Fondamenti di Informatica

- Accademia di Belle Arti di Verona
- Università degli Studi di Verona
- A.A. 2020-2021

- Docente - Vincenzo Giannotti

CAPITOLO 7 – SICUREZZA INFORMATICA

Sicurezza Informatica

Parlando di «Sicurezza Informatica» ci riferiamo a due aspetti principali:

- La **sicurezza delle informazioni**
- La **protezione dei sistemi informativi**

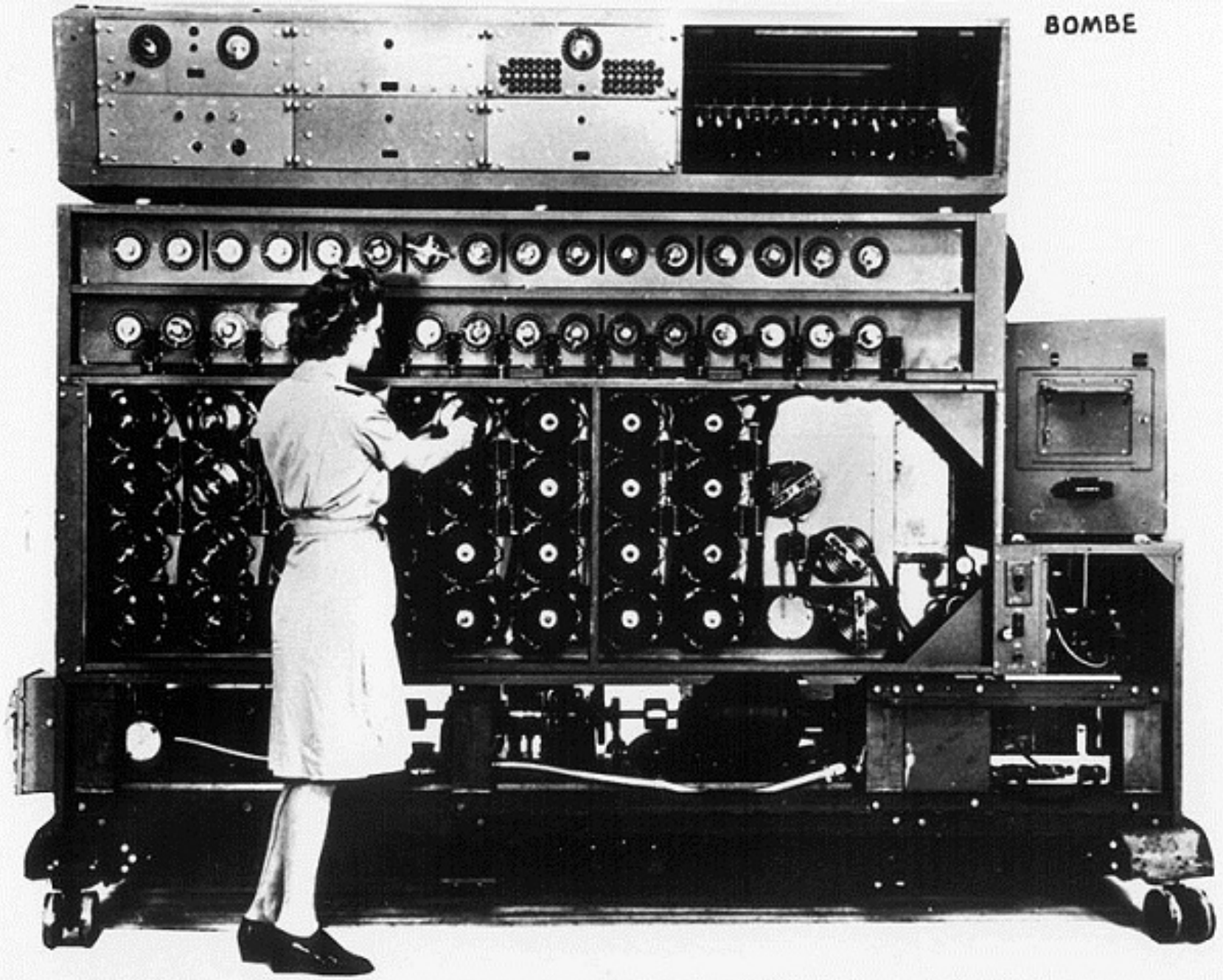
Questo significa che si deve affrontare il tema sia dal punto di vista dei «sistemi *stand alone*» sia dei «sistemi in rete» per proteggere i dati e i sistemi contro perdite, attacchi virali, intrusioni.

Sicurezza delle informazioni

- Il problema di «**come trasmettere informazioni in maniera sicura**» è antico quanto l'Uomo, o almeno, quanto l'Uomo da quando è in grado di comunicare.
- Un tempo la «riservatezza» delle informazioni riguardava prettamente il settore militare. Per garantire la riservatezza delle comunicazioni ci si affidava alla «**crittografia**», cioè alla scienza che si occupa di come codificare un messaggio e di come successivamente decodificarlo.
- Svetonio, nel suo «la Vita dei Cesari» (intorno all'anno 120 d.C.) racconta che Giulio Cesare, per la sua corrispondenza riservata, utilizzava un suo proprio codice di cifratura molto semplice: ciascuna lettera dell'alfabeto veniva sostituita con un'altra che la seguiva di qualche posizione. In pratica era come se utilizzasse un alfabeto che anziché da A -> Z andava per esempio da D -> C.

Sicurezza delle informazioni

- Alcuni importanti risultati di questa scienza si ebbero tuttavia nel periodo Rinascimentale (i.e. Tritemio – *Polygrafia* – Francoforte 1550; Giovan Battista della Porta – *De furtivis literarum notis* – Napoli 1563 e molti altri) nei quali si studiavano:
  - sistemi a trasposizione - inversione/spostamento di elementi del testo
  - sistemi a sostituzione – sostituzione di elementi del testo con segni e simboli
  - sistemi misti – entrambe le operazioni precedenti eseguite in sequenza
- Il maggiore impulso tuttavia si ebbe nel secolo scorso, durante la seconda guerra mondiale, con la costruzione di macchine molto sofisticate per la cifratura dei messaggi (Enigma - Germania) e di macchine altrettanto sofisticate per la loro decifratura (la Bomba - UK).



Sicurezza delle informazioni

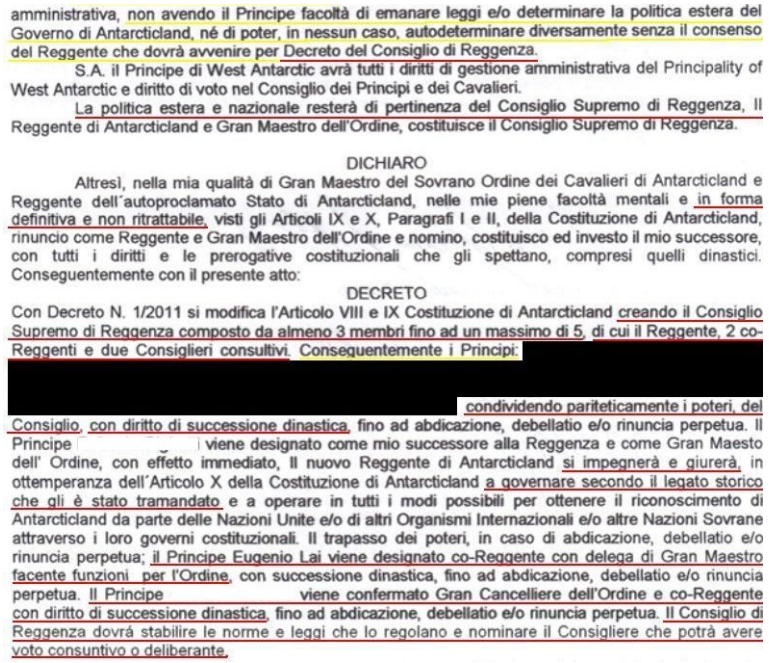
- La «**Bomba**» fu una macchina ideata da Alan Turing con lo scopo di individuare giornalmente la configurazione con cui veniva impostata la macchina «Enigma» (di cui gli Inglesi possedevano una copia esatta) utilizzata dai Tedeschi nella II Guerra Mondiale per criptare i loro messaggi.

Sicurezza delle informazioni

- Oggi, viviamo nella **società dell'informazione**, in cui lo scambio delle informazioni (per lo più digitalizzate) fa parte integrante del nostro modo di vivere e di qualsiasi nostra attività.
- Proprio per questo la sicurezza (security) è diventata una componente fondamentale da cui l'informazione stessa non può prescindere.
- Tuttavia, nel caso della informazione digitale, che come abbiamo visto riguarda ormai tutto lo scibile umano, non è più sufficiente limitarsi a garantirne la **riservatezza** – anche se la crittografia è ancora molto importante in moltissimi casi – ma è necessario garantirne anche la **disponibilità** e l'**integrità**.
- «Riservatezza», «Disponibilità» e «Integrità» sono i **tre obiettivi** fondamentali di qualsiasi sistema di sicurezza delle informazioni.

Riservatezza

- La **Riservatezza** si ottiene limitando l'accesso alle informazioni e alle risorse informatiche, solamente alle persone e ai sistemi autorizzati a farlo.
- Si può realizzare sia nella fase di archiviazione dell'informazione, sia durante la comunicazione.
- Poiché spesso una informazione è data dalla somma di più dati messi in relazione tra di loro – per esempio il mio nome e la mia data di nascita in taluni contesti hanno significato solo se abbinati, poiché consentono di riconoscermi univocamente – ne consegue che la riservatezza può dipendere dal contesto.
- Nel caso appena citato si può pensare di cifrare solo uno dei due dati (es. la data di nascita) cosicché la riservatezza dell'informazione (nome+data di nascita) sia preservata.



amministrativa, non avendo il Principe facoltà di emanare leggi e/o determinare la politica estera del Governo di Antarcticland, né di poter, in nessun caso, autodeterminare diversamente senza il consenso del Reggente che dovrà avvenire per Decreto del Consiglio di Reggenza.

S.A. il Principe di West Antarctic avrà tutti i diritti di gestione amministrativa del Principality of West Antarctic e diritto di voto nel Consiglio dei Principi e dei Cavalieri.

La politica estera e nazionale resterà di pertinenza del Consiglio Supremo di Reggenza, Il Reggente di Antarcticland e Gran Maestro dell'Ordine, costituisce il Consiglio Supremo di Reggenza.

DICHIARO

Altresì, nella mia qualità di Gran Maestro del Sovrano Ordine dei Cavalieri di Antarcticland e Reggente dell´autoproclamato Stato di Antarcticland, nelle mie piene facoltà mentali e in forma definitiva e non ritrattabile, visti gli Articoli IX e X, Paragrafi I e II, della Costituzione di Antarcticland, rinuncio come Reggente e Gran Maestro dell'Ordine e nomino, costituisco ed investo il mio successore, con tutti i diritti e le prerogative costituzionali che gli spettano, compresi quelli dinastici. Conseguentemente con il presente atto:

DECRETO

Con Decreto N. 1/2011 si modifica l'Articolo VIII e IX Costituzione di Antarcticland creando il Consiglio Supremo di Reggenza composto da almeno 3 membri fino ad un massimo di 5, di cui il Reggente, 2 co-Reggenti e due Consiglieri consultivi. Consequentemente i Principi: [redacted] condividendo pariteticamente i poteri, del Consiglio, con diritto di successione dinastica, fino ad abdicazione, debellatio e/o rinuncia perpetua. Il Principe viene designato come mio successore alla Reggenza e come Gran Maesto dell' Ordine, con effetto immediato, Il nuovo Reggente di Antarcticland si impegnerà e giurerà, in ottemperanza dell´Articolo X della Costituzione di Antarcticland a governare secondo il legato storico che gli è stato tramandato e a operare in tutti i modi possibili per ottenere il riconoscimento di Antarcticland da parte delle Nazioni Unite e/o di altri Organismi Internazionali e/o altre Nazioni Sovrane attraverso i loro governi costituzionali. Il trapasso dei poteri, in caso di abdicazione, debellatio e/o rinuncia perpetua; il Principe Eugenio Lai viene designato co-Reggente con delega di Gran Maestro facente funzioni per l'Ordine, con successione dinastica, fino ad abdicazione, debellatio e/o rinuncia perpetua. Il Principe viene confermato Gran Cancelliere dell'Ordine e co-Reggente con diritto di successione dinastica, fino ad abdicazione, debellatio e/o rinuncia perpetua. Il Consiglio di Reggenza dovrá stabilire le norme e leggi che lo regolano e nominare il Consigliere che potrà avere voto consuntivo o deliberante.

Riservatezza

- La riservatezza in gran parte dipende dalle procedure software che adottiamo e dall'hardware che utilizziamo, ma anche il fattore umano ha il suo peso.
- Poiché nella catena della sicurezza l'elemento più debole spesso siamo **noi stessi**, vi sono alcune semplici regole da seguire che ci possono aiutare a fare la nostra parte:
  - Mantenere segrete la propria password e cambiarla immediatamente se viene per qualche motivo comunicata ad altri
  - Utilizzare password non banali (e.g. il mio nome, la mia data di nascita etc.)
  - Tenere sotto controllo gli accessi al proprio sistema (p.e. con password di accesso al computer)
  - Rifiutare di fornire informazioni a persone di cui non siamo assolutamente certi (p.e. via mail a sedicenti tecnici che chiedono i vostri dati)
  - Cifrare i nostri documenti più riservati (*in primis* quelli che contengono le password)

Disponibilità

- Il secondo obiettivo è quello della **Disponibilità**.
- Garantire la disponibilità delle informazioni significa far si che queste siano **accessibili** agli utenti che ne hanno diritto, **nel momento in cui essi lo richiedano**.
- Questo implica che i nostri sistemi, la rete e le applicazioni, debbono fornire le prestazioni richieste e che in caso di malfunzionamento ovvero di eventi catastrofici, esistano delle procedure, degli strumenti e delle persone, in grado di ripristinare la completa funzionalità dei sistemi in tempi accettabili (**disaster recovery**).
- Si deve quindi:

Disponibilità

- preservare la disponibilità delle **condizioni ambientali** (energia, temperatura, umidità etc.), utilizzando idonei sistemi di controllo, sistemi di climatizzazione e gruppi di continuità
- preservare la disponibilità delle **risorse hardware e software** anche a fronte di problemi di varia natura (guasti, errori, disastri etc.), utilizzando sistemi di backup (per gli archivi) e sistemi ridondanti (per l'hardware)
- preservare i sistemi da **attacchi esterni**, per esempio provenienti da Internet, utilizzando sistemi di firewall (per il controllo degli accessi), sistemi antivirus (per la protezione del computer da software dannosi), sistemi antispyware (per la rimozione di software spia).

Disponibilità - esempio

- Il **backup** normalmente avviene su due supporti distinti che poi vengono mantenuti in luoghi distinti. Il cosiddetto **piano di backup** (programmato) consiste nella definizione di:
  - cosa salvare (dischi, database, cartelle, utenti, macchine, volumi, ecc.)
  - frequenza di backup (giornalmente, settimanalmente etc.)
  - ora di avvio del backup
  - supporto e percorso di archiviazione
  - tipologia di backup (completo, differenziale, incrementale)
  - modalità di compressione, tipo di log e messaggistica da esporre, tipo di verifica integrità, e molte altre opzioni a seconda della complessità del sistema.

Disponibilità - esempio

- La **ridondanza** in ingegneria consiste nella **duplicazione dei componenti critici** di un sistema con l'intenzione di aumentarne l'affidabilità e la disponibilità, in particolare per le funzioni di vitale importanza che servono a garantire la sicurezza delle persone e degli impianti o la continuità della produzione.
  - RAID (Redundant Array of Independent Disks) è una tecnica molto utilizzata anche in piccoli sistemi, per realizzare un insieme ridondante di dischi indipendenti
  - Talvolta si utilizzano sistemi ridondanti dislocati in aree diverse, con lo scopo di garantirne il funzionamento in caso di eventi catastrofici

Disponibilità - esempio

Incendio OVH a Strasburgo

- È un'azienda di web hosting francese che possiede 31 datacenter per un totale di 250.000 server. L'azienda ha implementato il protocollo IPv6 ed è uno dei più grandi hosting d'Europa.
- Il giorno 10 marzo è andato a fuoco un intero datacenter a Strasburgo che ha coinvolto moltissimi Virtual Private Service e sistemi di backup. Moltissime aziende coinvolte, alcune delle quali hanno perso irrimediabilmente i loro dati e i loro siti web, attendono di conoscere le cause d'incendio.
- La società rischia una class action se fossero confermate responsabilità oggettive nella gestione del datacenter e sulla "qualità" del recovery plan.

Integrità

- L’**integrità** riguarda il grado di correttezza, coerenza e affidabilità sia delle informazioni, sia delle risorse informatiche.
- Quando si parla di **informazioni**, il concetto di integrità riguarda il fatto che queste non possano venire alterate, cancellate o modificate per errore o per dolo. Questo significa, per esempio, che all’interno di un database i dati devono essere tra loro coerenti (quando inizia una transazione il database si trova in uno stato coerente e quando la transazione termina si deve trovare in un nuovo stato coerente; ciò significa che non debbono verificarsi contraddizioni tra i dati archiviati)

Integrità

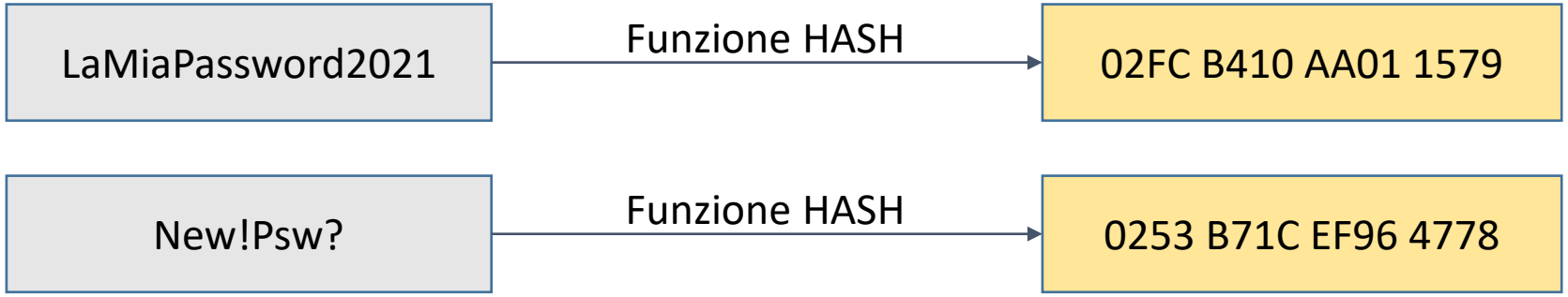
- Quando si parla di **hardware**, l'integrità si riferisce invece:
  - alla corretta elaborazione dei dati da parte della macchina (che potrebbe avere dei malfunzionamenti)
  - alla garanzia di un adeguato livello delle prestazioni (la rete può essere oberata o richiedere una banda maggiore di quella realmente disponibile)
  - al corretto instradamento dei dati in rete (nel caso di malfunzionamenti dovuti per esempio ad accessi indesiderati)
  - altri eventuali fattori.
- Infine l'integrità può riguardare il **software**; in tal caso ci si può riferire a:
  - completezza e correttezza delle applicazioni
  - correttezza dei file di sistema e dei file di configurazione
  - altri fattori.

Integrità - esempio

- Molti protocolli di comunicazione di rete, assicurano il controllo sull'integrità dei dati scambiati in una comunicazione attraverso un campo cosiddetto «**checksum»** contenuto nell'intestazione di ciascuna unità d'informazione (pacchetto) scambiata tra due peer. Alcuni degli eventuali errori di trasmissione possono essere corretti utilizzando delle opportune tecniche di recupero.
- Vi sono poi altri protocolli di tipo **crittografico** - come i Transport Layer Security (TLS) e i loro predecessori Secure Sockets Layer (SSL) - che assicurano il controllo dell'integrità dei dati attraverso meccanismi crittografici.
- Il «HyperText Transfer Protocol over Secure Socket Layer» (**HTTPS**) è un protocollo a livello applicativo che realizza la comunicazione sicura utilizzando il TLS (o SSL).

Integrità - esempio

- Ancora, le cosiddette tecniche di «**Hashing**» sono impiegate per verificare che le informazioni non vengano alterate per dolo o per errore (anche a causa di errori di trasmissione). Queste stesse tecniche sono anche utilizzate in crittografia.
- Una **funzione crittografica di hash** è un algoritmo matematico che trasforma un messaggio di lunghezza arbitraria in una stringa di bit di lunghezza fissa chiamata valore di hash o impronta del messaggio.
- La funzione crittografica di hash ideale ha tre proprietà fondamentali:
  - È molto semplice calcolare;
  - È irreversibile (dal hash non si può risalire al testo che l'ha generato);
  - È deterministica (lo stesso testo genera sempre lo stesso hash).



Integrità - esempio

- L'**Encryption**, a differenza del Hashing, è una operazione reversibile (two-ways function). Il messaggio può essere decriptato utilizzando una chiave.
- Le password vengono normalmente salvate sotto forma di hash e mai in chiaro. Essendo il hash una funzione one-way, la password non può essere ricostruita ed è per questo motivo che quando ce la dimentichiamo dobbiamo resettarla e sceglierne una nuova.

Altri obiettivi di sicurezza

- Oltre ai tre principali obiettivi di sicurezza citati, possiamo averne anche altri che oggigiorno sono considerati di rilevante interesse in relazione ad alcune specifiche tipologie di transazione:
- **Autenticità** – per essere certi che un messaggio o un documento sia attribuito al suo **autore** e a nessun altro
- **Non ripudio** – per impedire che un autore possa disconoscere la paternità di un dato documento da lui redatto.
- Entrambe queste caratteristiche trovano applicazione nella

FIRMA DIGITALE

- in cui vengono utilizzate specifiche tecniche che garantiscono sia l'integrità del documento (hashing) sia la sua provenienza (crittografia).

General Data Protection Regulation (GDPR)

- Dal momento che l'informazione è un bene che deve essere tutelato e garantito, ogni organizzazione aziendale deve adottare tutti i provvedimenti necessari affinché ciò avvenga.
- Nel contesto attuale, in cui si ha una proliferazione dei rischi informatici ed in particolare di quelli dovuti alla violazione dei sistemi di sicurezza, esistono a carico di Enti e Aziende dei precisi obblighi di legge, soprattutto in materia di tutela della **privacy e di trattamento dei dati personali.**
- In questo contesto si inserisce il **GDPR**: il nuovo Regolamento UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

General Data Protection Regulation (GDPR)

- Con **GDPR** è andata in soffitta la vecchia direttiva 95/46/CE (regolamento generale sulla protezione dei dati) che a partire dal maggio 2018 è stata completamente sostituita.
- GRPR prevede, oltre a una serie di raccomandazioni, che sia tenuto un **registro delle attività di trattamento**, che deve contenere una serie di informazioni, tra cui le finalità del trattamento, la descrizione delle categorie di interessati e di dati personali che vengono trattati, l'indicazione delle misure di sicurezza adottate.
- L'onere della tenuta del registro è a carico del titolare dell'impresa ed eventualmente del responsabile del trattamento.

General Data Protection Regulation (GDPR)

- Il registro permette di monitorare e tenere sotto controllo le varie operazioni di trattamento dei dati personali all'interno dell'organizzazione.
- Enti e Società devono eventualmente nominare un «Responsabile del trattamento dei dati», che è una persona competente e indipendente in grado di assicurare:
  - Trasparenza
  - Sicurezza dati
  - Adozione di misure tecniche e organizzative.
- Attraverso l'adozione di queste misure l'impresa persegue l'obiettivo fondamentale di garantire che «**solo persone autorizzate**» possano accedere a informazioni cosiddette «**sensibili**».

Il controllo degli accessi

- I processi di «**Autenticazione**» servono a verificare l'identità di chi sta accedendo ad un dato sistema, attraverso un procedimento che può essere di questo tipo:
  - Vengono eseguiti dei **test** sull'identità dell'utente
    - L'utente presenta alcune **credenziali** (password, certificato digitale) come prova della propria identità
  - Una volta che l'utente è stato autenticato, gli viene concesso l'accesso alle sole risorse per cui è **autorizzato** (per esempio mediante controlli di accesso, permessi, privilegi).
- La «**Autorizzazione»** che è un concetto ben distinto da quello di Autenticazione è il diritto accordato all'utente (che può essere una persona, ma anche un software) di accedere ad un sistema e alle sue risorse, in base ad un dato **profilo**.

Il controllo degli accessi

I metodi di Autenticazione più diffusi sono abbinati alla utilizzazione di:

- Password
- Token
- Dispositivi Biometrici

In generale si considera che tali metodi si basino su:

- qualcosa che **sai** (password, codice etc...);
- qualcosa che **hai** (token, smartcard etc...);
- qualcosa che **sei** (caratteristiche della retina, impronta digitale, voce etc…).

Il controllo degli accessi

- I metodi di Autenticazione da utilizzare possono dipendere da diversi fattori:
  - La tipologia di Utenza da autenticare
  - Il Valore delle Informazioni da proteggere
  - La Distribuzione delle risorse informative.
- In funzione dei fattori suddetti e del grado di sicurezza che intendiamo ottenere, adotteremo uno dei metodi citati ovvero una loro combinazione.
- Vale la pena di sottolineare che, poiché l'autenticazione tramite un dato noto solo al possessore è considerato un metodo vulnerabile (la password si può facilmente dimenticare), normalmente si tende a sostituirla con una combinazione di più metodi (e.g. scheda + PIN).

Il controllo degli accessi – la Password

- La richiesta di una **password** (parola d'ordine) è senz'altro uno dei più antichi metodi di autenticazione.
- Mentre nei primi computer i metodi di riconoscimento delle password erano piuttosto superficiali e spesso si limitavano a conservate un elenco di codici/stringhe in chiaro su un file (consideriamo però che a quel tempo non si parlava certo di attacchi informatici), con l'andar del tempo i metodi di confronto divennero sempre più sofisticati. Nel 1967 fu introdotto l'**hashing** delle password che come abbiamo visto è il metodo tuttora più utilizzato.
- Nel caso del hashing il sistema conserva in un file i nomi degli utenti e l'hash delle relative password; durante l'autenticazione, l'hash viene ricalcolato in base alla password digitata e viene confrontato con quello registrato.

Il controllo degli accessi – la Password

- Abbiamo anche visto che una funzione HASH è di tipo non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.
- Non è banale riuscire a carpire in maniera fraudolenta una password codificata tramite una funzione HASH. Questo tuttavia può avvenire nel caso in cui:
  - Vengano utilizzati dei metodi di keystroke sniffing o di network sniffing
  - Mediante tecniche del tipo «social engineering» in cui con dei metodi di manipolazione l'attaccante si fa rivelare dati riservati utili per l'accesso
  - attraverso la costruzione di un «dizionario» cui applicare l'algoritmo di hash

Il controllo degli accessi – la Password

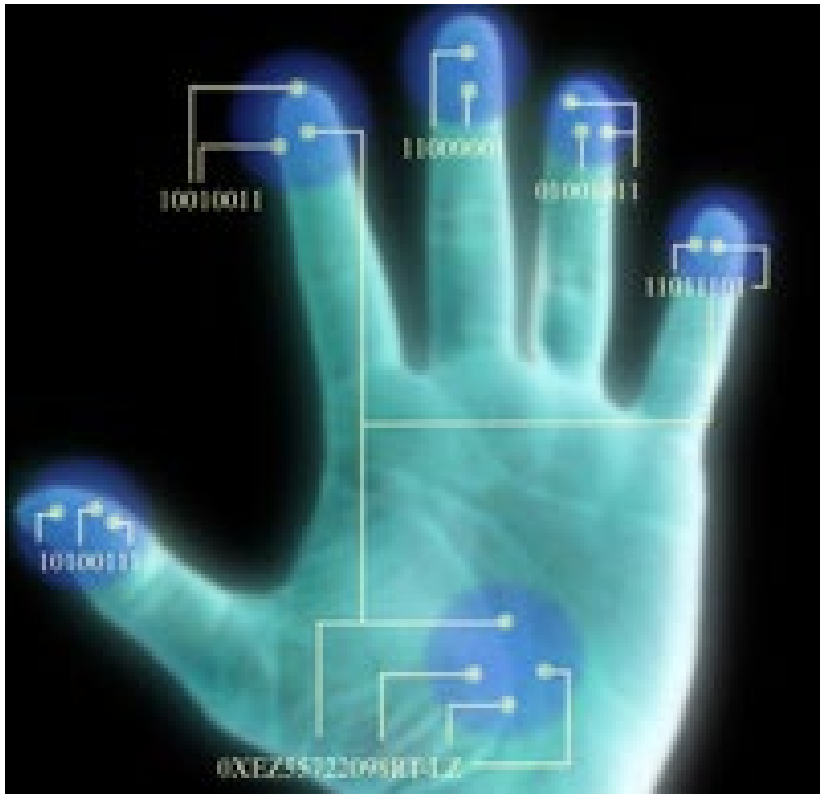
- Alcuni parametri da utilizzare per la creazione e il mantenimento di una buona password possono essere:
  - **Lunghezza -** più la password è lunga, più sarà difficile da decifrare
  - **Tipologia dei Caratteri –** possibilmente una password dovrebbe contenere minuscole, maiuscole, cifre ed altri segni (quando concessi)
  - **Contenuto -** dovrebbero essere evitati nomi di persone, luoghi, date, parole del dizionario e soprattutto nomi riconducibili all'utente
  - **Durata –** è consigliabile modificare la password con una certa frequenza, ovviamente scegliendo una nuova password diversa
  - **Conservazione** – se si intende memorizzare la password da qualche parte, conviene utilizzare un file crittato.

Il controllo degli accessi – il Token

- Il **token** è un dispositivo elettronico portatile in grado di generare un codice di sicurezza in base ad un algoritmo che talvolta tiene conto del «momento» in cui viene utilizzato.
- L'utente normalmente possiede un suo proprio codice che combinato con quello generato dal token fornisce una password che viene riconosciuta dal server di autenticazione.
- Questo metodo, di tipo misto, è uno dei più difficili da violare, poiché l'oggetto fisico deve essere posseduto al momento della autenticazione e il possessore sa se questo è stato smarrito o gli è stato rubato.
- Per contro il token ha un certo costo, si può rompere e può essere smarrito.
- I Token possono essere di tipo «**passivo**» (il bancomat o un dispositivo RFID) o di tipo «**attivo**» (una smartcard dotata di processore crittografico).

Il controllo degli accessi – la Biometria

- I **Sistemi Biometrici** utilizzano le caratteristiche fisiche o comportamentali di una persona per verificarne l'identità.
- Le caratteristiche fisiche più utilizzate per l'autenticazione biometrica sono:
- **Impronte digitali** - gli scanner per impronte digitali sono molto diffusi ed hanno un costo ridotto
- **Geometria delle mani** – è un metodo più solido del precedente che però richiede che le mani siano pulite
- **Scansione della Retina o dell'Iride** – utilizzata per lo più in installazioni militari o governative che richiedono elevati standard di sicurezza. Quest'ultimo metodo richiede un'esposizione prolungata a bassa intensità luminosa ed è considerato «intrusivo» sebbene non rechi alcun danno agli occhi.



Il controllo degli accessi – la Biometria

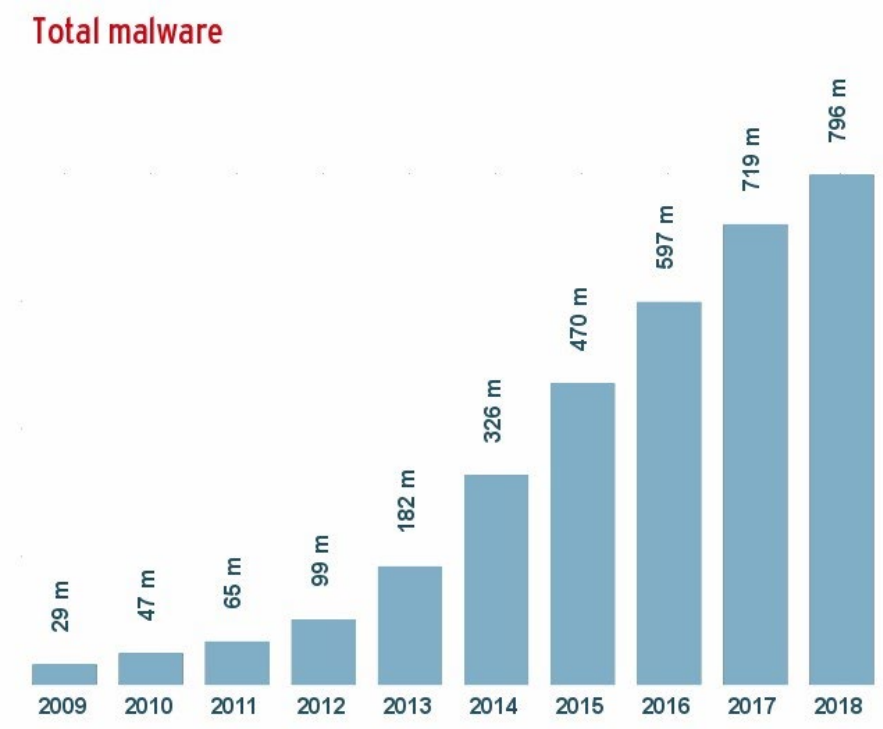
- **Riconoscimento del Volto** – può essere utilizzato all'insaputa del soggetto e in taluni casi anche tra la folla (sistemi antiterrorismo)
- **Voce** – è un metodo che analizza l'impronta vocale del soggetto e rientra tra i metodi di analisi comportamentale
- **Firma** – anche questo rientra tra i metodi di riconoscimento basati sul comportamento
- **Digitazione della Tastiera** – si tratta di un metodo che riconosce il comportamento dell'utente di fronte alla tastiera: pressione di battitura, ritardo tra le battute etc…

Attacchi informatici

Quando si parla di sicurezza informatica il termine **malware** indica un software creato per causare danni a un computer o ai dati degli utenti di un computer, oppure danno ad un intero sistema informatico.

Il termine deriva dalla contrazione delle parole inglesi «**mal**icious» e «soft**ware»** e significa «codice maligno».

In circolazione esistono diversi tipi di malware molti dei quali sono illegali e pericolosi. Il fenomeno della diffusione di malware è in continua evoluzione tanto che il 2017 ha fatto segnare un +20% di minacce a livello globale rispetto al 2016 e un +10% nel 2018 rispetto al 2017 (l'Italia è uno dei paesi più colpiti in Europa).



*Fonte: Cyber Security 360

Attacchi Informatici

- Tutte le minacce «… possono creare notevoli danni. Il più diffuso e comune è l'encryption dei dati locali e di rete della macchina infetta, che costringe l'utente al pagamento di un riscatto per poter ottenere i mezzi per recuperare i propri dati. Gli utenti e le aziende più sprovveduti, ovvero coloro che non si sono premuniti di avere un backup verificato, sono costretti a pagare. Spesso, purtroppo, succede che nonostante il pagamento i criminali svaniscano lasciando in seri guai i malcapitati»*.
- Col termine "**ransomware**" ci si riferisce proprio a questo: un attacco informatico teso alla richiesta di un riscatto.
- Quello portato da **WannaCry**, che nel maggio 2017 è stato capace di infettare centinaia di migliaia di computer nel giro di poche ore, è stato un attacco di questo tipo. Molti esperti del settore l'hanno considerato come il peggior attacco informatico degli ultimi anni, sia per velocità di contaminazione, sia per portata dell'attacco. WannaCry ha messo in pericolo il funzionamento di molti uffici pubblici, ospedali, catene di montaggio e fabbriche.

*__David Gubiani__, security engineering manager di Check Point Italia.

Tipi di Malware

- Nel seguito vediamo alcuni dei più diffusi tipi di Malware*:
  - **Virus**: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Sono in grado di replicarsi autonomamente.
  - **Worm**: questi malware non hanno bisogno di infettare altri file per diffondersi. Essi modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più le reti di computer e Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di **ingegneria sociale** (studio del comportamento individuale di una persona al fine di carpire informazioni utili) oppure sfruttano dei difetti (**Bug**) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

*fonte Wikipedia

Tipi di Malware - esempi

- Nel 1949 **John von Neumann** dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente.
- Nei primi anni ‘60 un gioco ideato da un gruppo di programmatori dei **Bell Laboratories,** nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda, dava l'inizio alla storia dei virus informatici.
- **Jerusalem** è uno dei più vecchi (1987) e noti virus informatici comparsi per i sistemi MS-DOS e fu il virus con il più alto numero di file infettati.
  - Il nome trae origini dal fatto che all'epoca si riteneva che il virus avesse fatto la sua prima comparsa in un computer di una università di Gerusalemme. Analisi successive (1991) hanno invece dimostrato che il virus ha fatto la sua prima comparsa in **Italia.**
  - Il virus si agganciava poi ai processi di **interrupt** del sistema (gli interrupt 8 e 21) e dopo 30 minuti di esecuzione rallentava le attività del computer di un fattore 10. Il virus aveva poi una bomba logica: se si accorgeva che la data del sistema era un «venerdì 13» iniziava a cancellare ogni file che l'utente cercava di aprire.

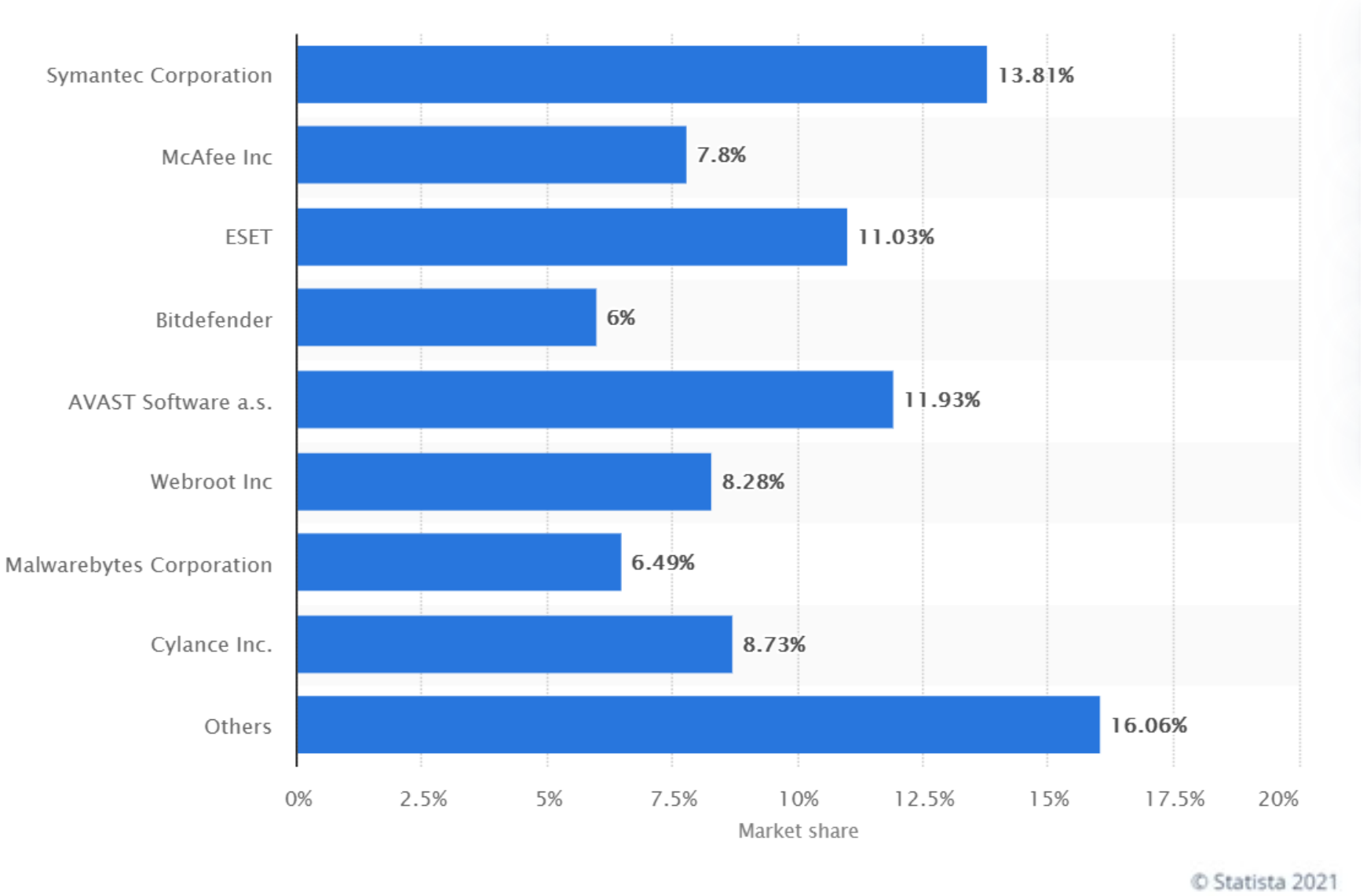
Tipi di Malware

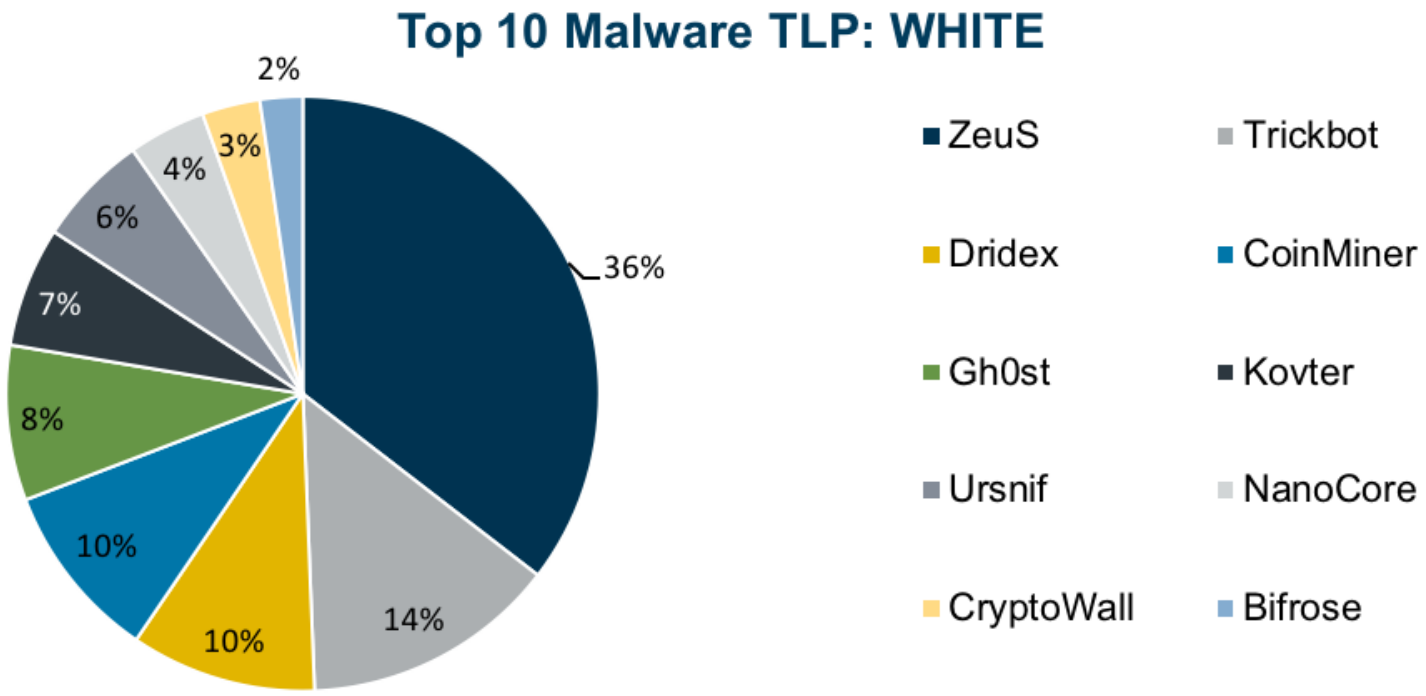
- **Trojan horse**: deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto. I trojan non si diffondono autonomamente.
- Spesso i Trojan (come pure virus e worm) hanno lo scopo di installare dei **Keylogger**, ossia degli strumenti di **sniffing**, hardware o software, in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio o di un altro computer.
- Altre volte i Trojan (come pure virus e worm) installano delle **Backdoor**, ossia delle porte che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico consentendo ad un Hacker di accedere illegittimamente al sistema.

Tipi di Malware

- **Spyware**: software che sono utilizzati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono essere di vario tipo: dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
- **Dialer**: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.
- **Adware**: programmi software che presentano all'utente messaggi pubblicitari durante l'uso. Possono causare danni quali rallentamenti del computer e rischi per la privacy in quanto talvolta comunicano le abitudini di navigazione dell’utente ad un server remoto.

Mercato dei principali produttori di anti-malware per sistemi windows





- **ZeuS** è un Trojan che attacca Microsoft Windows e altri SO come Android. Zeus agisce come un Trojan di servizi finanziari. Il malware riconosce che l'utente si trova su un sito di una banca e registra i tasti digitati. Il creatore del malware ha reso pubblico il codice sorgente di Zeus nel 2011, dando il via alla creazione di versioni nuove e aggiornate tuttora circolanti.

- **NanoCore** è distribuito principalmente con attacchi di phishing via e-mail: molte delle campagne in corso che distribuiscono il malware sono progettate per apparire come fatture o ordini di acquisto con nomi di allegati progettati per invogliare ad aprire gli allegati. Il creatore di questo malware è stato condannato per questa sua attività criminosa e tuttavia durante la sua permanenza in carcere il suo malware ha continuato a circolare. L'autore infatti ne ha distribuito il codice nel **dark web**.

NanoCore consente di compiere diverse azioni da remoto tra cui:

- Spegnimento e riavvio del PC
- Esplorazione dei file salvati
- Accesso e controllo del Task manager (Gestione attività)
- Modifica dell'editor di registro di sistema
- Controllo del mouse
- Apertura di pagine web
- Disattivazione del LED che indica l'uso della webcam
- Cattura di audio e video
- Rilevamento di password e credenziali di login

Deep-Web e Dark-Web

- Il **deep web** è l'insieme delle risorse informative del World Wide Web (www) non indicizzate dai normali motori di ricerca. Per dare l'idea dell'estensione del deep web si stima che dell'insieme delle informazioni di cui è costituito il web, solamente qualche percentuale sia effettivamente indirizzata dai maggiori motori di ricerca. Di questa categoria fanno quindi parte nuovi siti non ancora indicizzati, pagine web a contenuto dinamico, software, siti privati, pagine scritte in linguaggi diversi dal html, contenuti banditi dai normali motori di ricerca e molto altro.
- Il **dark web** invece è un sottoinsieme del deep web. Questa parte del web è normalmente non raggiungibile attraverso una normale connessione Internet in quanto si compone anche di parti di reti private sovrapposte alla rete Internet (le cosiddette darknet). Per l'accesso è necessario utilizzare dei software specifici che consentano l'utilizzazione di tali reti.
- Il dark web viene sovente impiegato per occultare materiale illegale. All'interno vi si può trovare un po' di tutto:
  - condivisione di file illegali o contraffatti
  - protezione della privacy di cittadini sotto sorveglianza
  - compravendita di beni o servizi illegali
  - aggiramento della censura propria di internet e dei sistemi di filtraggio
  - …..

Anti-Malware

- Gli Anti-malware (o più comunemente Anti-virus) sono dei software che hanno lo scopo di prevenire, rilevare ed eventualmente rendere inoffensivi i codici malware.
- Gli **Anti-virus** propriamente detti, non sono in grado normalmente di proteggere in maniera completa un sistema informatico, ma necessitano di essere abbinati ad altri software come gli **Anti-spam**, i **Firewall** etc..

Anti-virus

- I classici Anti-virus sono normalmente composti da più parti:
    - Un **file di firme** - è un archivio che contiene tutte le firme dei virus conosciuti.
    - Un **programma anti-virus** - permette di eseguire su richiesta una serie di operazioni, la scansione completa del sistema o di singoli files, l'eliminazione dei file sospetti etc..
    - Un **programma di ascolto** – caricato in memoria all'avvio richiama l'anti-virus ogni volta che viene creato o modificato un nuovo file o una zona di memoria.
    - Un **programma** che provvede su richiesta, all'aggiornamento del file delle firme

Anti-spyware

- Gli **anti-spyware** sono programmi utilizzati per eliminare dal sistema diverse tipologie di malware e in particolare spyware, adware. Le funzioni di questi programmi sono simili a quelle degli antivirus, ma non sono la stessa cosa poiché gli anti-virus propriamente detti proteggono il computer solamente da una tipologia di malware: i virus appunto.
- È vero però che spesso gli «anti-virus» sono distribuiti come suite complete che includono anche funzioni anti-malware e firewall.

Antispam

- Lo **spamming** è l'invio di messaggi indesiderati (generalmente di tipo commerciale e pubblicitario) ed è noto anche col nome di «posta spazzatura».
- Poiché lo spam viene inviato senza il permesso del destinatario è considerato altamente dannoso anche dagli Internet Service Provider.
- Questi ultimi vi si oppongono non solo per i costi generati dal traffico indesiderato ma anche perché può verificarsi una violazione contrattuale della «Acceptable Use Policy» che può essere causa di interruzione dell'abbonamento da parte dell'utilizzatore.
- Gli **antispam** sono software che analizzano la provenienza e/o il contenuto dei messaggi, effettuando una azione di filtraggio.

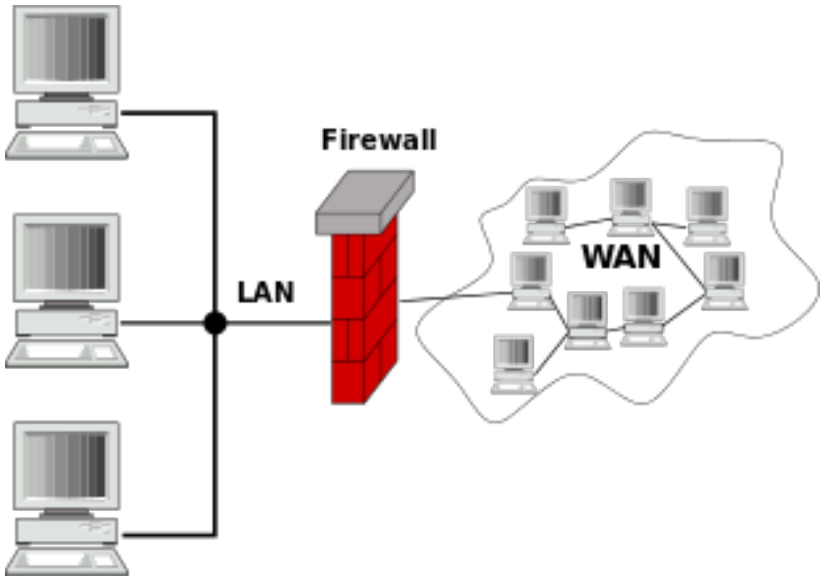
Anti-virus

- **Nod32** (ESET azienda slovacca) molto discreto, controlla, scansiona e si aggiorna in modo del tutto automatico e continuo.
  Più volte premiato in passato come miglior antivirus, viene venduto oggi in una suite che comprende anche la funzione di firewall, antispyware e di antispam.
- **Kaspersky** invece si presentava come una suite completa già da tempo e, teoricamente, per la sua completezza, dopo averla installata non ci si dovrà più preoccupare della sicurezza del proprio computer: è un firewall, un antispyware, un antivirus.
- **Norton** è un buon antivirus ma talvolta degrada le prestazioni del computer.
- **McAfee** come Norton ma più leggero.

Anti-virus

Tra gli antivirus free vale la pena di citare:

- **Bitdefender Free edition** viene da molti definito come il miglior antivirus sulla piazza, anche nella sua versione free.
- **Avira Antivirus Free** eccellente antivirus free in italiano. Offre una protezione real time che sta al livello di quelli a pagamento. Avira pesa poco sulle risorse, non occupa troppa cpu e ram e protegge senza farsi notare come deve essere.
- **Avast** è l'antivirus free in italiano salito alla ribalta perché è stato scelto da Google.
- **Comodo Internet Security** non è in italiano. È però probabilmente la migliore suite free di protezione del computer. Comodo è l'unico che offre un completo strumento di protezione gratis, con antivirus, antimalware e firewall di ottimo livello.



Firewall

- Il **firewall** (muro tagliafuoco) è un componente passivo (hardware o software) di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più parti di rete.
- Normalmente la rete viene divisa in due sottoreti: una esterna che comprende Internet, l'altra interna che comprende i computer utilizzati nella nostra rete locale (LAN).

Honeypot

- Il **honeypot** (barattolo del miele) è un sistema o componente hardware o software usato come «trappola» ovvero «esca» a fini della protezione contro gli attacchi di pirati informatici.
- Normalmente è utilizzato per proteggere reti locali.
- Solitamente consiste in un computer dedicato o un sito web che «sembra» contenere informazioni importanti e preziose ma che in realtà non contiene alcuna informazione sensibile.

Alcuni semplici consigli

- Scegliere password quanto più sicure possibile.
- Se dobbiamo visitare un sito che non conosciamo, meglio accedervi attraverso una ricerca fatta con un motore di ricerca. Questi ultimi infatti forniscono già essi stessi un primo livello di protezione ai loro utenti, segnalando eventuali siti o portali ritenuti non sicuri.
- Prestiamo attenzione quando vogliamo installare programmi scaricati da Internet; molti di questi infatti (anche molto diffusi) ci inducono subdolamente ad installare dei componenti aggiuntivi che in seguito possono rivelarsi molto fastidiosi.
- Se desideriamo fare acquisti on-line, meglio utilizzare PayPal o carte prepagate ovvero creare una carta di credito virtuale.
- Non rispondere mai a Mail che richiedono dati personali.

PROSSIMO CAPITOLO

Self Test #2

Applicazioni di produttività personale