# Malware (**MAL**icious soft**WARE**)

Il malware include qualsiasi programma software che viene implementato per scopi malevoli, quali:

* Furto di informazioni e spionaggio (**spyware**)
* Indebolimento delle difese per favorire un'intrusione successiva e creazione di "porte di ingresso" nascoste (**backdoor**)
* Danneggiamento e sabotaggio (**cracking**)
* Ricatto (**ransomware**), truffe (**scamware**)
* Acquisizione del controllo del computer da remoto fino allo stato di *zombie* all'interno di una **botnet**

# Virus

I **virus informatici** sono programmi di piccole dimensioni che sono in grado di replicarsi e di diffondersi in modo autonomo da un computer all'altro.

Trojan

Un veicolo per diffondere malware. Si tratta di un programma che è collegato ad un altro file apparentemente innocuo (es., videogame, file multimediale, pdf).

Si può prendere un trojan:

* Copiando file infetto da una chiavetta
* Scaricando un file e installandolo con la volontà dello stesso utente
* Aprendo un allegato di posta elettronica

Virus polimorfico

Il codice è crittografato in modo variabile, e la parte del virus che si occupa della decifratura può assumere diverse forme.

Un virus, di solito, viene crittografato per intero lasciando in chiaro solo la routine di decifratura

Un **virus polimorfico** modifica il codice della routine di decifratura a ogni nuova infezione (lasciando invariato l'algoritmo) mediante tecniche di inserimento di trash code, permutazione del codice, ecc...

Virus metamorfico

Il virus è in grado di mutare completamente il proprio codice.

È più potente del virus polimorfico in quanto evita alcuni software antivirus che possono riconoscere un virus da alcuni pattern nel codice a tempo di esecuzione.

#### Virus vs. Worm

Virus:

* Software che si aggancia ad altro software e viene eseguito allo scatenarsi di particolari eventi
* Un virus è un frammento di codice che non può essere eseguito separatamente da un programma ospite

Worm:

* Applicativo a sé stante
* Usa la rete per trovare vulnerabilità nei computer raggiunti e per diffondersi automaticamente
* Sfruttano vulnerabilità di sicurezza per diffondersi, e la loro diffusione non necessariamente dipende dal fatto di ingannare l'utente per farsi eseguire

Spyware (**SPY**ing soft**WARE**)

Tipologia di malware creato per spiare la vittima, raccogliendo informazioni sulle sue attività sul sistema e inviandole ad un host esterno.

* **criminosi**: furto di password, informazioni per accesso a conti online, numero di carta di credito, ecc...
* **fastidiosi**: reperire informazioni personali per scopi pubblicitari
* **dannosi**: tracciare tutte le azioni o tracciare l'uso di determinati servizi (es., pagine Web visitate, software utilizzato) come primo passo per ulteriori attacchi
* **investigativi**: policeware o software di parental control

# Advanced Persistent Threat (APT)

Con l'avanzamento delle tecniche di difesa, gli attacchi dei professionisti stanno diventando sempre più sofisticati, mascherati e persistenti nel tempo.

Gli APT sono tipicamente organizzazioni para-statali, ma possono essere anche organizzazioni criminali che mettono a disposizione le proprie competenze.

Passi dell'attacco:

1. Ricognizione
2. Intrusione nella rete
3. Stabilire una backdoor
4. Ottenere le credenziali dell’utente vittima
5. Installazione di molteplici programmi
6. Escalation dei privilegi, spostamento laterale ed esfiltrazione dei dati
7. Mantenere la persistenza

# Denial of Service (DoS)

La negazione del servizio (**Denial of Service – DoS**) può essere causata da:

* **Volume dei dati** trasmessi alla vittima, che provoca la saturazione delle risorse del sistema
* **Contenuto dei dati** inviati, appositamente progettati per sfruttare vulnerabilità nei servizi o nei protocolli

Metodi di attacchi:

* **Diretto**: attacco rivolto alla risorsa da rendere indisponibile
* **Indiretto**: attacco rivolto contro una risorsa differente dall'obiettivo ma indispensabile per esso

DoS che sfruttano bug, vulnerabilità:

* Ping of death
* WinNuke
* Land

DoS per esaurimento di risorse:

* DoS: Smurf e SYN flood
* DDoS: TFN
* Code Red Worm
* DrDoS

#### DoS che sfruttano vulnerabilità

Obiettivo: l'attacker sfrutta uno o più bug conosciuti dei software presenti nel sistema vittima per provocarne il crash o rendere il servizio inutilizzabile.

Ping of Death

DoS remoto mediante pacchetti ICMP malformati: sfrutta un bug del protocollo IP per cui si riusciva a generare pacchetti IP di dimensioni maggiori di 64KByte.

Invio di pacchetti ICMP echo request di dimensione maggiore della massima consentita (65535 bytes):

* Attaccante frammenta i pacchetti
* Frammenti riassemblati dalla vittima
* Errore in fase di riassemblaggio del pacchetto: crash del server della vittima

Teardrop

L'attacco **teardrop** prevede l'invio di pacchetti frammentati con porzioni dei frammenti "sovrapposti". In fase di riassemblaggio del pacchetto, la vittima non sa come procedere: crash del server.

WinNuke

WinNuke è un attacco di tipo DoS da remoto mediante l'invio di pacchetti malformati.

WinNuke prevede l'invio di un pacchetto OOB (Out Of Band, con bit URG=1) malformato alla porta TCP 139.

E’ dovuto ad un errore di progettazione della funzione che si occupa di NetBIOS: non controlla la struttura dei pacchetti Out Of Band. In ricezione, questi pacchetti sono passati direttamente al kernel senza verificare la correttezza della sintassi.

Esito dell'attacco: **Fermo del sistema**.

Land

L'attacco Land è un DoS da remoto ottenuto mediante l'invio di pacchetti creati ad hoc.

* Attaccante invia pacchetti **TCP SYN** con sorgente e destinazione identiche
* Host di destinazione tenta di instaurare una connessione con sé stesso sulla sua stessa porta di invio
  + **3-way handshake non terminerà mai**
* **Risultato**: notevole rallentamento o reboot del server vittima

Attacchi che mirano a generare DoS inondando di traffico la vittima

TCP SYN Flood

Il **TCP SYN** Flood è un attacco che si basa sulla richiesta di numerose commessioni solitamente con indirizzi IP sorgenti "spoofed" generati casualmente, senza mai completare il "three-way handshake".

Esaurimento delle risorse:

* Banda
* Coda connessioni
* Numero massimo clienti servizio

I firewall più moderni includono meccanismi per ridurre gli effetti di attacchi SYN Flood.

Primi attacchi a coinvolgere diversi host

Smurf e Fraggle

* **Smurf**: fa uso del protocollo ICMP e dei pacchetti ICMP ECHO (ping)
  + Un pacchetto ICMP (con sorgente IP spoofed) viene inviato all'indirizzo di broadcast di una rete di host
  + Tutti gli host della rete (che ricevono il ping) generano pacchetto ICMP ECHO (pong) verso quello che ritengono essere l'IP sorgente
* **Fraggle**: come Smurf, ma usando pacchetti UDP

#### Problemi degli attacchi DoS

Difficoltà nel rintracciare gli esecutori:

* Reti con strutturamulti-livello: **attaccante > master > demoni > vittima**
* Utilizzo di tecniche di spoofing
* Pacchetti con sintassi lecita

**Possibilità di saturazione della banda di rete di qualunque host collegato ad Internet**: basta un numero sufficiente di demoni per l'attacco.

# Distributed Denial of Service (DDoS)

Attacchi DoS che spingono all'estremo il concetto di flooding tramite bandwitdh consumption. Utilizzando più sorgenti per la generazione del traffico di flood (**vittime di II livello**).

Botnet (roBOT + NETwork)

Rete di computer robotizzati (zombie) che costituisce un vero e proprio esercito di computer compromessi (bots).

1. Nei computer zombie vengono installati diversi tool di cracking: scanner, exploit tool, rootkit, DoS/DDoS tool, ecc.
2. Attivazione degli host compromessi: utilizzando i tool installati, ricerca e compromissione di altri host
3. Creazione della rete per DDoS: uno o più **master** e gli altri **demon**
4. L'attacco DDoS inizia quando l'attaccante invia l'ordine ai **demon tramite il master**. Il master deve avere la lista dei demon

Creazione botnet

1. Ricerca di sistemi che possano essere compromessi, preferendo host con connessioni Internet permanente e a banda larga
2. Exploit delle vulnerabilità a scopo di compromissione degli host per conquistarne l'accesso
3. Il bot viene caricato con codice servant e molteplici strumenti di exploit, attacco e cracking: scanner, exploit tool, operating system detector, rootkit, DoS/DDoS tool
4. La botnet è gestita da un unico centro di comand e controllo (C&C) logico, che viene realizzato mediante diversi computer distribuiti in comunicazione tra loro (per affidabilità)

Metodi di propagazione

Prevalentemente "drive-by-download" che sfrutta browser e/o sistemi operativi vulnerabili.

Password deboli (incluse quelle dei database di tipo MS-SQL), Email e sistemi Peer-to-Peer.