Fondamenti di Informatica

Accademia di Belle Arti di Verona

Università degli Studi di Verona

A.A. 2018-2019

Docente - Vincenzo Giannotti

CAPITOLO 7 – SICUREZZA INFORMATICA

Sicurezza informatica

Col termine «Sicurezza Informatica» intendiamo:

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

Questo significa 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

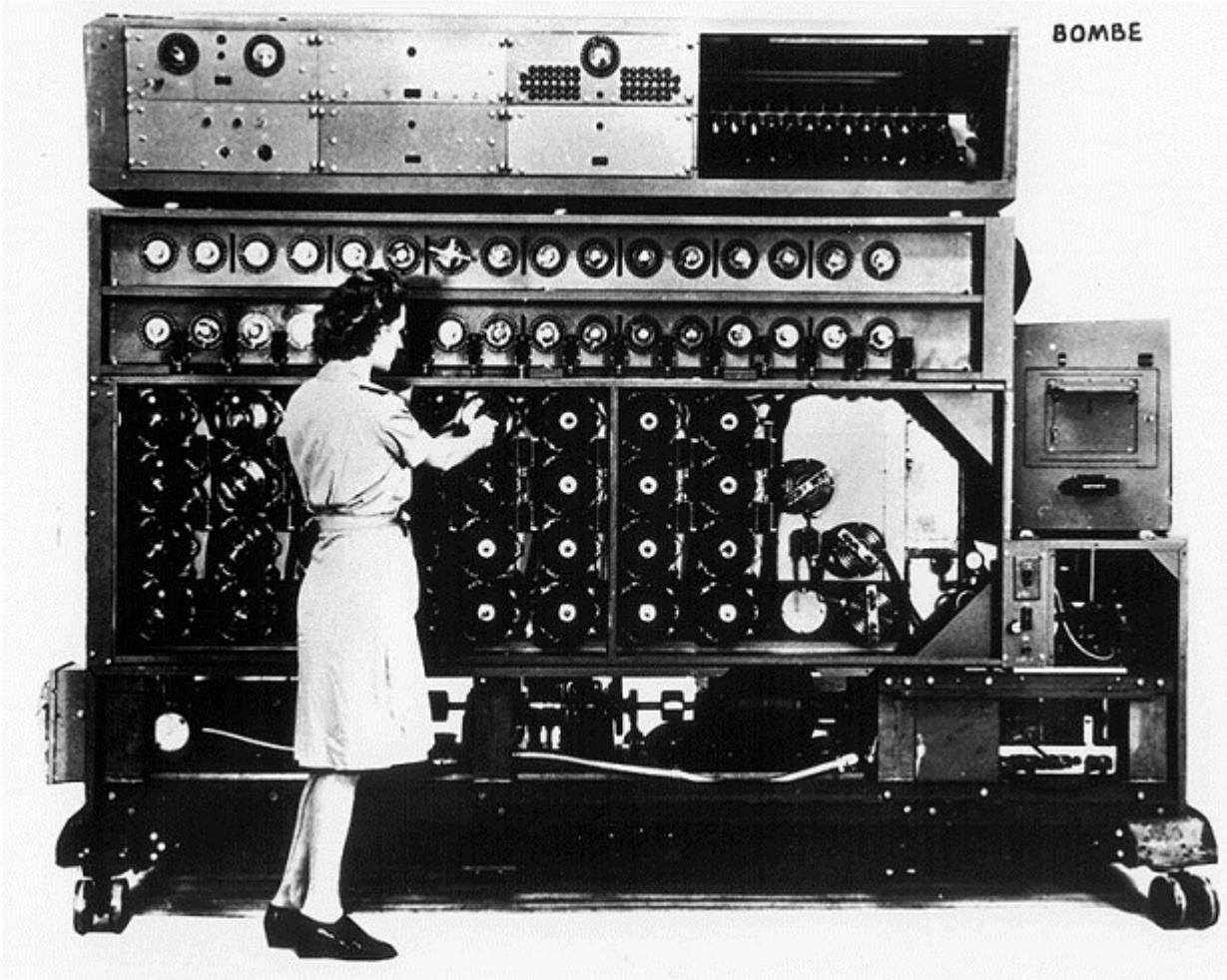
Il problema della «**sicurezza delle informazioni**» è antico quanto l'Uomo, o almeno, quanto l'Uomo da quando può comunicare.

Un tempo la «riservatezza» delle informazioni riguardava prettamente il settore militare e la «**crittografia**», cioè la scienza che si occupa di come codificare un messaggio e di come successivamente decodificarlo.

Alcuni importanti sviluppi di questa scienza (già nota a Greci e Romani) si ebbero nel Rinascimento (sistemi a trasposizione, a sostituzione o sistemi misti), ma il maggiore impulso si ebbe nel secolo scorso, durante la seconda guerra mondiale, con la costruzione di macchine molto sofisticate per la cifratura dei messaggi (Enigma) e di macchine altrettanto sofisticate per la loro decifratura (la Bomba).

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** – 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.

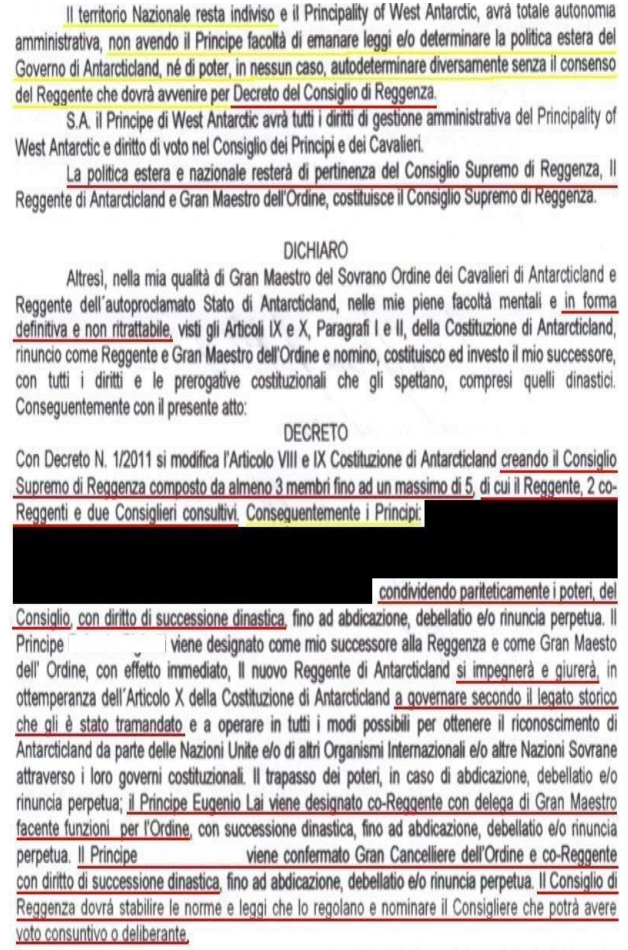
Riservatezza

La **Riservatezza** consiste nel limitare l'accesso alle informazioni e alle risorse informatiche, solamente alle persone e ai sistemi autorizzati a farlo.

La riservatezza 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 (e.g. la data di nascita) cosicché la riservatezza dell'informazione (nome+data di nascita) sia preservata.



Il territorio Nazionale resta indiviso e il Principality of West Antarctic, avrà totale autonomia 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 dovrà 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 le proprie password
- Utilizzare password non banali (e.g. il mio nome)
- Tenere sotto controllo gli accessi al proprio sistema (p.e. con password di accesso)
- 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)

Un esempio recente di violazione

Recentemente è stato diffuso pubblicamente il database «Collection #1», una raccolta di oltre 770 milioni tra email e password, generata in alcuni anni raccogliendo i dati di una serie di successive violazioni realizzate da fonti diverse.

Questa Collection #1 è stata posta recentemente al centro dell'attenzione mediatica in quanto è stato pubblicato un servizio web, raggiungibile su https://haveibeenpwned.com/ che consente a chiunque di verificare, in maniera gratuita, se la propria email o la propria password, ovvero entrambe, siano state violate e fanno parte della collezione, quindi di fatto a disposizione degli hacker.

Un esempio recente di violazione

Attraverso la pubblicazione di **Collection #1** un qualsiasi hacker sarebbe in grado di incrociare senza grossi problemi le email ele password violate o semplicemente le password utilizzate sui diversi siti con un account email, per prendere il controllo dei servizi sottoscritti da un qualsiasi utente inconsapevole.

Le conseguenze di un tale accesso indesiderato, per esempio ad un account violato, potrebbero essere diverse:

Il phishing, con cui un hacker potrebbe recuperare l'elenco dei contatti di una vittima con tutto ciò che ne potrebbe conseguire; un attacco mirato ad effettuare il furto di una identità digitale che potrebbe portare alla sottrazione di denaro alla vittima o a comprometterne un profilo sui social.

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

1. preservare la disponibilità delle **condizioni ambientali** (energia, temperatura, umidità etc.), utilizzando idonei sistemi di controllo, sistemi di climatizzazione e gruppi di continuità;
2. 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);
3. 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** consiste nella definizione di:
  - cosa salvare (dischi, database, cartelle, utenti, macchine, volumi, ecc.)
  - quanti backup effettuare
  - frequenza di effettuazione dei diversi backup (settimanalmente, giornalmente, più volte al giorno etc.)
  - orario 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.
  - Talvolta si utilizzano sistemi dislocati in aree diverse.
  - Nel nostro piccolo quotidiano possiamo per esempio utilizzare un NAS (Network Attached Storage) in configurazione RAID (Redundant Array of Independent Disks):
    - RAID 0 che permette di collegare due o più dischi sommandone la capacità (nessuna ridondanza).
    - RAID 1 detto *mirroring* nel quale i dati vengono replicati su ciascun hard disk (minimo 2) garantendo il funzionamento del NAS anche in caso di rottura di uno di questi.

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.
- Ancora, le cosiddette tecniche di «**hashing**», 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.

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).

Verifica dell’identità, controllo degli accessi e protezione dei dati personali

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: un metodo tuttora 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

Alcuni parametri da utilizzare per la creazione e il mantenimento di una buona password possono essere:

- **Lunghezza -** più la password è lunga, più è difficile da decifrare
- **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 necessita di un'esposizione prolungata a bassa intensità luminosa. E' considerato un metodo «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…

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 sia garantita la **Privacy** delle persone.

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)

- **GDPR** abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ed è divenuto pienamente applicabile a partire dal 25 maggio 2018.
- GRPR prevede 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.
- Debbono essere garantiti una serie di diritti a tutti coloro che in qualsiasi modo mettono a disposizione i propri dati per gli usi più disparati (i.e. per una assunzione) e le necessarie informative debbono essere comunicate in maniera chiara ed inequivocabile.

General Data Protection Regulation (GDPR)

- La tenuta del registro costituisce un adempimento molto importante in quanto permette di monitorare e tenere sotto controllo le operazioni di trattamento dei dati personali all'interno dell'organizzazione.
- Enti e Società debbono nominare un «Responsabile del trattamento dei dati»: una persona competente e indipendente che ha diversi obblighi tra cui:
  - Garantire gli obblighi di trasparenza
  - Garantire gli obblighi di sicurezza dei dati
  - Adottare le necessarie misure tecniche, organizzative e informative.

Per questo motivo uno dei principali obiettivi di una qualsiasi azienda è quello di garantire che «**solo persone autorizzate**» possano accedere a informazioni cosiddette «**sensibili**».

Attacchi informatici

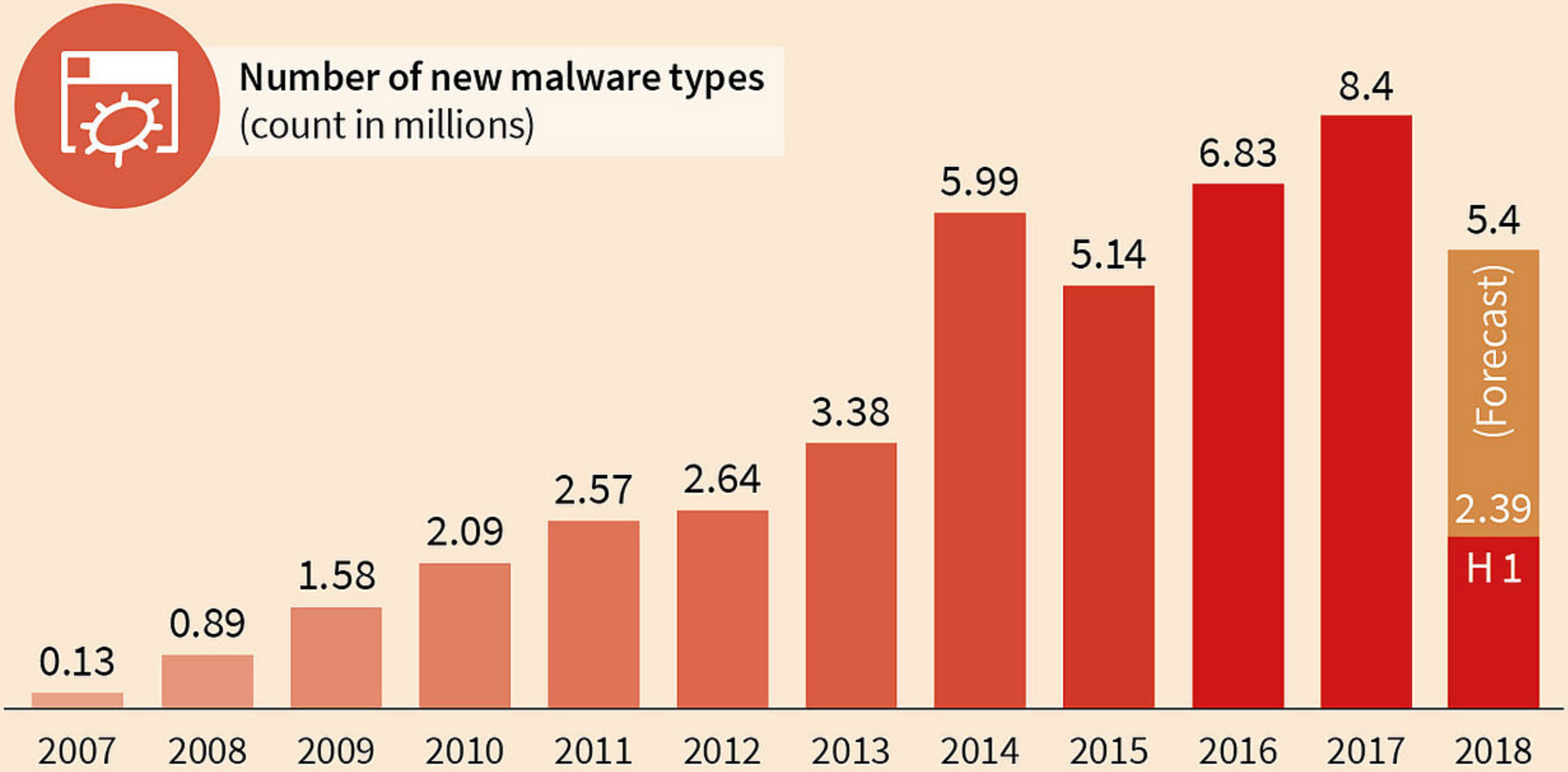
Quando parliamo di sicurezza informatica utilizziamo frequentemente il termine **malware.** Questo indica un software creato per causare danni a un computer o ai dati degli utenti di un computer, oppure ad un intero sistema informatico.

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

In circolazione esistono diverse tipologie di codici maligni e molti di questi sono illegali e pericolosi. Il fenomeno della diffusione di malware è in continua evoluzione tanto che il 2016 ha fatto segnare un +30% di nuove minacce* a livello globale rispetto al 2015 e un ulteriore +20% circa nel 2017. Nel 2018 dovrebbe esserci stato un certo calo.

*Fonte: G Data

Number of new malware types
(count in millions)



Ransomware

Tutte i metodi di attacco «… 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»*.

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

Tipi di Malware

Gli attacchi informatici, come il ransomware che abbiamo appena visto, per essere attuati hanno bisogno di qualcosa che riesca a penetrare le difese di una rete o di un computer o di una persona. Questi possono essere dei programmi (i malware già citati) o anche dei metodi. Nel seguito ne vediamo alcuni tra i più diffusi (fonte Wikipedia):

1. **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. **Jerusalem** fu uno dei primi (1987) e noti virus informatici comparsi per i sistemi MS-DOS e fu il virus con il più alto numero di file infettati. All'epoca si riteneva che il virus avesse fatto la sua prima comparsa in un computer di una università di Gerusalemme. Analisi successive (1991) dimostrarono che il virus comparve per la prima volta in **Italia.**

Tipi di Malware

2. **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.
3. **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.

Tipi di Malware

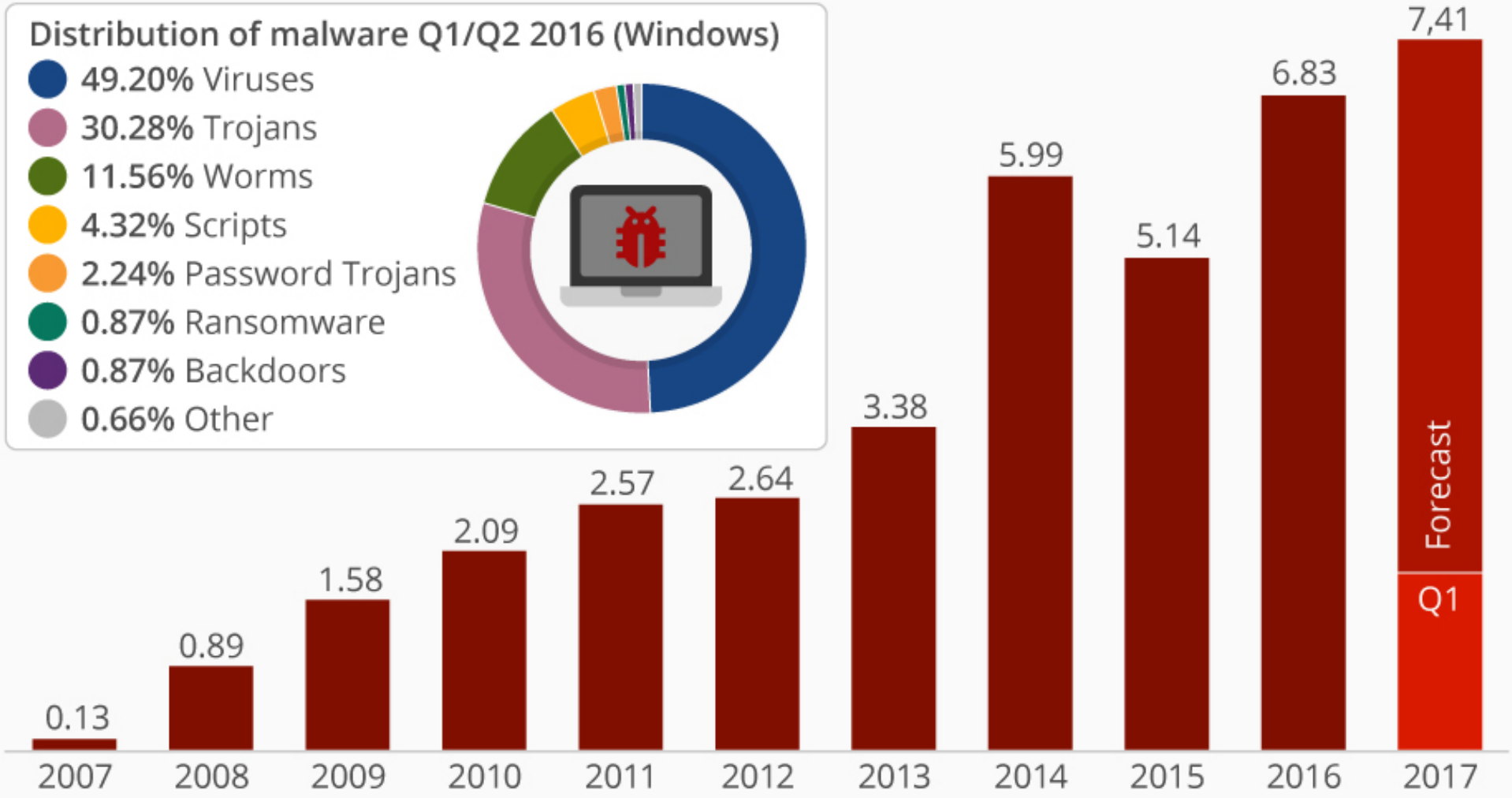
3. Spesso i Trojan (come pure virus e worm) hanno lo scopo di installare dei **Keylogger**, ossia degli strumenti di **sniffing**, hardware o software, in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio o di un altro computer.
4. Altre volte i Trojan (come pure virus e 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.
5. **l'ingegneria sociale** (social engineering) è invece un **metodo** utilizzato per lo studio del comportamento individuale di una persona con lo scopo di carpire informazioni utili, per esempio una chiave crittografica di accesso ad un sistema. E’ un modo molto efficace e di amplissima diffusione.

Tipi di Malware

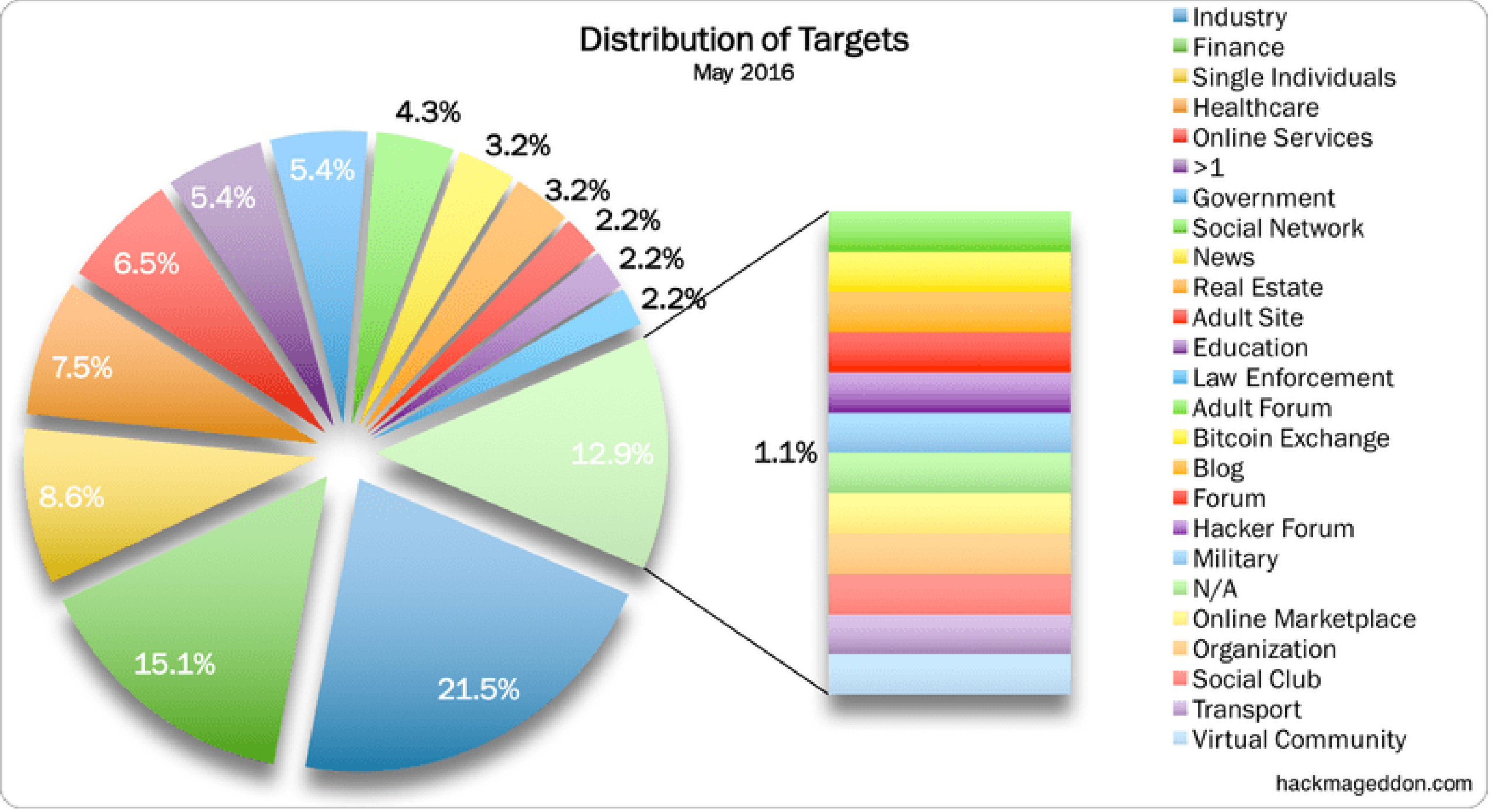
6. **Spyware**: software che sono utilizzati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono essere di vario tipo: dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
7. **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.
8. **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.

Viruses, Worms and Trojan Horses

Number of new malware specimen (in millions)



 Source: G DATA, AV-TEST


Distribution of Targets
May 2016
4.3%
3.2%
3.2%
2.2%
2.2%
2.2%
5.4%
5.4%
6.5%
7.5%
8.6%
15.1%
21.5%
12.9%
1.1%
Industry
Finance
Single Individuals
Healthcare
Online Services
>1
Government
Social Network
News
Real Estate
Adult Site
Education
Law Enforcement
Adult Forum
Bitcoin Exchange
Blog
Forum
Hacker Forum
Military
N/A
Online Marketplace
Organization
Social Club
Transport
Virtual Community
hackmageddon.com

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:

1. Un **file di firme** - è un archivio che contiene tutte le firme dei virus conosciuti.
2. Un **programma anti-virus** - permette di eseguire su richiesta una serie di operazioni, come l'aggiornamento del database delle firme, la scansione completa del sistema o di singoli files, l'eliminazione dei file sospetti etc..
3. 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.
4. 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.

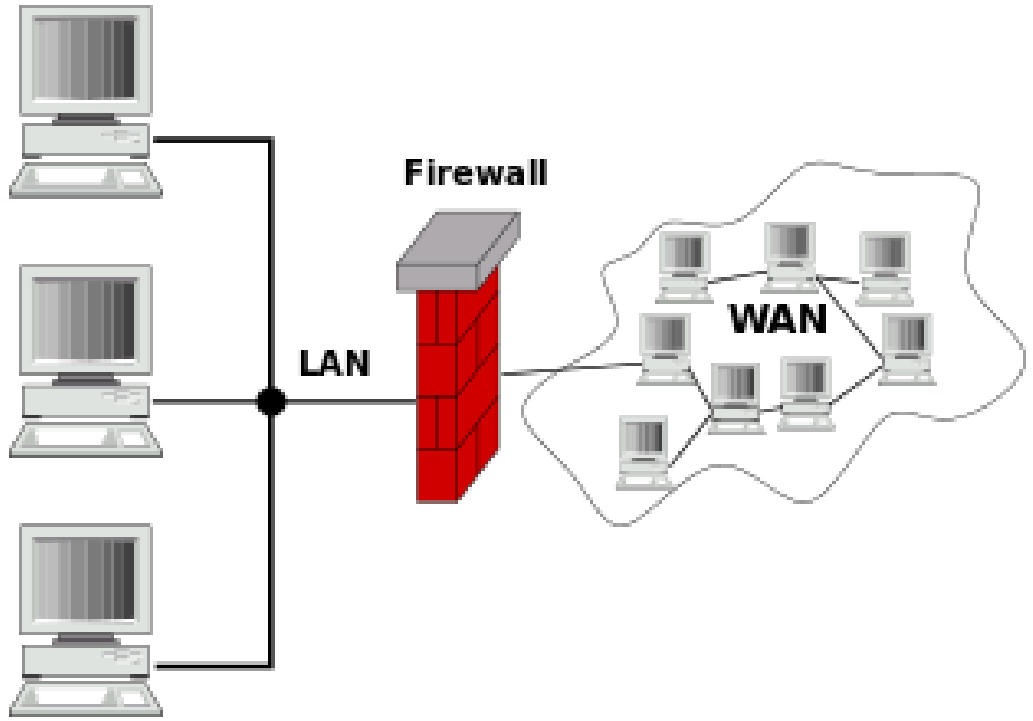
È vero però che spesso gli «anti-virus» sono distribuiti come suite complete che includono anche funzioni anti-malware e firewall.

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.

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

1. Scegliere password quanto più sicure possibile.
2. 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.
3. 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.
4. Se desideriamo fare acquisti on-line, meglio utilizzare PayPal o carte prepagate ovvero creare una carta di credito virtuale.
5. Non rispondere mai a Mail che richiedono dati personali.

PROSSIMO CAPITOLO

GIS, Progetti EU e Nuove Tecnologie