Il Fattore Umano: Social Engineering

Classifica


Fattore umano
Aspetti organizzativi
Aspetti tecnologici (HW/SW)
1
2
3

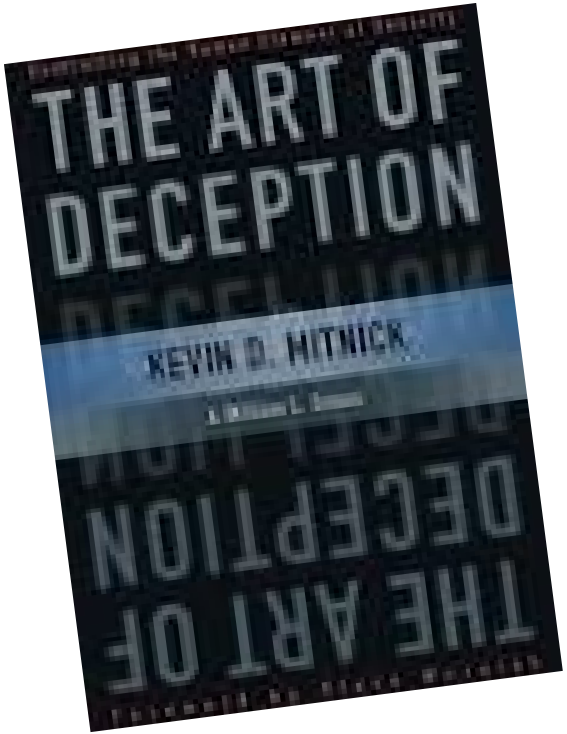
L’uomo è sempre l’anello debole !!

Problem Exist Between Keyboard And Chair

The *weakest link*

"No matter how strong your Firewalls, Intrusion Detection Systems, Cryptography, Anti-virus software, you are the weakest link in computer security! People are more vulnerable than computers"

[Kevin D. Mitnick & William L. Simon – The Art of Deception]



L’uomo è sempre l’anello debole

Fake News

- L’uomo viene attaccato tramite la rete: si sfruttano la pervasività, la velocità della rete e le vulnerabilità intrinseche degli utenti

Social Engineering

- Le strutture in rete vengono attaccate usando l’uomo per acquisire informazioni utili allo scopo

Social Engineering

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

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

Social Engineering

- Combinazione di tecniche sociologiche, psicologiche e di raccolta di informazioni utilizzate per manipolare le persone e convincerle a rilasciare informazioni sensibili o a compiere azioni che non rispettano le normali misure di sicurezza

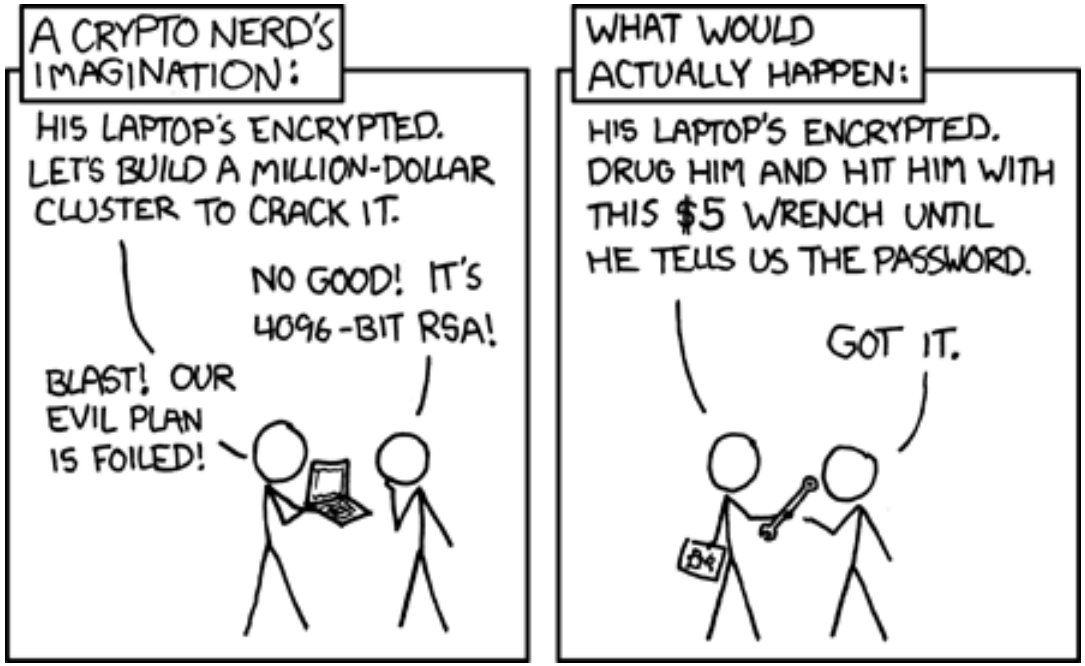
Social Engineering - Target

- Target primario è il personale di help desk, segretariale o di supporto

Social Engineering - Target

- Target primario è 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 - Target



Social Engineering - Obiettivi

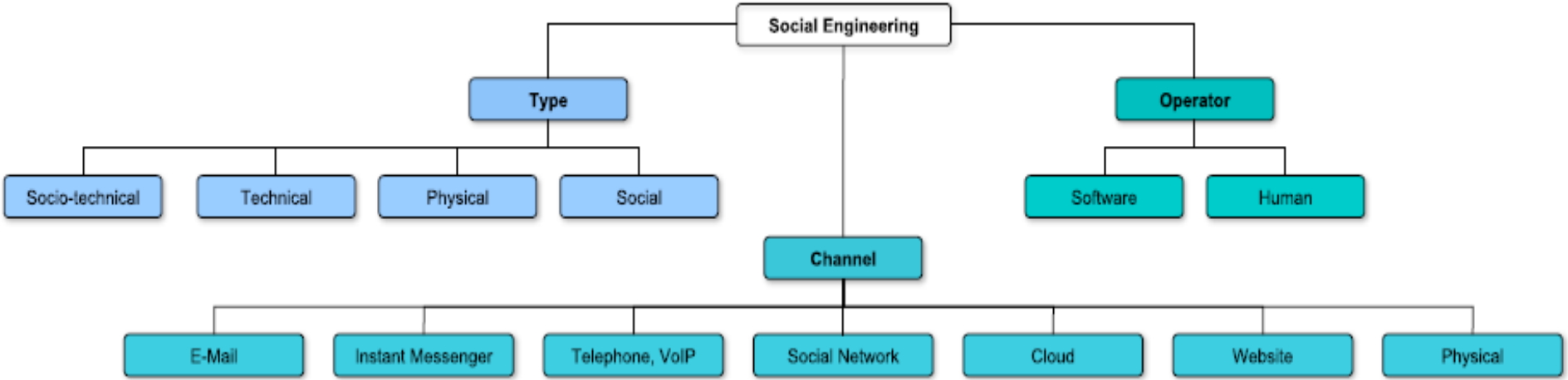
- Furto d’identità e informazioni
- Spionaggio industriale
- Furto di denaro/valori
- Acquisizione di privilegi

Esempi di attacchi

- https://www.youtube.com/watch?v=lc7scxvKQOo
- http://www.ilfattoquotidiano.it/2016/11/04/identita-digitale-ce-un-buco-nella-sicurezza-cosi-ti-divento-matteo-renzi/3093093/

Social Engineering – Ciclo di Attacco

Social Engineeting - Tassonomia



Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Social Engineering – I vettori di attacco

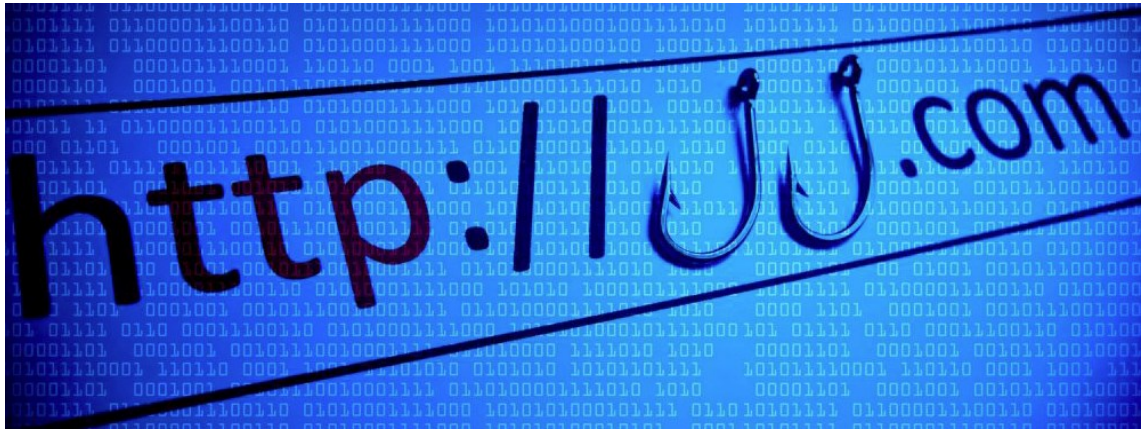
- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Phishing

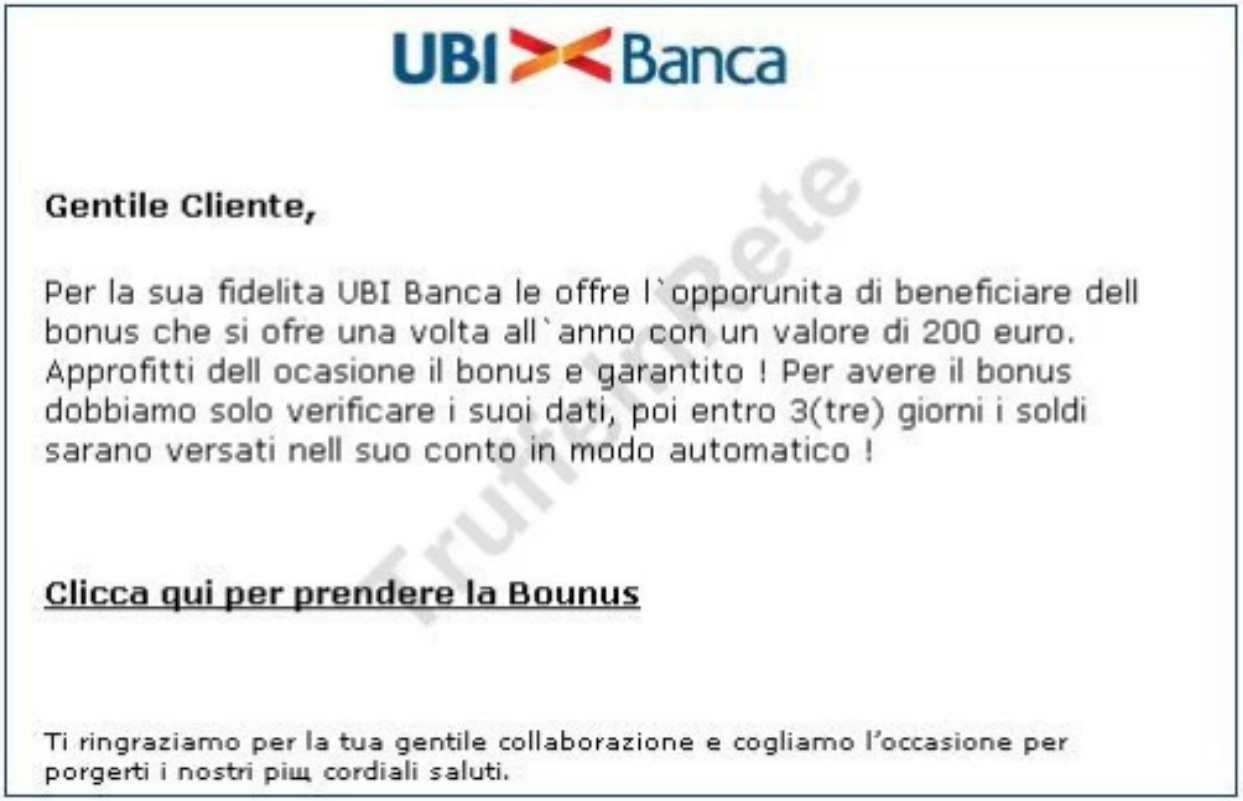
- Truffa via Internet in cui l’aggressore cerca di ingannare la vittima inducendola a fornire informazioni personali, come credenziali d’accesso, dettagli sul conto corrente bancario e sulle carte di credito.

Phishing – Come si realizza

- 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



UBI Banca

Gentile Cliente,

Per la sua fidelita UBI Banca le offre l`opporunita di beneficiare dell bonus che si ofre una volta all`anno con un valore di 200 euro. Approfitti dell ocasione il bonus e garantito ! Per avere il bonus dobbiamo solo verificare i suoi dati, poi entro 3(tre) giorni i soldi sarano versati nell suo conto in modo automatico !

Clicca qui per prendere la Bounus

Ti ringraziamo per la tua gentile collaborazione e cogliamo l'occasione per porgerti i nostri piщ cordiali saluti.

Unusual, non-IC sender

From: Helpdesk [paulsmith@stp-mineral.com]
To: Undisclosed Recipients
Subject: UPGRADE ACCOUNT

Your email missing

Hello Customer,

Impersonal greeting

Poor spelling and clunky grammar

As part of our upgrades to new Office system we require to verfy your mailbox.

Hover over the link to check the URL. Not an Imperial address.

Please click here to submit your updated information.

http://192.168.235.144/submit/index.jsp

If action is not taken by you we will terminate your online services.

Threats / urgency

Thank you
ITS Help Desk Administrator

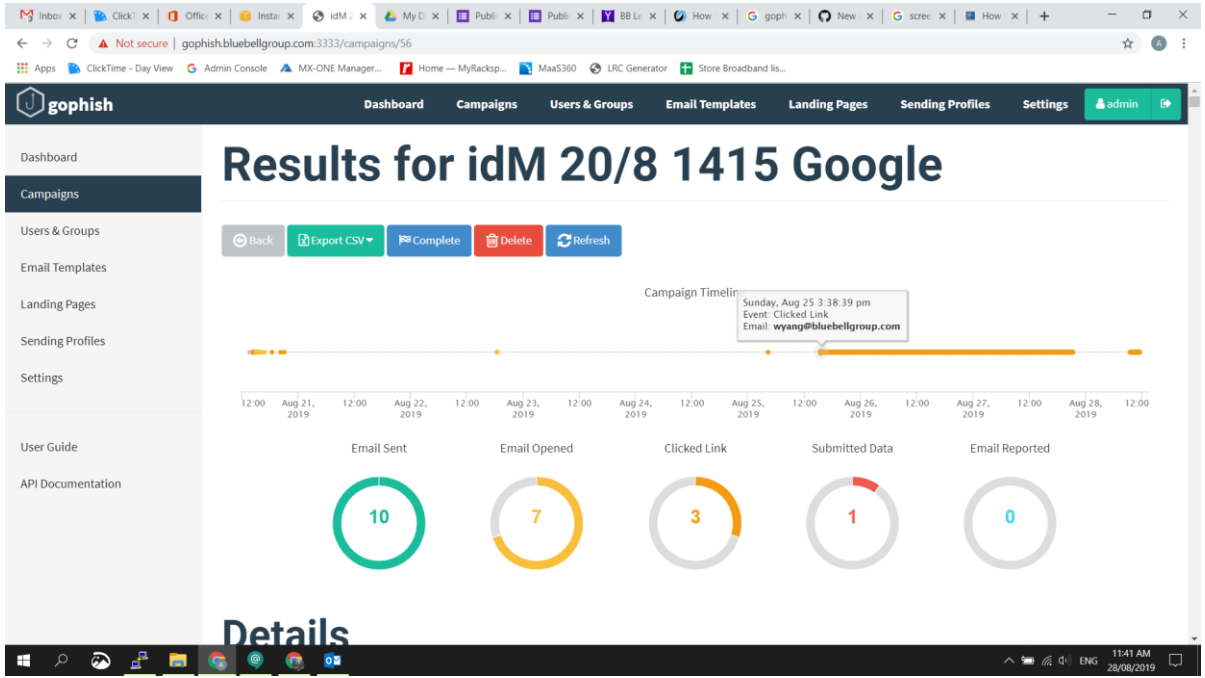
Generic signature, no contact information

"Il tuo pc e' bloccato", La polizia postale segnala nuova ondata truffe

Navigando può capitare di trovarsi di fronte ad una schermata di (finto) blocco, accompagnata dall'invito a chiamare un numero di telefono per ottenere supporto tecnico online: è un raggiro

27 aprile 2019

GoPhish


Not secure | gophish.bluebellgroup.com:3333/campaigns/56
gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
Results for idM 20/8 1415 Google
Back
Export CSV
Complete
Delete
Refresh
Campaign Timeli
Sunday, Aug 25 3:38:39 pm
Event: Clicked Link
Email: wyang@bluebellgroup.com
12:00 Aug 21, 2019 12:00 Aug 22, 2019 12:00 Aug 23, 2019 12:00 Aug 24, 2019 12:00 Aug 25, 2019 12:00 Aug 26, 2019 12:00 Aug 27, 2019 12:00 Aug 28, 2019 12:00
Email Sent
10
Email Opened
7
Clicked Link
3
Submitted Data
1
Email Reported
0
Details
ENG
11:41 AM
28/08/2019

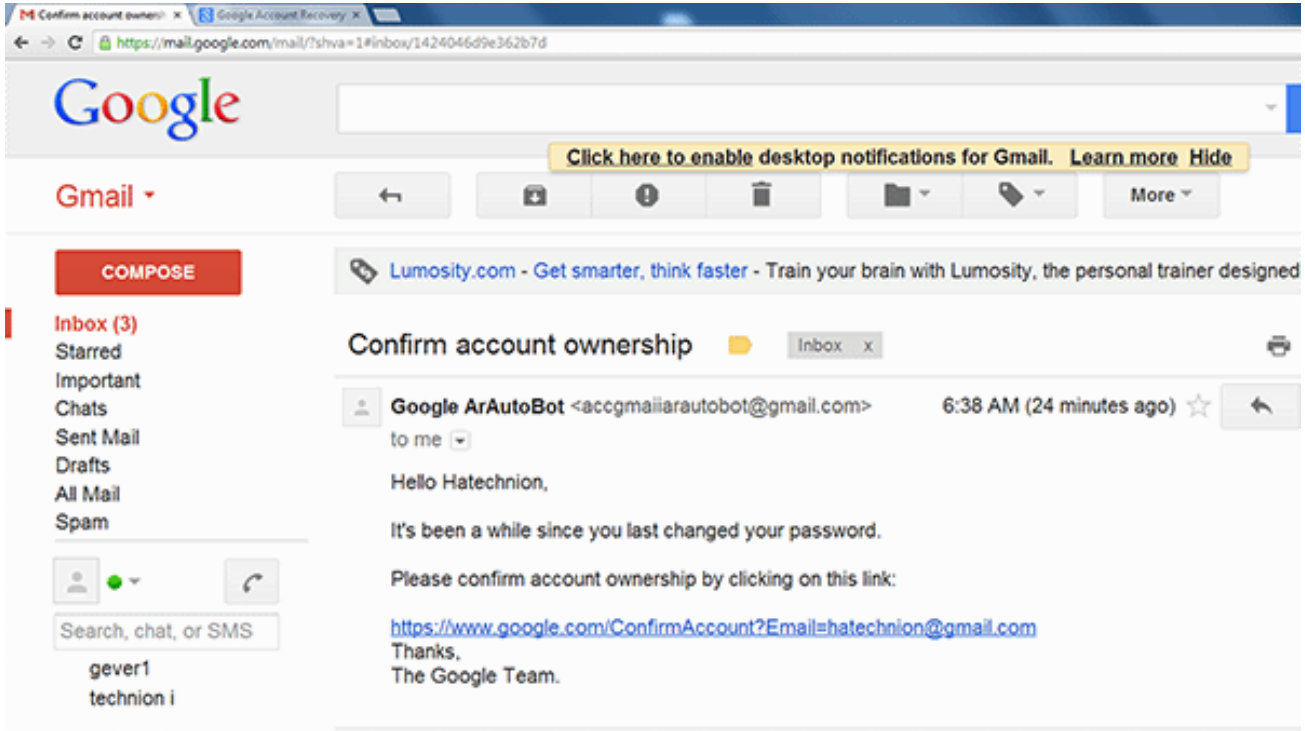
Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Spear Phishing

- È la forma mirata del phishing, orientata quindi 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



Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Whaling

- Attacchi di phishing diretti specificamente verso senior executive e altre persone di elevato profilo del mondo della finanza e dell'industria in generale.

Whaling

- Attacchi di phishing diretti specificamente verso senior executive e altre persone di elevato profilo del mondo della finanza e dell'industria in generale.

- Il termine whaling (da whale - balena) è stato coniato per questi tipi di attacco per evidenziare la “grandezza” e l'importanza degli obbiettivi

Whaling

- https://www.ilpost.it/2017/09/30/confindustria-dell-alba-truffa-500mila-euro-email-falsa/

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation

- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Vhishing

- Per vishing si intende il phishing tramite mezzo telefonico.

Vhishing

- 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.

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Baiting

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

Baiting

- Si tratta spesso di un'esca fisica, di un supporto informatico come un cd, un dvd o una chiave USB, che viene lasciata incustodita dall’attaccante in un luogo dove possa essere presa e utilizzata dall’attaccato per imprudenza o leggerezza.

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des
- Quid pro Quo
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Dumpster Diving

- Prevede una raccolta e un’analisi di oggetti rottamati o di materiale gettato dalla vittima.

Dumpster Diving - Esempi

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

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation

- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Impersonation

- Consiste nel fingersi qualcuno per:
  - ottenere informazioni o
  - effettuare una operazione ostile.

Impersonation

- Si divide in:
  - *Personificazione*
  - *Pretexting*

Impersonation

Personificazione

- L’attaccante sfrutta le info che ha raccolto precedentemente per ottenere credenziali al fine di persuadere l’attaccato di essere in comunicazione (più spesso virtuale che fisica) con una persona a lui nota

Pretexting

- L’attaccante interpreta un ruolo che, grazie alla sua autorità o alla sua attività professionale, gli permette di avere accesso a informazioni sensibili

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation

- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Do ut des

- 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

Do ut des

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

Do ut des - Esempio

- 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
- L’attaccante "aiuta" la vittima, ma le farà digitare dei comandi che gli permetteranno di installare un malware

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Hoaxing

- Tentativo di convincere le vittime che qualcosa di falso sia invece vero
- Corrisponde al noto concetto di "bufala".

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking o Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Piggybacking (o Shoulder Surfing)

- 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

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Trojan

- Software malevoli spacciati per applicazioni legittime
- Trattati più in dettaglio nella lezione sui malware

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSINT & SoCINT

Physical Access

- Accesso non autorizzato da parte dell'attaccante a una struttura cui non avrebbe diritto di accedere
- Per esempio spacciandosi per tecnici della manutenzione

Social Engineering – I vettori di attacco

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Baiting
- Dumpster Diving
- Impersonation
- Do ut des (Quid pro Quo)
- Hoaxing
- Piggybacking or Shoulder Surfing
- Fake software – Trojan
- Physical Access
- OSInt & SocMInt

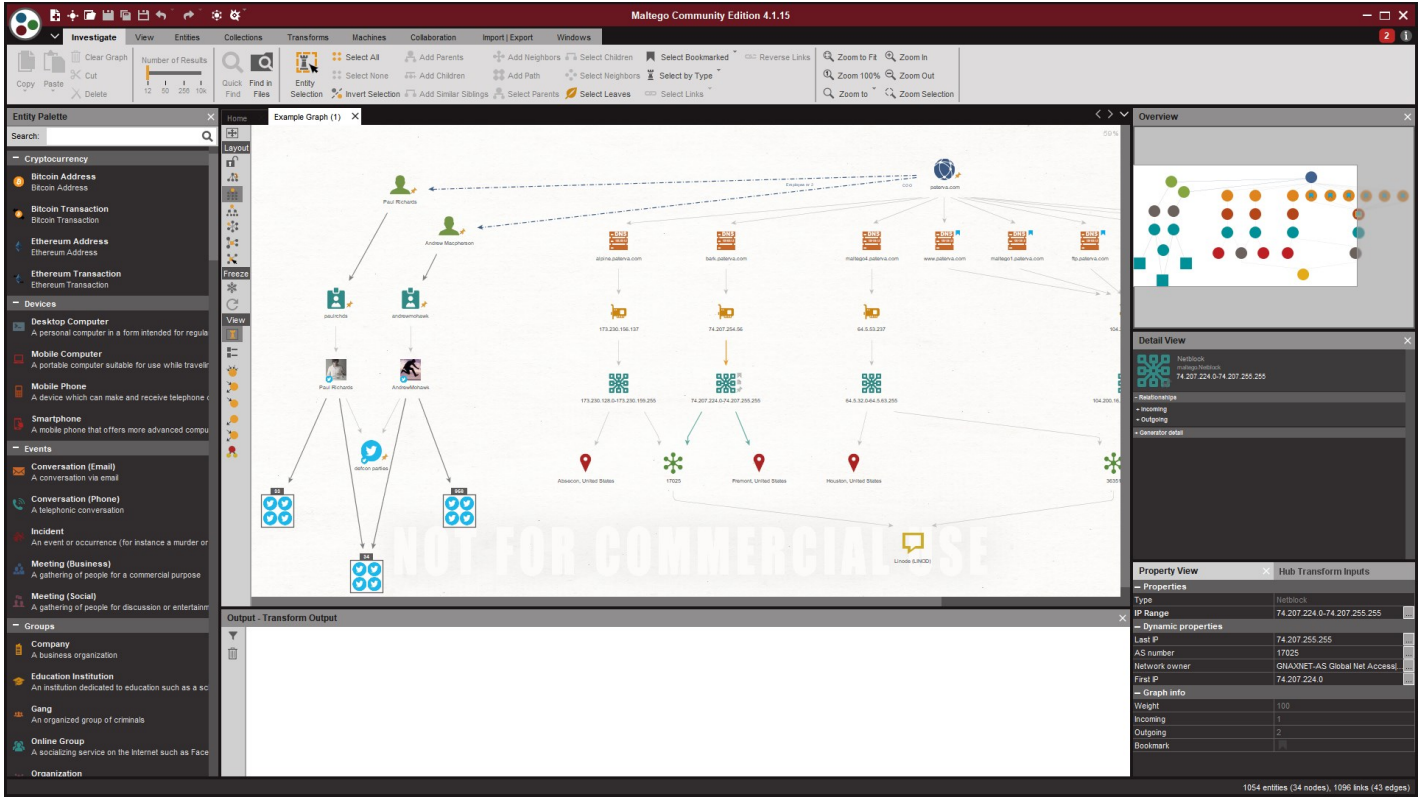
OSInt – Open Source Intelligence
SocMInt – Social Media Intelligence

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

Maltego

- 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

Maltego


Maltego Community Edition 4.1.15
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
Cryptocurrency
Bitcoin Address
Bitcoin Address
Bitcoin Transaction
Bitcoin Transaction
Ethereum Address
Ethereum Address
Ethereum Transaction
Ethereum Transaction
Devices
Desktop Computer
A personal computer in a form intended for regula
Mobile Computer
A portable computer suitable for use while travelli
Mobile Phone
A device which can make and receive telephone
Smartphone
A mobile phone that offers more advanced compu
Events
Conversation (Email)
A conversation via email
Conversation (Phone)
A telephonic conversation
Incident
An event or occurrence (for instance a murder or
Meeting (Business)
A gathering of people for a commercial purpose
Meeting (Social)
A gathering of people for discussion or entertainm
Groups
Company
A business organization
Education Institution
An institution dedicated to education such as a sc
Gang
An organized group of criminals
Online Group
A socializing service on the Internet such as Face
Organization
Example Graph (1)
Overview
Detail View
Property View
Hub Transform Inputs
Properties
Type
Netblock
IP Range
74.207.224.0-74.207.255.255
Dynamic properties
Last IP
74.207.255.255
AS number
17025
Network owner
GNAXNET-AS Global Net Access
First IP
74.207.224.0
Graph info
Weight
100
Incoming
1
Outgoing
2
Bookmark
Output - Transform Output
1054 entities (34 nodes), 1096 links (43 edges)

Prevenzione

- Attacchi di social engineering non possono essere bloccati dalla sola tecnologia

Prevenzione

- Servono:

Prevenzione

- Servono:
  - Addestramento ed Educazione

Prevenzione

- Servono:
  - Addestramento ed Educazione

- Igiene Cibernetica
- Corsi
- Educazione Continua
- Formazione
- Strutture
- Certificazioni
- …

Prevenzione

- Servono:
  - Addestramento ed Educazione

- Igiene Cibernetica
- Corsi
- Educazione Continua
- Formazione
- Strutture
- Certificazioni
- …

#1 123456	#18 lovely	#36 football
#2 123456789	#19 7777777	#37 charlie
#3 qwerty	#21 888888	#38 letmein
#4 password	#22 princess	#39 !@#$%^&*
#5 1234567	#23 dragon	#40 secret
#6 12345678	#24 password1	#41 aa123456
#7 12345	#25 123qwe	#42 987654321
#8 iloveyou	#26 666666	#43 zxcvbnm
#9 111111	#27 1qaz2wsx	#44 passw0rd
#10 123123	#28 333333	#45 bailey
#11 abc123	#29 michael	#46 nothing
#12 qwerty123	#30 sunshine	#47 shadow
#13 1q2w3e4r	#31 liverpool	#48 121212
#14 admin	#32 777777	#49 biteme
#15 qwertyuiop	#33 1q2w3e4r5t	#50 ginger
#16 654321	#34 donald	
#17 555555	#35 freedom	

#1 123456	#18 lovely	#36 football
#2 123456789	#19 7777777	#37 charlie
#3 qwerty	#21 888888	#38 letmein
#4 password	#22 princess	#39 !@#$%^&*
#5 1234567	#23 dragon	#40 secret
#6 12345678	#24 password1	#41 aa123456
#7 12345	#25 123qwe	#42 987654321
#8 iloveyou	#26 666666	#43 zxcvbnm
#9 111111	#27 1qaz2wsx	#44 passw0rd
#10 123123	#28 333333	#45 bailey
#11 abc123	#29 michael	#46 nothing
#12 qwerty123	#30 sunshine	#47 shadow
#13 1q2w3e4r	#31 liverpool	#48 121212
#14 admin	#32 777777	#49 biteme
#15 qwertyuiop	#33 1q2w3e4r5t	#50 ginger
#16 654321	#34 donald	
#17 555555	#35 freedom	

The 50 Most Common — And Worst — Passwords Of 2019

digg Digg Dec 18, 2019 @13:35 PM · Updated: Dec 18, 2019 @13:46 PM

Il ruolo della legge

La California ‘banna’ le password facili (admin, 12345) per contrastare gli hacker

> *Per contrastare il crimine informatico la California ha approvato una legge che renderà illegale per le aziende di elettronica utilizzare password predefinite semplici come "password" o "admin" a partire dal 2020.*

di **Piero Boccellato** | @pieroboccellato | 8 ottobre 2018, ore 11:30

Prevenzione

- Servono:
  - Addestramento ed Educazione
  - Consapevolezza

Prevenzione

- Servono:
  - Addestramento ed Educazione
  - Consapevolezza
- 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 della persona

Prevenzione

- Servono:
  - Formazione e Educazione
  - Consapevolezza
  - Politiche adeguate

Prevenzione

- Servono:
  - Formazione e Educazione
  - Consapevolezza
  - Politiche adeguate

- Non consentire la divulgazione di informazioni private
- Impedire ai dipendenti di essere sottoposti a pressioni sociali o ingannati
- Il concetto del *Need-to-know*

Prevenzione

- Servono:
  - Formazione e Educazione
  - Consapevolezza
  - Politiche adeguate
  - Supporto di terze parti

Prevenzione

- Servono:
  - Formazione e Educazione
  - Consapevolezza
  - Politiche adeguate
  - Supporto di terze parti

- Ricorrere a un ente terzo per:
  - Provare a penetrare nella rete
  - Scoprire i problemi che le persone hanno con la sicurezza
- Programmi di Bug-Bounty e Hacking etico
- Organizzare campagne di social engineering rivolte ai dipendenti

Riferimenti

- https://ricerca.repubblica.it/repubblica/archivio/repubblica/2017/10/06/sessanta-mail-una-telefonata-due-bonifici-cosi-la-truffata12.html
- https://www.paterva.com/buy/maltego-clients/maltego-ce.php