Tipologie e metodi di attacco

Tipologie di attacco

Acquisizione di informazioni

L’obiettivo è quello di acquisire informazioni, attraverso l’intercettazione di comunicazioni riservate o ottenendole in altri modi. Spesso le informazioni raccolte servono a facilitare l’attacco vero e proprio, per cui, questo tipo di azione può preludere agli attacchi descritti di seguito.

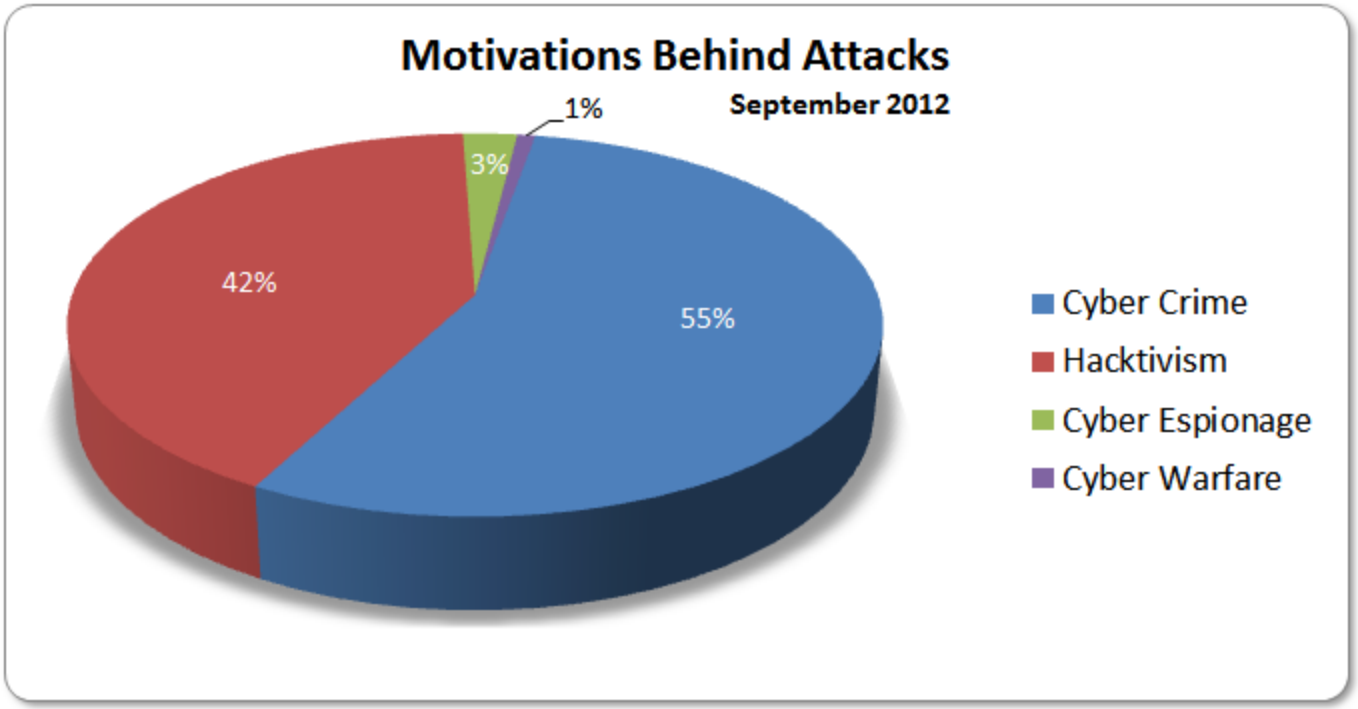
Accesso non autorizzato

L’obiettivo è quello di ottenere l'accesso ad una rete o ad un computer, pur non avendone l'autorizzazione, ottenendo informazioni riservate e\o provocando danni di vario genere al sistema.

Denial of Service

L’obiettivo è quello di rendere un sistema, un servizio o una rete non disponibile agli utenti autorizzati.

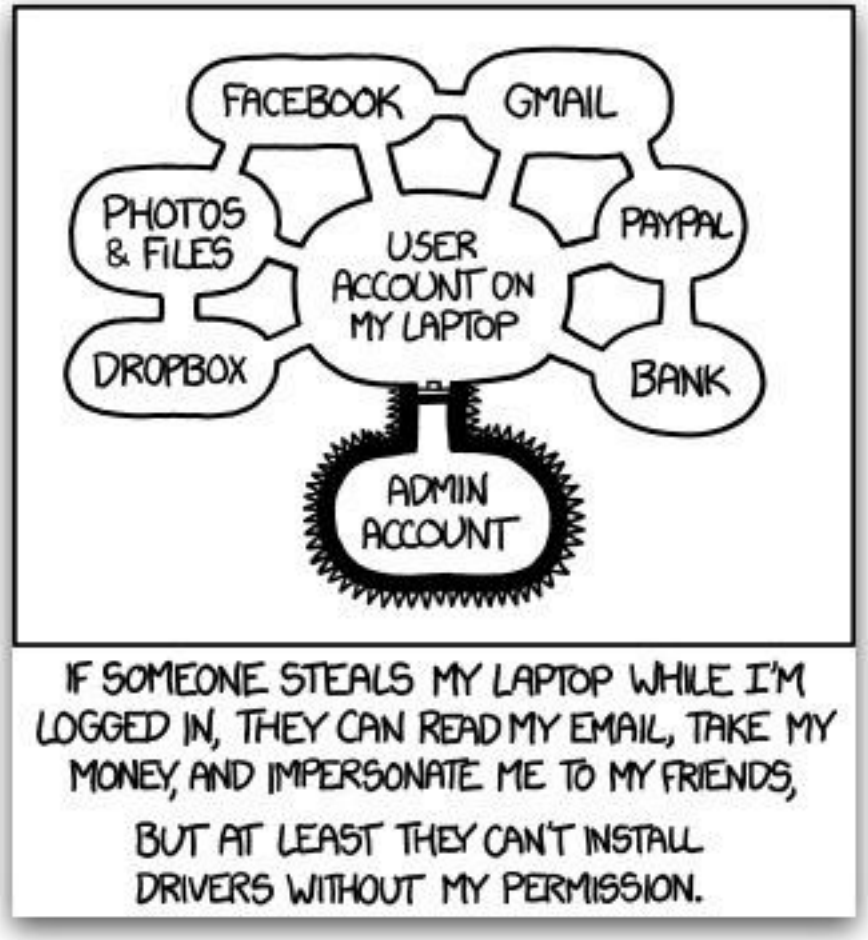
Motivazioni Attacchi



Strumenti

- Trojan, Backdoor, Keylogger (accesso al sistema)
- Virus e Worm (denial of service, acquisizione informazioni)
- Spyware, Adware (acquisizione informazioni)
- Social engineering (accesso al sistema)
- Sniffing, spoofing,…(acquisizione informazioni)
- Intrusione fisica, furto hardware,…

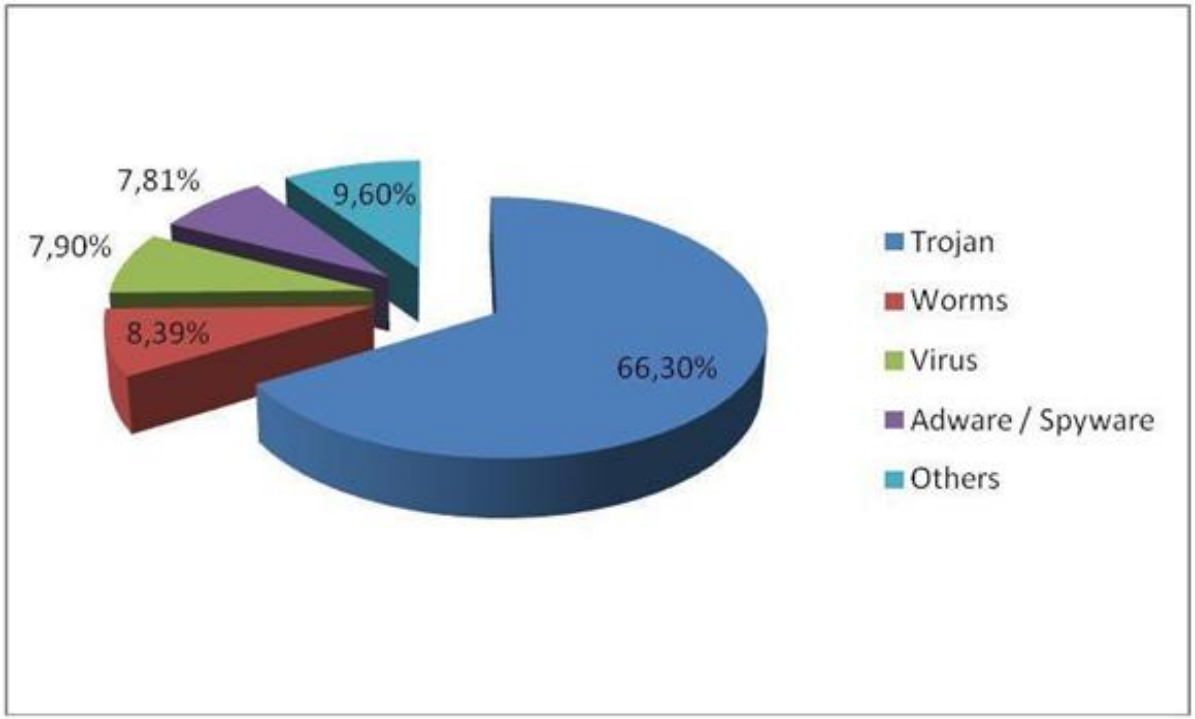
Furto hardware...



Malware

Qualsiasi software che abbia lo scopo di provocare danni o di eseguire operazioni non desiderate dall'utente (*malicious software*)

Statistiche

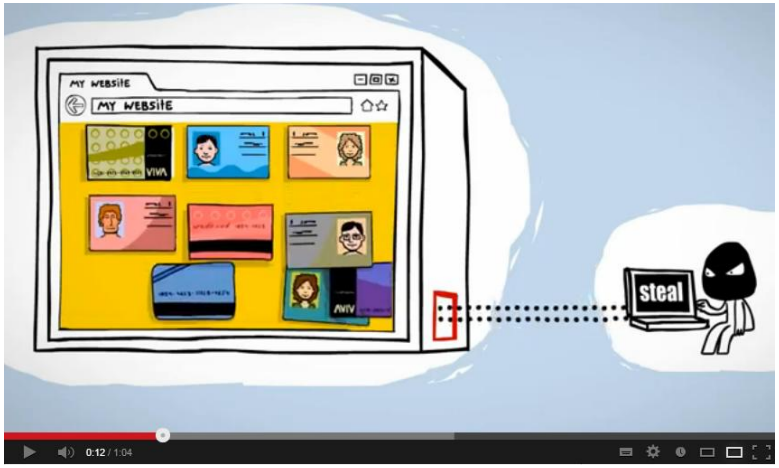


Trojan Horse

- Programma che l'utente installa volontariamente pensando che non sia dannoso.
- Una volta installato sul computer può installare backdoor, spyware, adware, keylogger...
- I rischi sono molteplici, tra cui la perdita di dati e l'utilizzo della macchina per fini criminosi(botnet).

Backdoor

- Nati con lo scopo di facilitare il lavoro su macchine remote (es. servizi di assistenza),
- permettono di avere il pieno controllo del sistema infetto da un host remoto(attraverso internet).



Virus

- Sono porzioni di codice in grado di replicarsi ed «infettare» altri file
- Non sono programmi eseguibili e pertanto richiedono che l'utente mandi in esecuzione un programma «ospite» all'interno del quale c'è anche il codice del virus
- «Infettano» altri programmi copiando il proprio codice al loro interno
- Possono installare backdoor, keylogger,…

Storia virus

Storia virus 2

Virus

per rendere più difficile la loro individuazione da parte dei sistemi antivirus possono:

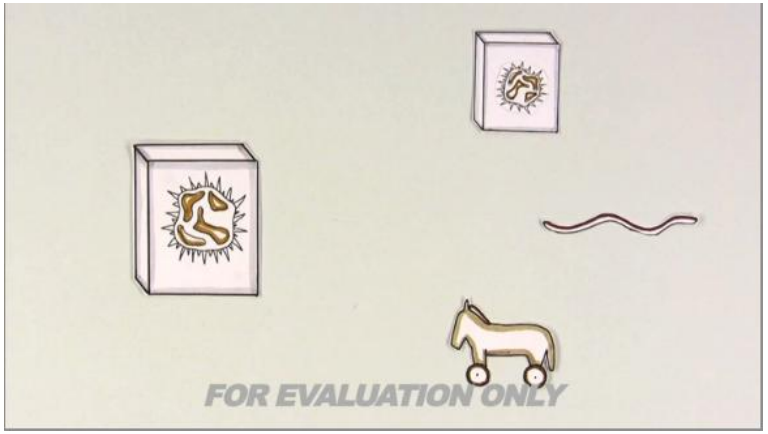
- «mutare» ad ogni infezione(polimorfici),
- comprimere il proprio codice,
- suddividerlo tra più file,
- modificare parti del sistema operativo,
- «Sabotare» l'antivirus

Worm

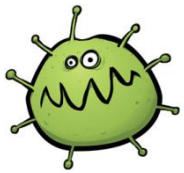
- Programmi eseguibili in grado di autoreplicarsi e di diffondersi attraverso internet
- I primi worm si autoreplicavano senza controllo rallentando la macchina in maniera tale da impedirne l'utilizzo (oggi questi tipo di worm si chiamano Rabbit)
- I worm come i trojan e i virus possono installare keylogger, spyware,…
- Possono essere utilizzati per creare botnet

Video


I virus più pericolosi della storia
bonsai
0:47 / 2:37


FOR EVALUATION ONLY


Biggest
with
DANGER
worm
IS THE ABILITY TO
REPLICATE
@ EMAIL ADDRESS BOOK
Copy
Matt@yahoo.com
John @gmail.com
Bob @hotmail.com
x 100
OR x MILLION
e si invia a tutti i contatti presenti in ciascuna delle rubrica del ricevitore, e la
1:29 / 3:09



Spyware

- Spiano l'attività dell'utente (es. siti visitati)
- possono ricercare dati quali password, numeri di carte di credito, … inviandoli ad un server remoto.

Adware

- Programmi che raccolgono informazioni sugli utenti a fini pubblicitari.
- pop up , spam, violazione privacy e sicurezza (non si è al corrente di quali dati vengano inviati in rete)
- Spesso sono installati in maniera del tutto legale insieme ad altri programmi applicativi (es. kazaa)

Keylogger

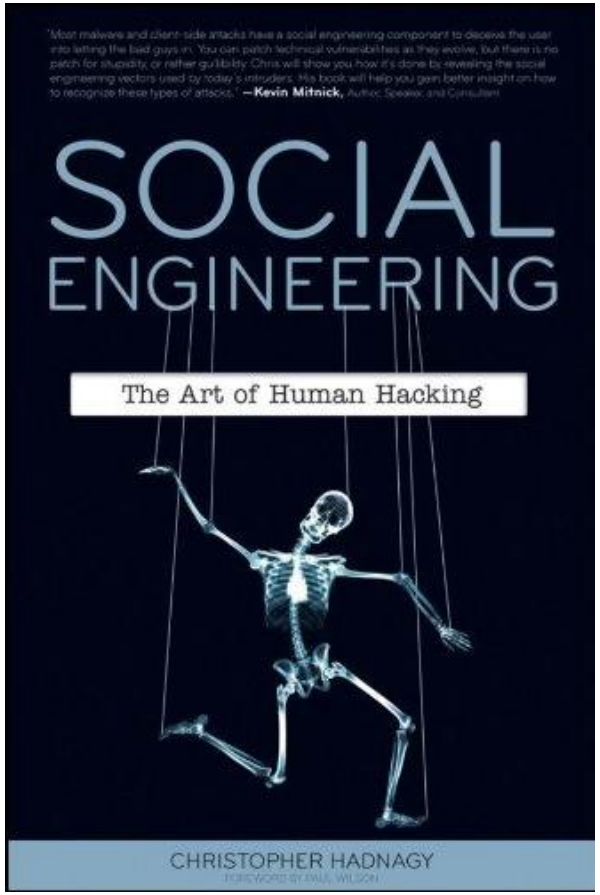
- Abbreviazione di Keystroke Logger
- Programmi che registrano le azioni eseguite dagli utenti: tasti digitati, programmi avviati,…

Keylogger


SofForYou Keylogger
User: All Users
Program: All Programs
Refresh
SoftForYou Keylogger
Objective
SoftForYou Keylogger is a FREE, powerful and easy-to-use keyboard tracking software (a.k.a. keylogger) to monitor your children online conversations and make sure they don't make any dubious acquaintances and don't spread out personal information.
Main Features
Intuitive and easy to use.
Keeps track of all key strokes - logs everything typed in almost all applications
Magic Word: sfyklg
Mode: Text Only
Log Size (KB): 4096
Clear
Uninstall
About...

Ingegneria Sociale

Studio del comportamento individuale di una persona al fine di carpire informazioni utili.

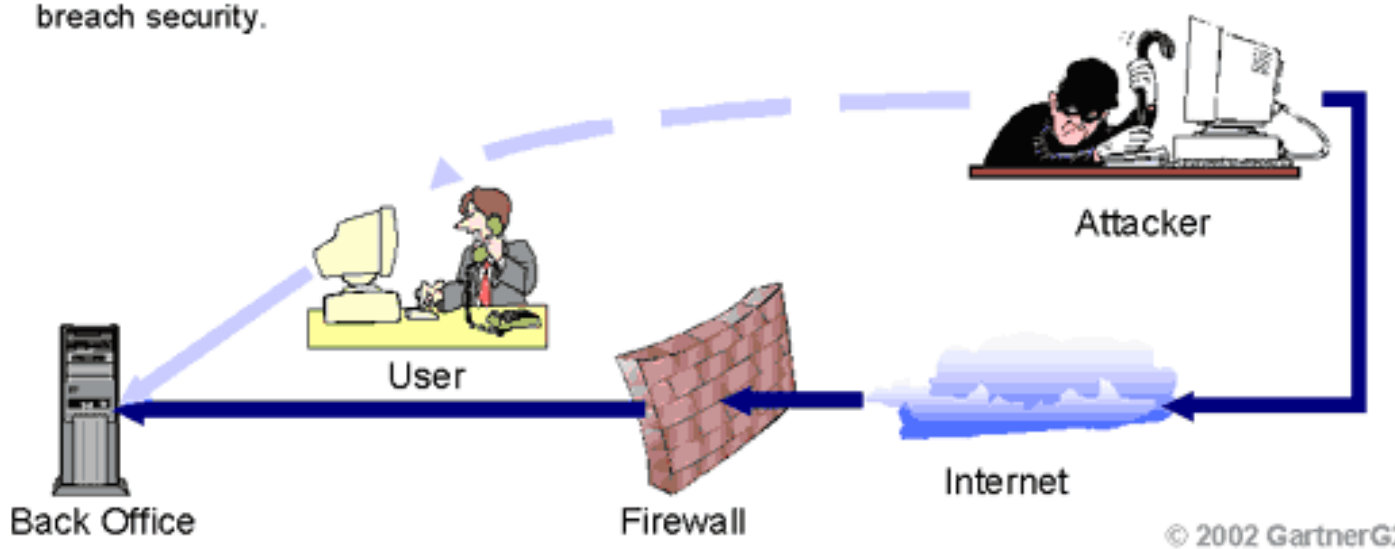


per approfondire...

Ingegneria Sociale

Social Engineering

- Includes extensive research information (legal and illicit) about an enterprise, which is gathered and used to exploit people.
- Successful social engineering results in partial or complete circumvention of an enterprise's security systems. The best firewall is useless if the person behind it gives away either the access codes or the information it is installed to protect.
- Social engineering *principally* involves the manipulation of people rather than technology to breach security.



Ingegneria Sociale

DEMONSTRATION OF DMS FOR NLUP

Date: 25.8.2011
Time: 1200 Noon
Name and Signature of the Participant

Venue: NIC, Saiha.

Sl.No	NAME	DESIGNATION	CONTACT NO	SIGNATURE
1.	T. LALRINAWMA	R/Operator	9612606164	
2.	Lalrinawma	IPO	9436149024	
3.	P. Lalbiaktani	RO (Soil)	9612063844	
4	B. Lalrinliana	DSO	9436147397	
5.	T. Vanlalthana	DHO	9436147910	
6.	C. SIMON	DIO	9436149364	
7.	Arunjyoti Das	Scientific Officer	9435152768	
8.	H. K. Vanlalpeka	V.O.	9612112112	
9	S.P. Singh	DADO	9436149004	
10.	Lalhmingmawia	SDAO	9436146114	

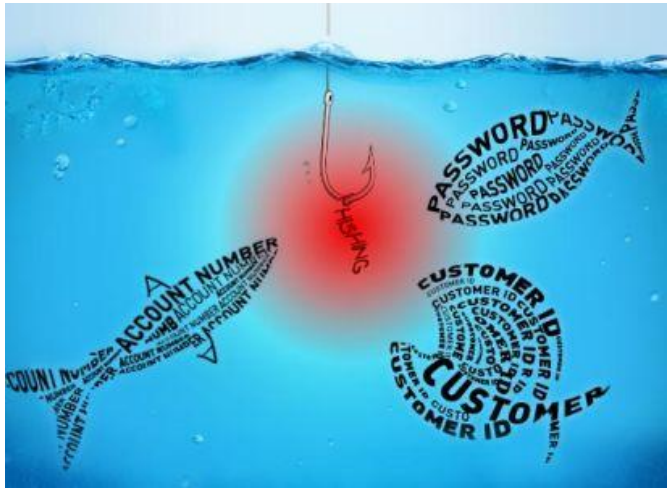
Phishing

- L’obiettivo è di indurre l’utente ad inserire dati confidenziali o credenziali di accesso come username e password facendogli credere che la richiesta provenga da una fonte affidabile.

- La vittima viene in genere adescata con una email o clonando un sito web.

Phishing


WEBMAIS.COM
E AGORA, VOU NAVEGAR NA MINHA CONTA BANCÁRIA !
WINDOWS
DIGITE SUA SENHA
E EU TAMBÉM, IDIOTA...


PHISHING
PASSWORD
ACCOUNT NUMBER
CUSTOMER ID
CUSTOMER

Phishing

Security & Safety
Sicurezza Logica | Posteitaliane

Egregio Cliente,

La preghiamo di esaminare con la massima serieta e immediatamente questo messaggio di posta elettronica che mostra le nuove misure di sicurezza.

Il reparto sicurezzo della nostra banca le notifica che sono state prese misure per accrescere il livello di sicurezza dell'online banking, in relazione ai frequenti tentativi di accedere illegalmente ai conti bancari.

Per ottenere l'accesso alla versione piu sicura dell'area clienti preghiamo di dare la sua autorizzazione.

Accedi ai servizi online »

Se scegliete di ignorare la nostra richiesta, purtroppo non avremo altra scelta che bloccare temporaneamente il suo account.

Distinti saluti,
BancoPostaonline

Ingegneria Sociale

Denial of Service

L'obiettivo è interrompere l'erogazione di un servizio. Due strategie principali:

Flooding DoS

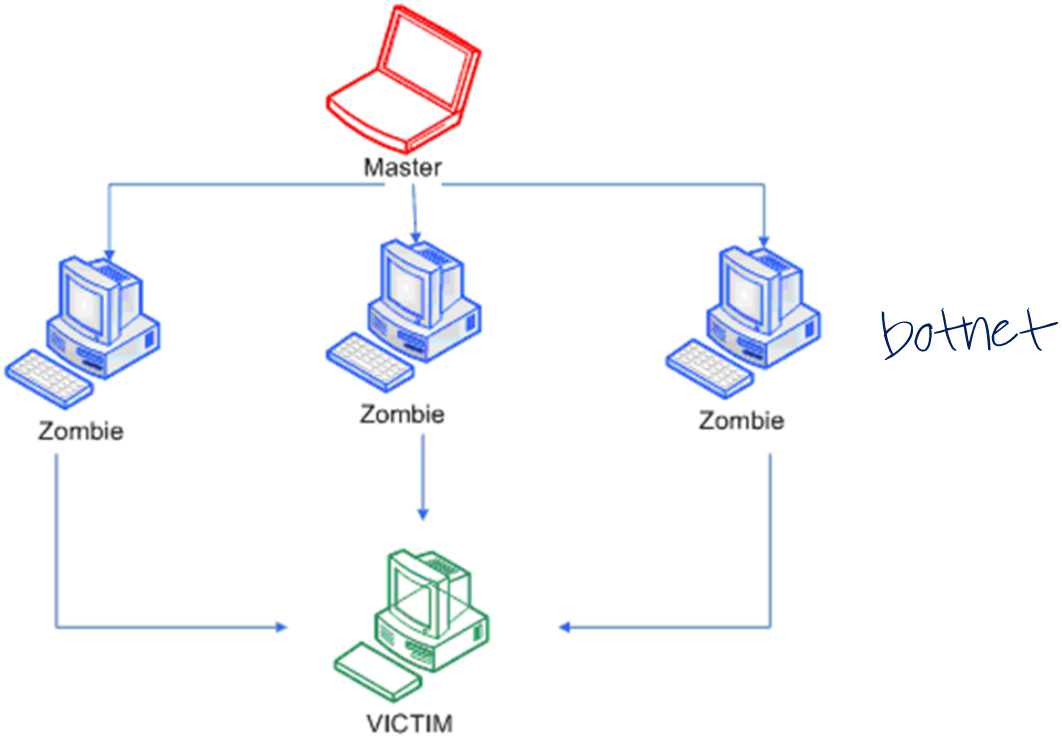
- Si «inonda» un server con un numero di pacchetti/false richieste di connessione,… più elevato di quello che è in grado di gestire «saturando» le risorse (memoria, banda,…) del server(DDoS,DRDoS)
- L'effetto è quello di un aumento nei tempi di risposta agli effettivi fruitori del servizio fino all'impossibilità di accedere al servizio stesso

Flaw Exploitation

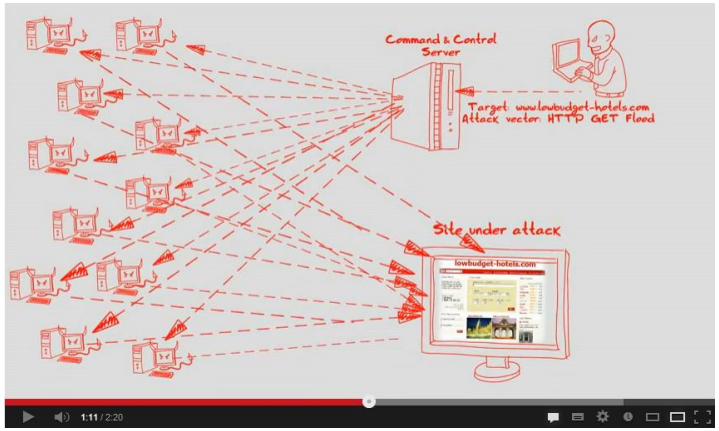
- si sfruttano delle «falle» nel software del server per mandarlo in errore (es. Ping of Death, Buffer Overflow)

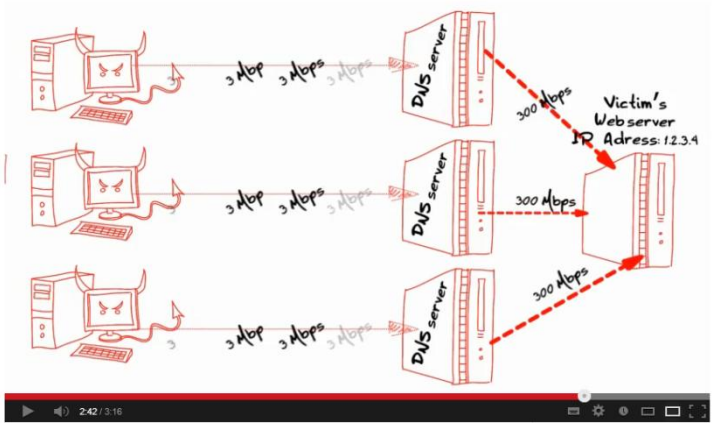
DDoS

- L’ hacker si serve di computer/server compromessi per sferrare l’attacco in maniera da non essere facilmente rintracciabile
- Gli host attaccanti(sotto il controllo dell’hacker) formano una «botnet»



DDoS e DRDoS





Per approfondire…

DoS su Wikipedia

Dos e NIDS(in inglese)

Per approfondire

- Malware_Pizzonia
- Malware_Dini
- le minacce della sicurezza dalla A alla Z
- Virus_informatici
- sicurezza_computer