

Computer Security Threats

Le minacce cyber hanno iniziato ad interessare da quando tutti i settori economici hanno iniziato ad appoggiarsi ad internet. Questo problema, non è un discorso globale, bensì nazionale. Si tratta di proteggere i propri confini, precisamente il proprio CYBER SPACE, composto da estensione di internet, dai dati e dai sistemi informativi.

Molte aziende sono state colpite → gli hacker rubano i BENI INTANGIBILI (brevetti, informazioni sui clienti, metodologie...) che sono il cuore dell'azienda, e ne costruiscono un'altra, che produce le stesse cose ma le vende a metà. → le industrie crollano e sono centinaia le azioni legali in corso.

Gli attacchi arrivano a tutti, recentemente, è stato colpito per una settimana il nostro sistema militare.

All'inizio i sistemi Power-Grid possedevano sistemi prioritari, cioè dei protocolli privati, che erano più sicuri. Infatti chi li sapeva usare, era un numero finito di persone, facilmente rintracciabili nel caso di attacchi. A causa dell'aumentare dei prezzi, si sono iniziati ad appoggiare a sistemi open (TCP/IP).

TCP/IP era efficiente ma era molto vulnerabile, infatti quando fu pensato, non si era dato peso alla sicurezza ma più ad un problema di resilienza.

Si è d'accordo nel pensare che la prosperità di un Paese sarà legato al livello di sicurezza del proprio Cyber Space → già ora, quando si fanno dei workshop per attirare investitori in una Nazione, si informano su: la presenza di lavoro e la cyber security.

La crescita economica di una nazione è legata alla digitalizzazione infatti vi è un aumento dell'1-2% del PIL per ogni 10% dei cittadini connessi.

Quindi in questo momento si sta avendo una forte digitalizzazione, ma anche un aumento dei problemi cyber crime (es. attacchi di fishing tramite email).

Casi di EMAIL DI FISHING:

1. Il CEO di un'azienda invia un'email, contenente un allegato, sul 50° anniversario della relazione diplomatica tra Germania e Israele. In verità, era finta → appena si apriva l'Excel allegato, era richiesto di abilitare le macro. Dopo aver consentito, si infiltrava il primo stadio del malware. Per farlo crescere, successivamente, venivano inviati altri componenti.
2. È successo poche settimane fa: il CEO di una grande azienda europea manda un'email al suo corrispettivo americano richiedendo, per motivi di advertising (insospettabili e scritti dal punto di vista stilistico in maniera perfetta), il trasferimento di 15 milioni di euro su un conto corrente → in pochi minuti tutti i soldi sparirono

Le prime infrastrutture attaccate furono quelle critiche, cioè quelle del gas, le centrali idriche, del petrolio. Venivano prese di mira per prenderne il controllo. Anche i ministeri sono nel mirino → si ha molta paura, infatti se il MEF (Ministero dell'Economia e della Finanza) italiano, che si occupa di gestire il bilancio nazionale, viene conquistato, l'Italia verrebbe messa in ginocchio nel giro di un giorno.

Si ricevono un numero dell'ordine delle migliaia di attacchi al giorno. Per ATTACO si intende una mossa fatta da internet verso i confini del cyber space per vedere se ci sono delle vulnerabilità da cui entrare → si è compreso che gli hacker agiscono la sera o nei week-end, cioè quando si pensa che le difese siano meno forti

Perché Internet è un posto interessante da cui attaccare? 3 motivi:

- È un punto asimmetrico, da casa posso attaccare diversi target
- I tools necessari sono poco costosi (1000-2000 euro) e le console sembrano dei videogiochi
- Grande difficoltà nell'attribuire un reato → solitamente se si scopre è dovuto ad una fuga di notizie

Il NIST nel Computer Security Handbook definisce la computer security come: la protezione garantisce a un sistema informativo automatizzato di preservare gli obiettivi di integrità, disponibilità e riservatezza delle risorse del sistema di informazione stesso,

La sicurezza si basa su 3 pilastri:

1. La Confidenzialità: che comprende:

- la riservatezza dei dati → garantisce che le informazioni private o riservate non siano rese disponibili o divulgare a persone non autorizzate
- privacy → assicura che gli individui abbiano il controllo e l'influenza su quali informazioni su loro stesse possono essere conservate e da chi e a chi possono essere comunicate

In relazione alla Privacy, recentemente, ci fu un top attack chiamato TOP SECRET (DOSSIERAGGIO) che prendeva informazioni prima sulle celebrità e poi sui cittadini. Questo potrebbe portare ad un uso improprio delle informazioni.

2. L'Integrità: suddiviso in:

- integrità dei dati → assicura che le informazioni ed i programmi possono essere modificati solo tramite una specifica ed autorizzata maniera
- integrità del sistema → garantisce che un sistema esegue la sua funzione prevista in maniera perfetta, esente da manipolazioni non autorizzate intenzionali o accidentali.

3. La Disponibilità → assicura che un sistema lavora subito e un servizio non è negato agli utenti autorizzati

Un esempio di attacco alla disponibilità è quando un gruppo di host viene infettato e un orchestratore li lancia tutti verso un web server che si sovraccarica e muore. (NASA) → ora è più difficile in quanto non esiste un unico server ma un gruppo, il problema è che le botnet, cioè le nuvole infette, si allargano sempre più e anche attraverso protocolli di amplificazione, gli available server non riescono più a controllarli. Il fatto è che se si attacca un webserver, il danno è contenuto, ora però cercano di recare danno alle infrastrutture di telecomunicazione occupando l'intera banda.

Altri due concetti aggiuntivi sono:

1. Autenticità → la proprietà di verificare chi gli utenti dicono di essere e che ogni ingresso, che arriva al sistema, proviene da una fonte attendibile
2. Tracciabilità → l'obiettivo della sicurezza genera la necessità di azioni di una entità tracciabile univocamente. Ciò permette di supportare il rilevamento e la prevenzione di intrusione, l'isolamento di guasti...

Minacce

La loro descrizione viene fatta nella RFC 2828:

1 tipico quando si fa un attacco (EXPLIT) si cerca di vedere quali sono i bug e si fa il salto dei diritti

1. Divulgazione non autorizzata → l'entità ottiene l'accesso a dei dati a cui non è autorizzato
È un attacco alla Confidenzialità → vengono inclusi:
 - Exposure → intenzionalmente od accidentalmente vengono rilasciate informazioni sensibili (dimenticanza di una pennetta o un computer, errori di software...)
 - Intercettazione → qualsiasi dispositivo collegato ad una rete LAN può ricevere copia dei pacchetti destinato ad un altro dispositivo. Su internet possono essere prese e-mail o trasferimento dati

- Interferenza → un hacker può ottenere informazioni osservando il modello di traffico su rete

Usato anche per difesa → un'azienda era fallita ma aveva dei conti particolarmente cristallini → tramite l'interferenza dello scambio di email, si riuscì a tracciare come avvenivano le conversazioni e fu arrestato un gruppo di 7 persone (presidente e dirigenti strategici) che falsificava i conti

- Intrusione → un hacker supera le protezioni di controllo di accesso di sistema entrando anche se non autorizzato

2. Inganno → un ente autorizzato riceve dati falsi credendoli veri

Viene attaccata l'integrità. Abbiamo due sottocategorie:

- Masquerade → un utente non autorizzato cerca di entrare fingendosi uno autorizzato (logica dei cavalli di Troia → sembra che svolgono funzioni utili in realtà cercano di accedere alle risorse di sistema)

- Falsificazione → alterazione o sostituzione di dati validi o introduzione di dati falsi in un file o database

3. Rottura → impedimento del corretto funzionamento dei servizi di sistema e delle funzioni

Si attacca la disponibilità o l'integrità del sistema. Ne fanno parte:

- Incapacità → distruzione fisica o danneggiamento all'hw del sistema. Oppure un sw maligno potrebbe disabilitare il sistema o alcuni servizi

- Corruzione → un sw dannoso potrebbe far operare le risorse del sistema o le funzioni dei servizi in una maniera non volontaria. Oppure un utente potrebbe ottenere l'accesso non autorizzato e modificare delle funzioni di sistema

4. Usurpazione → il controllo dei servizi o le funzioni del sistema passa ad un soggetto non autorizzato

Viene intaccata l'integrità del sistema

Nella realtà, gli attacchi furono suddivisi in altre 4 categorie:

- a. Upstream monitoring → un hacker fa un accordo con un Telco provider, il quale si impegna ad inviargli tutti i messaggi, email, dati scambiati di una o più persone → non esiste più sicurezza → caso SNOWDEN → ha scoperto che gli USA ottenevano ed analizzavano i dati di tutti i cittadini da aziende come Microsoft, Google, Apple...erano 13 → costretti da una clausola di un atto a seguito dell'11 settembre

Furono spiate anche Petronas e Saudi Aramco (compagnie petrolifere) → Brasile legiferò che se si vuole aprire un servizio di posta, i server devono trovarsi tutti nel loro paese → nel 2014 anche la Russia introdusse questa legge

Lo spionaggio potrebbe portare ad una nuova configurazione di internet

- b. Downstream monitoring → caso di prima esteso con gli ISP
- c. Malware → armi digitali che cercano di penetrare sistemi → se interessanti vengono ingranditi tramite l'invio di componenti, altrimenti uccisi

Esempi:

STUXNET → malware che ha rallentato di anni il programma atomico iraniano → venivano attaccati i sistemi SCADA che gestivano le centrifughe che purificavano l'uranio. Infatti se giravano al di sotto di un certo limite, venivano distrutte. Il malware le rallentava un minuto ogni due ore → tramite fuga di notizie si suppose che i responsabili furono gli USA (partito da Bush e continuato da Obama) grazie all'operazione Olympics Game → l'infezione fu introdotta tramite una pennetta

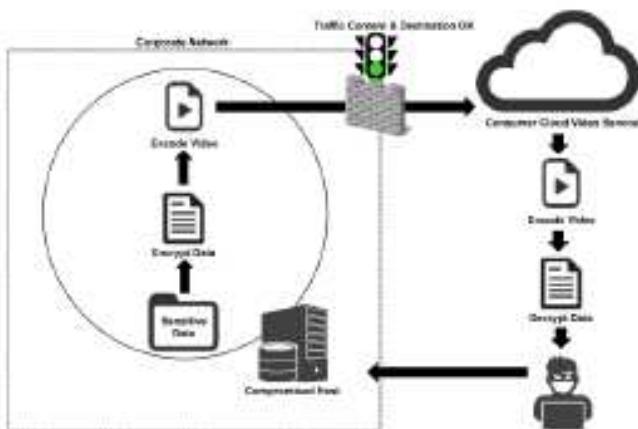
GAUSS → è ancora in corso un attacco alle banche libanesi → non si trova la sede principale del malware

I malware solitamente sono cifrati, anche se lo trovassi, non sempre si capisce che fa. Per questo è stata introdotta la SAND BOX in cui possono essere fatti detonare e possono essere studiati. Ormai sono così intelligenti che riescono a capire quando vengono aperti da un umano, in una sand box, quindi non scoppiano più → nuovo campo di ricerca che cerca di ricreare movenze umane da delle macchine.

- d. Denial Service → sovraccarico delle risorse (esempio fatto prima sull'utilizzo dei botnet)

Operazioni per scaricare dati:

1. Hacker inserisce il malware nel sistema, tramite attacchi, email di fishing o fisicamente
2. Filma un video, tramite webcam, dei dati interni e grazie alla stenografia li cifra
3. Automaticamente viene caricato su un gestore di media pubblico, il firewall non lo blocca
4. L'hacker scarica il video e lo decifra



Top attack nel 2014:

- ◊ Ramsonware → l'amministrazione italiana subì due attacchi (ott e gen) fu pagato il riscatto
- ◊ Cyber Espionage → furono registrate numerose conversazioni della Germania, e quindi della Merkel, dal cosiddetto Regin, infrastruttura della Balcom. I mandanti sembrerebbero gli USA e Inghilterra
- ◊ Wiping → ci fu la cancellazione totale dei sistemi della SONY, non si è più sicuri della responsabilità della Corea del Nord
- ◊ Cyber2Physical → sono i tipi di attacchi più paurosi, (altro esempio è STUXNET) → paura per le centrali idroelettriche o elettriche → degli altriforni in Germania si spensero
- ◊ Dox(x)ing → raccolta di informazioni prese sia da open source (facebook, twitter...) sia attraverso attacchi a strutture (ospedali, amministrazione...) → prima si cercavano dati su celebrità, ora su chiunque → gli hacker le prendono per fare, ad esempio, delle email di fishing più attendibili, oppure per un furto di identità che gli permette di aprire mutui → lo sviluppo di una "big-data mentality" permette di fare attacchi mirati ed efficaci

Negli ultimi anni gli attacchi a strutture ospedaliere raddoppiarono, questo è sempre legato alla raccolta di informazioni.

Information is beautiful è un sito che raccoglie un insieme dei dati sugli attacchi fatti dal 2000 ad oggi. Considera il numero, il tipo ed a chi. Si può notare che negli anni, l'uso dei malware è aumentato esponenzialmente, e le strutture prese di mira, non sono le grandi società, ma legate alla quotidianità della gente (supermercati, negozi di bricolage...) → il motivo non è chiaro ma si pensa che sia sempre per raccogliere più informazioni possibili, e sia per la facilità di infiltrazione

Chi è dietro le minacce cyber?

All'inizio erano ragazzi universitari che creavano virus con l'obiettivo di diffonderli il più possibile. Spesso si firmavano o si "costituivano" per ottenere più notorietà possibile.

Dal 2004 gli hacker cambiarono il loro obiettivo. Iniziarono ad attaccare strutture importanti ed a nascondersi dietro la rete. Molte volte sono "sponsorizzati" dallo Stato stesso, ad esempio in Cina ci sono tre squadroni, di cui uno, chiamato 5541, è stato individuato a Shanghai.

Anche l'ISIS riuscì ad infiltrarsi nei webserver di molti giornali, non recarono danni ma posizionarono la loro bandiera virtuale su tutte le pagine.

I nomi dei vari malware (STUXNET, GAUSS, ZEUS...) sono inventati da chi li scopre.

Per prima cosa si cerca di attribuirli ai vari gruppi conosciuti.

Cosa si studia di un avversario?

1. Il livello di esperienza

Un esempio di gruppo organizzato molto avanzato è l'Equation Group: i loro attacchi sono considerati tra i più efficaci e sconvolgenti. Il procedimento era semplice: colpivano un computer, se il malware trovava dati interessanti, richiedeva altre componenti.

Solitamente, per liberarsi di un malware, è sufficiente resettare il computer, ma il loro persisteva. Successivamente si scoprì che avevano attaccato circa 12 case hardware. Non si capisce come hanno fatto, infatti, per fare questo erano necessari attack command propri dei proprietari dell'azienda.

2. Le risorse disponibili → più sono esperti, più hanno soldi

3. Obiettivi → se cercano dati, o vogliono prendere il controllo...

4. Come entrano → tramite email fishing, o usb...

5. Comportamento del danno

Tre concetti fondamentali sono:

1. Software Bug → sono gli errori che un software appena creato potrebbe avere → gli utenti inviano dei feedback e la casa manutrice li risolve nelle successive realizzazioni → più il tempo passa e più i bug diminuiscono

2. Vulnerabilità → studio del software in maniera diversa dal suo effettivo utilizzo in modo da portarlo in errore → l'obiettivo è trovare i punti deboli → andamento opposto dei bug, più passa il tempo e più la vulnerabilità aumenta → dovuto anche al fatto che la casa produttrice non lo controlla più (es. XP)

Bug e vulnerabilità potrebbero anche coincidere

3. Exploit → situazione in cui l'hacker prende il controllo della macchina tramite i sw bug o le vulnerabilità

Un esempio di presa del controllo tramite vulnerabilità è: creare un overflow del buffer, cioè inviare più informazioni di quelle che la macchina può ricevere → errore del sistema → potrebbe restituire il prompt

Advanced Persistent Threats (APT)

- Sono un'evoluzione dei malware
- Sono usati da hacker con un sofisticato livello di esperienza
- Obiettivi:
 - Raccolta dati
 - Impedimento degli aspetti critici di una missione, programma, o organizzazione (STUXNET)
 - Posizionamento dell'APT in una macchina, per poi utilizzarlo in un secondo momento

- Diversi attack vector → email fishing, usb, attacchi perimetrali
- Comportamento:
 - Perseguire i suoi obiettivi ripetutamente per un certo periodo di tempo (GAUSS)
 - Adattarsi agli sforzi difensivi per resistere
 - Determinazione a mantenere il livello di interazione necessaria per l'esecuzione dei suoi obiettivi

Comando e controllo:

Il Malware prende le informazioni, le impacchetta e le manda, ad esempio, caricandole su un dropsite. L'hacker, in maniera indisturbata, le scarica.

Perché è così difficile individuare il mandante?

Perché, per connettersi, utilizza un protocollo chiamato TOR che permette di nascondere dove effettuo l'accesso. Ad esempio compare che entro su quel sito dall'America, in verità sono in Russia.

Il governo americano (creatore di Tor) ha cercato di chiudere un sito, simile ad Amazon, dove veniva effettuato questo caricamento illegale. Un modo per scoprirli è di creare un sito fake, identico all'originale ma che contiene dei malware. Quando l'hacker entra, recupera i dati ma si porta dietro una minaccia. Appena si riconnetterà ad internet, verrà incastrato.

Fu attaccata anche la rete ESA (European Space Agency) [controlla le rampe di lancio e delle orbite dei satelliti] → il malware riuscì a superare il firewall esterno e il primo interno, infiltrandosi nella rete degli impiegati (enterprise network). Raggiunse la rete di emissione → fu trovato in una scheda SCADA che si occupava del controllo di un'orbita di un satellite.

Malicious Software Overview:

Malware (MALicious softWARE) → Sw creato per causare danni o per prendere risorse da un computer. Alcuni di essi sono parassiti che contengono dentro altro sw dannoso. Potrebbero autoreplicarsi e quindi propagarsi

Backdoor → sono porte remote lasciate aperte, ad esempio dalle aziende, per i programmati che aggiornano il sistema. Sono dei punti segreti di entrata → in Cina il governo ha voluto che tutti i computer avessero delle backdoors aperte, ufficialmente, per la sicurezza, uffiosamente, per avere il controllo di tutto il popolo

Logic Bomb → sono stati i primi ad essere creati → scoppiano in presenza di certe condizioni: apertura di specifici files, in giorni particolari, o quando entra in esecuzione un determinato programma

Cavalli di Troia → programmi utili che contengono codici nascosti che, quando richiamato svolge una funzione indesiderata o nociva. Può essere utilizzato per realizzare funzioni a cui un utente non ha normalmente accesso

Mobile Code → trasmesso da un sistema remoto a un sistema locale. Eseguito senza istruzioni di un utente specifico → un esempio tipico è il cross – site che attaccano siti web

I primi che si impegnarono nel campo della sicurezza, furono gli americani.

Nel 2013 gli Usa approvarono un decreto legge in cui tutte le aziende si dovevano impegnare a sottostare a degli standard sulla sicurezza. Tutto ciò è stato fatto perché, in questo momento, sono il Paese più attaccato.

Anche in Italia è stato fatto qualcosa di simile dal governo Monti.

La prima cosa da fare, quando si riceve un attacco, dovrebbe essere l'Information Sharing → ciò significherebbe informare i propri competitors → nei Paesi latini è un concetto molto difficile da diffondere.

In Italia è stato creato il CERN, un centro di controllo degli attacchi, che poi comunica i più pericolosi alle cariche superiori. Ancora, però, è molto disorganizzato e in più c'è poco investimento di soldi da parte del governo.