.

[<https://www.pcprofessionale.it/news/security/cancellare-hard-disk-sicuramente/>]

Alcuni metodi di Wiping

113

- **DoD Short:** è la versione “corta” del DoD 5220.22-M, rispetto a cui fa solo tre passate (la 1,2,7) contro le 7 del sistema standard. Anche in questo caso, di media sicurezza.
- **DoD 5220.22-M:** è uno standard del *Department of Defense*, il Dipartimento di Difesa statunitense, a 7 passate, di media sicurezza. Nella passata 1, 4 e 5 scrive sempre un byte random (o tutti 1 o tutti 0), nella 2 e nella 6 scrive tutti 0, mentre nella passata 3 e 7, scrive dati random.

[<https://www.pcprofessionale.it/news/security/cancellare-hard-disk-sicuramente/>]

Alcuni metodi di Wiping

114

- **Gutmann Wipe:** è l'algoritmo teorizzato da Peter Gutmann nella sua analisi "*Secure Deletion of Data from Magnetic and Solid-State Memory*" e conta ben 35 passate, con scrittura dei dati casuali. Le prime 4 passate sono scritte in maniera casuale, così come le ultime 4. Nelle passate dal 5 alla 31 segue uno schema complesso, di dati non casuali, ma con applicazione casuale. Il livello di sicurezza è altissimo, ma molto oneroso in termini di tempo.
- **PRNG Stream:** con questo metodo la cancellazione avviene sovrascrivendo il disco con una sequenza di dati pseudo casuale. La sicurezza di questo metodo dipende dal numero di passate (rounds) che avete impostato: 4 è un numero di media sicurezza, da 8 in su si ha un livello di sicurezza alto.

[<https://www.pcprofessionale.it/news/security/cancellare-hard-disk-sicuramente/>]