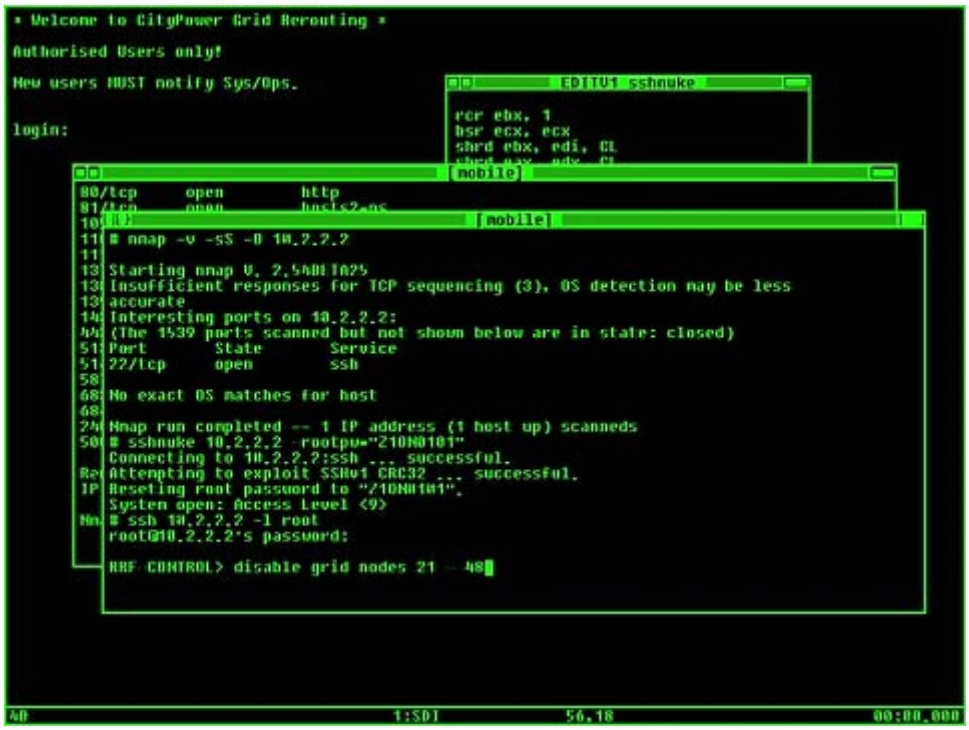
DIZIONARIO INFORMATICO SULLA SICUREZZA



Access point: o punti di accesso; generalmente costituiscono un'interfaccia tra reti wi-fi e reti Etherner; di norma sono costituiti da dispositivi eletronici che permettono l'accesso alla rete, a computer con tecnologia di connessione wi-fi.

ACL: Access Control List, o lista di controllo accesso, informazione relativa ad ogni utente, riportante i suoi permessi e i suoi privilegi nella modifica di files o impostazioni di sistema, su di essa si basa l'autentificazione utente nei sistemi NT.

ActiveX: componenti eseguibili, presenti nelle pagine web, questi possono essere usati come metodi di diffusione di codici maligni.

Adware: programmi molto simili agli spyware per tipologia di comportamento e danni arrecati alla privacy degli utenti, una differenza risiede nella loro presenza visibile su un sistema informatico, infatti generalmente crea finestre pubblicitarie. Un adware che spia e lede la privacy dell'utente viene definito in tutto e per tutto come spyware. Tali malware ha volte sono inclusi nelle versioni free di software a pagamento, in tal caso la pubblicità l'autorizza l'utente.

Algoritmo di crittografia: funzione matematica atta alla cifratura e decifratura di dati. Attualmente questi si servono di una chiave (K) per modificare i dati in uscita, secondo la seguente formula: $E_k(P) = C$ (processo di cifratura)

ove: E = funzione di cifratura (Encryption);

K = chiave;

P = dato o “testo in chiaro” (Plaintext);

C = dato cifrato (Cyphertext).

Cioè, la funzione E opera su P per ottenere come risultato il dato cifrato C. Il processo inverso alla cifratura, cioè la decifratura, avviene secondo la funzione inversa:

$D_k(C) = P$ e poiché entrambi i processi utilizzano la stessa chiave k, i due processi di cifratura e decifratura sono simmetrici.

Anonimyzer TOR: (o The Onion Router), software che offre l'accesso al servizio di navigazione sul web, in modo anonimo.

Application Layer: (Livello Applicazione) Nel protocollo TCP/IP costituisce il livello più alto della relativa architettura a strati, esso gestisce l'interfaccia macchina/utente: è in questo livello che l'utente richiama programmi che permettono di accedere ai servizi offerti da internet.
Quando un utente spedisce un messagio email, richiama il software atto a tale funzione, compila il messaggio, e nel momento in cui si comanda al software di spedire, il messaggio parte da questo livello (Application Layer) scende fino allo strato più basso (Network Interface Layer) e parte dal nostro hardware per essere trasportato sulla rete e arrivare quindi all'anologo livello del destinatario, fino a quando quest'ultimo non decide di leggerlo, e cioè lo fa risalire varso il livello più alto, appunto l'Application Layer

Attacco attivo: generalità di attacco avente come obiettivo la compromissione dell'integrità delle informazioni presenti sui sistemi informatici nonché il loro danneggiamento.

Attacco passivo: generalità di attacco informatico avente come scopo la compromissione della riservatezza e l'autenticazione di informazioni riservate e personali.

Autenticazione 802.1X: tipologia di autenticazione che permette la protezione delle reti Ethernet supportate da cablaggi e reti wireless 802.11. Per l'autenticazione e convalidazione degli utenti viene usato un server che concede

l'accesso alla rete. Se installata su reti wireless, supporta l'integrazione sia con chiavi WEP che WPA. Di norma è usata come protezione d'accesso per reti aziendali.

Backdoor: malware in grado di scansionare le prote aperte, alllo scopo di sfruttarle per creare un passaggio di informazioni dal sistema locale alla rete (malintenzionato)molte volte si sfruttano a tale scopo, falle dei sistemi operativi, attraverso queste i virus possono insidiarsi, infettando, il nostro sistema operativo; in linguaggio informatico,queste porte sul retro, sono particolari applicazioni che aprendo porte di comunicazione nella connessione, garantiscono l'accesso remoto (controllo a distanza del sistema infettato), queste applicazioni, una volta lanciato il trojan vengono installate in cartelle di sistema, garantendo così l'avvio automatico in background ad ogni avvio del sistema operativo e la irrintracciabilità dai software di protezione; Inizialmente questi software son stati creati allo scopo di risolvere eventuali problemi, su macchine molto distanti dalle zone di assistenza, garantendo appunto l'assistenza a distanza. Clasico è stato il caso Sony/BMG, che distribuivano una backdoor sui cd musicali nel 2005, attraerso questa porta il sistema contattava in background i server dell'azienda inviando nformazioni sull'uso della musica acquistata.

Le backdoors possono essere simmetriche o asimmetriche, le prime possono essere sfruttate da chiunque le individui, mentre le seconde permettono l'accesso solo da determinate postazioni.

Bastion host: in una particolare politica di progettazione di una rete privata, mirata a garantire alti standard di sicurezza informatica, viene usato un Bastion host, cioè una macchina in prima linea a difesa della rete privata; rappresenta l'unica macchina, in collegamento sia con la rete interna che con internet, dalla quale transista tutto il traffico tra reteLAN/Internet; come detto nella definizione dei dispositivi firewall, questo dispositivo deve essere affiancato da screen router, appositamente settato e configurato. Poiché in caso di attacco informatico proveniente da internet, questo bastion host, rappresenta la macchina (unica raggiungibile da internet), da oltrepassare per ottenere l'accesso alla rete privata, dovrà presentare le seguenti caratteristiche (prinicpali): Host livelli di protezione elevati; sistema operativo sicuro; assenza di software non strettamente necessario; disinstallazione dei compilatori; collegamento mediata da proxy server; numero ridotto al minimo dei servizi attivi; funzione di salvataggio automatico e controllo dei file di log; disattivazione del source routing; ecc.

Browser: software che permette l'accesso al servizio www (word wide web o accesso banche dati), in grado quindi di visionare le pagine web consentendo inoltre l'accesso ai loro contenuti.

Client: software usato dagli utenti per poter usuffruire dei servizi offerti dalla rete internet; la caratteristica che identifica queta tipologia di software, consiste nel rendere possibile la comunicazione (di sola richiesta) con un programma server, e questo rapporto è specifico; es. client mail, si collega al server per accedere al servizio di posta (SMTP/POP3); client broweser, si collega al servizio Web (HTTP); ecc.

Cookie: dati generalmente inviati da un Web server ad un browser client, con lo scopo di personalizzare (su l'utente) la pagina visitata, questi dati vengono memorizzati dal browser e di norma contengono informazini riguardandi le connessioni ad internet, i siti visitati, indirizzi IP, dati che possono mettere a rischio la nostra privacy. Il meccanismo di funzionamento generale dei web server, alle richieste dei client, consiste nelle seguenti fasi: il pogramma client si collega al web server (connesione web tipicamente *stateless*) e gli richiede la visualizzazione di una pagina, succssivamente il server web restituisce l'oggetto HTTP (pagina) al client, agiungendoci un'informazione di stato (*cookie*) che il client memorizza. Queste informazioni associate al coockie, presentano: nome del server, condizioni di attivazione, data scadenza, nome del coookie, valori specifici. I cookie vengono usati per i seguenti possibili usi: determinazione numero utenti con divisione tra utenti vecchi e nuovi; determinazione frequenza di collegamento al server web; raccolta dati privati relativi all'utente;

Crack: programma creato per annulare le restrizioni di software o dati coperti da Copyright, o più genericamente, software in grado di eludere i sistemi di protezione a difesa di dati; questo software viene progettato studiando i codici sorgenti delle protezioni, individuando all'interno di questi, i punti deboli e le porzioni di codice che apportano le restrizioni. L'iso del crack, ciòè l'azione del “crackare” non è legale, e la legge prevede sanzioni sia per chi lo genera, sia per chi lo diffonde sia per chi si serve, come reato di pirteria informatica. I crack, pertanto possono essere usati per annullare le limitazioni funzionali dei software in versione shareware, per eliminare le restrizioni temporali dei programmi in versione trial, e anche per eliminare le protezioni a difesa della copia immesse in cd-rom coperto da diritti d'autore. Tuttavia questi software hanno una larga diffusione e si trovano facilmente reperibili sul web e nelle reti P2P.

Crittografia: tecnica di cifratura che rende possibile impedire la lettura di dati a persone diverse dal destinatario, il quale dovrebbe essere l'unico in grado di decifrarli.

Cross Site Scripting: (XSS) bug di sicurezza, presente in siti web dinamici (home bancking) che possono permettere attività di hacking del sito stesso, attraverso l'introduzione ne sorgetnte della pagina web originale un frame che va a sovrapporsi al legittim, richiedendo nome utente e password di accesso al servizio di gestone conto corrente, dati che veranno protamente trasmessi non alla banca, ma al malintenzionato regalandogli l'accesso alle nostre risorse economiche.

DES: Algoritmo di crittografia a chiave segreta, definito come "decodificatore a blocchi di 64 bit " che codifica e decodifica i dati usando una chiave a 56 bit. Progettato neglia anni 70 ed adottato come standard dal Governo degli Stati Uniti. Tutt'oggi usato nell'ambito delle organizzazioni finanziarie, ma in continuo declino nel mondo delle agenzie governative a causa del suo punto debole incentrato sulla chiave a soli 56 bit, ormai vulnerabile dalle potenze di calcolo raggiunte. Tuttavia per la sua violazione si ha bisogno di risorse hardware difficilmente gestibili da piccole comunità o da utenti singoli, mentre risulta facilmente vulnerabile per i sistemi informatici in forza agli enti governativi, apparati militari e forze di polizia. Una sua variante, usata per rafforzare i livelli di sicurezza di tale algoritmo è il 3DES consistente nell'applicazione di 3 algoritmi DES (in serie) nella criptazione dei dati.

Dialer: tipologia di malware, capaci di dirottare le nostre connessioni verso numeri a pagamenti molto onerosi, molto diffusi nello standard di comunicazione analogico 56 kbps, i dialer normalmente arrivano sui nostri computer l'utente clikka volontariamente su banner pubblicitari che li ospitano.

Diffie Hellman: algoritmo di crittografia a chiave pubblica che basa la cifratura sulla difficoltà di problemi logaritmici, tale algoritmo riesce ad assicurare una certa sicurezza solo con chiavi di una certa lunghezza.

DNS: (Domain Name Server), è la funzione esplicata da alcuni computer collegati in rete (Internet) consistente nella traduzione dell'Host Name nel relativo IP Adress, e viceversa;

pertanto sono in grado di svolgere l'operazione *Reverse DNS*, cioè di risalire dall'IP (numerico) all'Host name di un sito.

Effetti virali: danni apportati dall'infezione da virus, alla parte software dei sistemi operativi (Compromissione funzionamento, crash di sistema, violazione privacy, furto e duplicazione dati personali, K.O. Sistema operativo, avvio applicazioni non richieste dall'utente).

E-mail harvesting: metodo usato dagli spammer per la raccolta di un'enorme quantità di indirizzi e-email; è reso possibile dall'utilizzo di particolari software in grado di setacciare, i codici HTML delle pagine web, in modo da recuperare gli indirizzi degli eventuali visitatori.

Exploit: script introdotto da un malintenzionato nel sistema del computer altrui, quindi attaccato, successivamente all'individuazione di una falla (bug) nella sua sicurezza, che permetterà la gestione del sistema.

Firewall: dispositivo software o hardware interposto fra il computer e la rete (e viceversa) a cui è connesso, in grado monitorizzare e filtrare i dati (pacchetti) in transito dalle porte di comunicazione con lo scopo di evitare l'accesso non autorizzato a pirati informatici.

E' usale indicare il firewall come *Bastion host*, (termine medievale indicante un particolare punto nella fortificazione di un castello). Vista l'architettura dei dati rice-trasmessi dal computer con la rete, anche i firewall, presentano molte

tipologie di architetture (firewall a livello rete, firewall a livello applicazone, firewall a livello di circuito), le soluzioni più funzionali, pertanto devo essere in grado di filtrare tutti i livelli dello stack TCP/IP partendo dallo *Screen Routing*.

Le loro limitazioni principali, da tener consapevolamente in considerazione, interessandoci alla sicurezza informatica, sono da attribuire a 3 fondamentali fattori:

Il dispositivo, non è in grado di garantire l'integrità dei dati (nelle normali soluzioni non è prevista la scansione antimalware dei pacchetti, ma si limita ad un'azione di filtraggio); incapacità di controllo sugli accessi fisici alla macchina; incapacità di autenticazione delle fonti (questi sono da garantire risolvendo i bug di sicurezza a livello di protocollo TCP/IP).

Firewall a livello applicazione (proxy): o comunente indicato come server proxy (o proxy semplicemente); questa tipologia prevede l'interposizione di questi server come interfaccia comunicativa tra due diverse reti; in una normale comunicazione configurata come client(interno)/server proxy/ server (esterno ed appartenete a rete differente del client) appare evidente come l'indirizzo IP con cui i server esterno intergisce, non identifica il client ma il proxy, pertanto questa configurazione può essere sfruttata come misura atta a garantire la privacy del client, attraverso una navigazione anonima sul web; da quanto detto, si deduce la netta divisione tra rete interna (client) e rete esterna (server), infatti ogni pacchetto costituente la comunicazione client/server, viene processato e inoltrato dal proxy, sia verso la rete interna sia verso la rete esterna; Tale tipologia di firewall opera a livello applicativo HTTP, FTP, SMTP, BOOTP, TFTP ecc, i quali possono essere abilitati, disabilitati o limitati.

Firewall a livello di circuiti: analogamente ai proxy, questa tipologia è sempre operante a livello applicazioni, ma il firewall proxy ha la funzione di creare il circuito di comunicazione tra client e server, in maniera oscura alle applicazioni: praticamente il proxy esamina ogni tipo di collegamento TCP a disposizion, instardando in seguito la comunicazione (handshake); il proxy crea quindi un elenco di collegamenti validi che usa per rendere possibile la comunicazione client/server, a cui fa riferimentodurante il collegamento, tale lista viene eliminata chiusura della connessione; tale tipologia si presenta molto vantaggiosa per la capacità di supportare svariati protocolli a livello applicativo, inoltre la gestione del server proxy risulta molto semplice; tuttavia fra gli svantaggi che tale tipologia concerne, si ha una scarsa efficienza di controllo sui pacchetti.

Firewall a livello rete: i genere questa tipologia è rappresentata da uno *sceen routing*, e come tale processa pacchetti provenienti dal livello data-link o dal livello rete IP; la capacità do controllo sugli IP, rende la funzionalità di questo dispositivo firewall subordinata alla creazione di una black list di IP da respingere; altre informazioni su cui èpossibile l'applicazione di filtri a questo livello sono: IP sorgente e destinatario, protocolli dati TCP, UDP, ICMP; e ralative porte di servizi; data e ora comunicazione;

Firma digitale: file di tipo EXE (esadeciamale), presente in tutti i vari tipi di files, che indica una sigla (stringhe) inequivocabile e specifica, atta ad individuare la tipologia (estensione) del file a cui si riferisce e da cui è contenuta, è possibile leggerla aprendo un qualsiasi file con il Block notes di Windows, oppure usando (metodo più preciso) un editor esadecimale, buona norma norma da attuare in caso di non sicura provenienza del file, infatti potrebbe aiutare a smascherare files eseguibili (magari virus) all'interno di files di sola lettura (audo, video, foto, ecc). Con l'ausiolio dell'editor esadecimae è possibile creare una firma digitale relativa all'utente da applicare a tutti files presenti nel sistema informatico e facilitarne le operazioni di ripristino o backup degli stessi. Molti virus hanno la capacità di modificare la firma digitale, ma gli antivirus, tra le rgole di scansione, presentano, la corrispondenza tra tipo di file e firma digitale, pertanto questa forma virale non ha avuto larga dffusione.

Foistware: programmi spia inclusi in altri software legittimi, questi malware costituiscono una parte essenziale del programma vero e proprio, pertanto la loro rimozione causa l'impossibiltià di utilizzodi quest'ultimo. Tuttavia nelle clausule di licenza dei software che le contengono devono essere, a norma di legge, mensionati. Uno dei tanti casi riguarda programma di file sharing “Kazaa”. Tale normativa in molti casi si è ritorta contro all'utenza, infatti basti pensare a quante volte ci capita di installare un software che presenta un contratto di licenza che va oltre le venti pagine e magari in lingue non conosciute.

Inoltre rimane sempre il problema della possibile intercettazione dei nostri dati trasmessi in rete.

Formattazione: tecnicamente rappresenta l'operazione che rende utilizzabile una memoria di massa, cioè che sia possibile la sua rilevazione e utilizzo da parte dei vari sistemi operativi; Più precisamente è la successione dei seguenti tre processi:

- Formattazione a basso livello: pre-formattazione;

- Partizionamento: divisione della memoria in volumi;

- Formattazione ad alto livello: creazione file system;

Formattazione a basso livello: processo di formattazione vero è proprio consistente nella creazione delle tracce e dei settori in una memoria di massa; processo detto anche di "pre-formattazione" perchè in passato spettava all'installatore dei pc tramite il bios della scheda madre o tramite particolari software; oggi le memorie di massa vengono vendute già preformattate e molte volte la loro struttura si presenta protetta verso eventuali mofìdificazioni; tale processo precede l'operazione di partizionamento.

Importante chiarire che la formattazione effettuata tramite i normali sistemi operativi non prevede la modificazione o la creazione di tracce e settori.

Formattazione ad alto livello: Ultima opreazione del processo di formattazione (in s.s.) che va ha creare il file system sul supporto di memorizzazione, cioè crea la struttura di riferimento, sulla quale ogni sistema opereativo si basa per la memorizzazione dei dati e la gestione dei volumi della memoria stessa. Costituisce il comune processo di formattazione è prevede la perdita dei dati memorizzati sul supporto. E' da tener presente che le strutture o meglio i file system con cui organizzare i nostri supporti di memorizzazione sono in funzione dei vari sistemi operativi utilizzati.

FTP Bounce: tecnica di attacco informatico consistente nell'uso improprio di un server piratato, il quale attraverso dei precisi comandi interni al protocollo FTP, imposti dal malintenzionato e salvati come file eseguibile sul server, dopo aver acpuisito l'accesso shell, attaccherà un'altro sistema, usando la connessione mediata dalla porta 21(porta FTP per servizio di trasmissione files); questa tipologia è stata sfruttata in quanto rende quasi impossibile risalire all'IP dell'individuo che ha pianificato e sferrato l'attacco, infatti l'IP da cui si originano i pacchetti con azione diretta sull'attacco, porteranno come indirizzo IP quello del server piratato (in gergo "*base*").

Gateway: punto di comunicazione tra reti locali differenti.

Ghost: stato in cui un utente normalmente collegato ad un canale IRC rimane virtualmente presente sul server ma realmente è disconnesso; tale situazione si verifica per cauese accidentali (disconnessioni improvvise) ed è una situazione momentanea, infatti dura il tempo necessario affinchè il server non ricevendo più imput da quel client lo rileva come inattivo e automaticamente lo disconnette cancellandolo dal canale.

Joe Job: tipologia di attacco prevedente l'inondazione di messaggi email sovraccaricando un server al fine di provocarne il crash, questa tipologia parte con l'invio di email con mittente fasullo, di norma l'inderizzo che l'email mostra come mittente è la vittima dell'attacco, queste email inviate tipo spam, presentano contenuti molto accattivanti (hard in genere) o offerte commerciali molto convenienti, in modo da indurre chi legge la mail a rispondere, partecipando così attivamente al sabotaggio del server di posta;

Keylogger: programma in grado di registrare su file ogni digitazione effettuata sulla tastiera del computer, rapporto spedito poi al malintenzionato, attraverso il nostro account mail. Un keylogger può presentarsi anche come supporto fisico che si inserisce tra unità centrale e tastiera. Il loro uso è mirato di norma all'acquisizione di nome utente e password.

Hash: codice di identificazione inequivocabile ed univoco, di un qualsiasi files presente du un computer, riportandone data e ora di creazione, modificazione ecc. di fondamentale importanza nel campo dell'investigazione del crimine informatico, in quanto va a rendere valida una qualsiasi prova (files modificato o residuo da attacco informatico) presente su un sistema; senza di esso la prova non può essere ritenuta valida in ambiente legale.

Hashing: tecnica, usata nella computer forensis, mirata allo rendere valida (legalmente) una prova informatica, attraverso il calcolo dell'hash della prova (file).

Hijacker: malware capace, una volta attivato, di gestire il pieno controllo del browser, agendo sulle impostazioni di sistema, con lo scopo di pilotarne la navigazione internet, dirottando le pagine richieste (o la pagina iniziale) su siti di convenienza e da cui il programmatore che lo sviluppa, lucra; la sua diffusione è mediata solitamente da trojan, come è possibile dedurre, ha fini di marketing nella migliore delle ipotesi, tuttavia non è da escludersi la il possibile dirottamento verso siti di cui le pagine contengono script maligni, qundi questi software possono essere usati per pianificare attacchi più consistente su scala internet. Molti sosno stati i casi in cui questi malware hanno bloccato l'accesso a determinate pagine web (siti di case produttrici di antivirus e simili) o hanno disattivato le protezioni antispyware in modo da non essere rilevati. In altri casi, più aggrssivi, veniva sfruttata la capacità di Internet Explorer di eseguire automaticamente script ActiveX da pagine web.

Di norma la loro installazione è mediata dal consenso ignaro dell'utente, ma ci sono stati casi in cui si sfruttava dei bug nelle misure di sicurezza dei vari browser.

Alcuni hijacker, hanno la capacità di accedere nel file HOST del sistema, manomettendo a loro favore l'associazione degli indirizzi DNS con i rispettivi indirizzi IP in modo, che se l'utente inserisca un URL di un qualsiasi sito, nel browser questo comunque andrà a dirottarne la navigazione sulla pagina preimpostata dal malware.

Un indizio della presenza di un tale malware nel nostro sistema può essere la modifica non voluta dall'utente della pagina iniziale, la quale anche se reimpostata dall'utente, sarà sempre dirottata e modificata dal software maligno. Generalmente vengono diffusi attraverso le barre degli strumenti con cui è possibile integrare i browser. Oltre al danno arrecato al sistema, possono rendere fastidiosissima la nostra navigazione se non impossibile, infatti alcuni hijacker dirottano la navigazione verso centinaia di finestre pubblicitarie che molte volte non presentano neanche il comando di chiusura o magari chiudendone ne apriamo delle altre.

Hoax: (burla) false notizie diffuse tramite i servizi di posta elettronica, informanti i destinatari della presenza di virus particolarmente virulenti e non rilevabili dai software di protezione, riportandone il nome e la loro normale allocazione all'interno delle cartelle del sistema operativo, con le istruzioni per procedere alla rimozione manule del virus, il più delle volte il file eliminato era però un essenziale file di sistema, rendendo così la sua rimozione molto rischiosa per la stabilità del sistema stesso.

Host Name: nome in formato standard che identifica un sito, di norma è completato da un'estensione che rappresenta la natura del sito quali: .com (commerciale); .org(organizzazione); .mil (militare); .it (italiano); .uk (inglese);

Hub/switch: dispositivi hardware atti alla gestione e smistamento dei pacchetti nelle reti Lan, infatti consentono il collegamento di computer, stampanti, e qualsiasi altro dispositivo in grado di comunicare con connessioni Ethernet.

IANA: International Assigned Numbers Authority, organismo che gestisce gli indirizzi IP, assegnandoli in base alla locazione geografica; gli IP vengono associati a blocchi geografici gestiti dai RIR;

ICT o Information and Comunication Tachnology: tecnologia della comunicazione e dell'informazione.

IDEA: (International Data Encryption Algorithm)algoritmo di crittografia a chiave segreta progettato dalla ETH Zurich (Svizzera) nel 1990, si basa su una chiave a 128 bit, assicurando tuttora un livello di sicurezza molto buono, infatti è tra i più diffusi algoritmi chiave segreta. A suo favore va la non conoscenza di attacchi che hanno portato alla sua violazione.

Internet Layer: livello che nell'architettura a striti del protocollo TCP/IP si interpone tra il Lransport Layer e Network Interface Layer; ha il compito di gestire la comunicazione tra diverse macchine localizzate sulla stessa rete, esso trasmette e riceve i pacchetti da e verso le altre macchine, attraverso richieste e accettazioni di richieste di dati. Tale livello non è in grado di garantire sicurezza sull'avvenuta ricezione dei dati trasmessi. Rappresenta inoltre il livello peculiare della rete Internet da cui il nome Internet Protocol (IP). Sostanzialmente esso ricee i pacchietti TCP provenienti da livello sovrastante (Transport Layer), li suddivide ancora (incapsula), svolge gli header e attraverso gli algoritmi di routing inoltra i pacchetti al destinatario (Trasmissione). E' a questo livello che si svolge l'instradamento vero e prorpio dei pacchetti e se ne controlla la validità.

IP (indirizzo): (Internet Address o IP Address) indirizzo reale nel web che identifica un qualsiasi host (computer connesso) sulla rete, oltre a siti, pagine web ecc. Un IP Adress identifica pertanto in modo univoco un Host Name. Si presenta come una sequenza (binaria a 32 bit) di 4 numeri a tre cifre comprese nell'intervallo 0-255, spaziati da 4 punti (Dotted Decimal Notation) del tipo 200.222.13.2, (il nome del sito è solo un modo più mnemonico per identificarlo); le quattro cifre identificano la zona geografica di residenza dell'indirizzo, e vengono assegnate da un solo organismo detto IANA. In sostanza esso serve come identificatore universale. Pertanto ogni indirizzo IP è una coppia netid-hostid, ove netid rappresenta la rete di connessione e l'hostid identifica quel computer su quella rete.

IRC: Internet Relay Chat, software che permette la comunicazione in tempo reale (Chat) e lo scambio di files.

ISP: Internet Service Provider, fornitore del servizio internet;

IT o Information Technology: Tecnologia dell'informazione; tecnologia su cui si basano i computer allo scopo di creare, memorizzare, gestire e processare l'informazione.

Logic Bomb: malware creato appositamente per sabotare un sistema, la sua peculiarità consiste nella capacità di rimanere inattivo fino al momento in cui si desidera scatenare l'attacco, tale momento può essere impostato in base cronologica ecc.

LSA: Local Security Authority, conosciuto anche come Security Subsystem, rappresenta il componente centrale della sicurezza nei sistemi microsoft NT, ed atto a svolgere la funzione di autentificazione degli utenti (logging).

Netiquette: insieme di regole morali e comportamenti sviluppati dalla comunità internet con lo scopo di rendere pacifica la convivenza mondiale sul web, sostanzialmente costituisce il galateo di internet.

Network Interface Layer: Tra gli strati dell'architettura del protocollo PCP/IP, rappresenta il livello più basso, sottostante cioè al Internt Layer; è rappresentato dall'interfaccia di rete alla quale vengono trasmessi i pacchetti in uscita (o in entrata) provenienti (o diretti) dal (o al) livello superiore. In questo livello i pacchetti vengono inglobati in peculiari frame e inoltrati sul supporto di rete (cavo, ecc.) cioè spediti all'altra macchina.

Macrovirus: o anche virus da macro, sono pericolosi codici, in grado di attaccare solo alcuni tipologie di files, (documenti word, excel ecc.) sfruttano l'uso anomalo di funzioni messi a disposizione dai relativi editor (macro) per permettere di agevolare l'esecuzione di azioni ripetitive, questi virus, oggi poco diffusi, hanno costituito in passato, il passaggio dai virus da eseguibile, ai virus da documenti, abbattendo la teoria secondo l'infezione da virus potesse avvenire solo nel caso in cui il codice maligno risiedesse in un file eseguibile.

Malware: termine usato per individuare la categoria di software maligni o virus.

Master Boot Record: settore del HD contenente le informazioni primarie necessarie all'avvio del sistema.

Owned: normalmente consite nel messagio che un pirata informati, successivamente all'attacco di un sisto web, lascia sulla home page, come firma personale o per spiegare le motivazioni che hanno indotto l'attacco.

Partizionamento: operazione intercalata tra la pre-formattazione e la creazione del file system, consiste nella divisione del supporto di memorizzazione in volumi logici. Il supporto può essere diviso in una sola partizione (primaria “C”) o in più volumi (1 primaria più le altre), in tal caso le partizioni verranno identificate con lettere diverse. Le informazioni sulle diverse partizione presenti sulla memoria vengono memorizzate nel MBR (master boot recod) primo settore del supporto.

Password: parola o comunque stringa chiave, rappresentata da un codice identificativo personale e segreto, usata per proteggere e regolare l'accesso a connessioni, dati o sistemi sensibili o comunque privati.

Payload: alla lettera “carico consegnato”, nel gergo tecnico sta a rappresentare il programma che un worm deposita sul sistema locale e che usano per la diffusione; in certi casi questo programmino può eliminare modificare e ultimamente criptare files, in modo da richiedere un riscatto all'utente.

Worm molto particolari sono stati il “Sobing”, “Mydoom” e “Sasser”, questi con portavano in carico una backdoor, in modo da dare i controllo della macchina infettata, al creatore del worm, molti sono stati i casi di reti messe in ginocchio e trasformate in “botnet”.

PGP: (Pretty Good Privacy) algoritmo di cifratura a chiave pubblica che vanta una larga diffusione in parte dovuta alla sua distribuzione come pacchetto freeware; tale algoritmo riesce a garantire sicurezza, autnticità e integrita dei dati, anche su canali comunicativi privi di livelli di sicurezza accettabili; le caratteristiche che esso riesce ad offrire troviamo la capacità di gestione delle chiavi, sia pubbliche che private, accettazione di chiavi a diversa lunghezza, certificazione delle chiavi e autenticazione degli utenti che interscambiano i file.

Phisher: colui che attua attacchi di phishing.

Phishing: tecnica e metodologia di truffa informatica (basata sull'ingegneria sociale), atta al furto di dati segreti, in genere bancari (dati di accesso alla gestione dei conto correnti), facendo in modo che l'utente venga ingannato attraverso l'uso di siti clonati (falsi, e con URL diverso dal sito legittimo) e pagine controllate dal phisher, oppure l'invio di messaggi di posta clonati sulla base di email leggittime che vengono inviate all'utente, a nome di società bancarie, inviatandolo con dialettica professionale, a fornire nome utente e password di accesso alla gestione dei propri conti correnti. Gli attacchi di norma si consumano a carico di società bancarie, postali o siti di shopping on line.

Ping: software in grado di identificare la presenza di un computer (o sito) sulla rete fornendo inoltre informazioni sulla velocità dell'eventuale connessione stabilita.

Port Scanning: azione svolta di norma, in pre attacco di omologo tipo, in questa fase si pianifica un eventuale attacco e questa scansione porta all'indiduazione di porte recettive sul computer vittima connesso in rete.

Port scanning SYN-TCP: scansione riguardante porte TCP, le quali vengono interrogate con pacchetti SYN in modo da stabilirne una connessione, questa tecnica molto complessa può rendersi quasi invisibile.

Port scanning TCP: scansione mirata alle porte del protocollo TCP, l'nterrogazione avviene inviando pacchetti alle porte (determinate), con lo scopo di stabilire una connessione stabile fra i computer attaccante/vittima. (metodologia largamente usata).

Port scanning TCP a frammentazione: tecnica simile al port scanning TCP (comune scansione), differente per la grandezza dei pacchetti inviati, infatti in questo caso l'Header TCP risulta frammentato, quindi non intercettabile dagli eventuali filtri o sistemi di protezione.

Port scanning TCP-FIN: questa metodologia di scansione delle porte TCP si basa sul funzionamento delle porte, relativo all'interrogazione con pacchetti FIN ed è sempre mirata all'identificazione delle porte recettive.

Port scanning UDP-ICMP: scansione delle porte basate sul protocollo UDP; l'identificazione delle porte recettive in questo caso avviene per esclusione, in quanto le porte UDP rispondo solo se non recettive, pertanto interrogando una porta disponibile alla connessione, non si avrà risposta.

Port surfing: azione consistente nel cercare, attraverso un collegamento via telnet, alle porte dei server, via d'accesso non controllate o informazioni utili.

Principio di Kerckhoffs: “ La sicurezza di un sistema crittograco non deve dipendere dalla segretezza dell'algoritmo usato, ma solo dalla segretezza della chiave”.

Prof-thief: pirata informatio specializato nel furto su commissione di dati sensibili, attività che svolge come lavoro e quindi a scopi di guadagno.

Propagazione dal settore di avvio: meccanica di diffusione di un virus, molto pericolosa, prevedente il caricamento del virus 8virus di avvio), in memoria, precedente l'avvio del sistema operativo e quindi anche dei software antivirus; situazione posta in essere quando il virus ha la capacità di infettare il Mater Boot record, rendendosì così irremovibile

dai software di difesa; infatti, avvalendosi della priorità sul sitema operativo, inganna, le funzioni API; questi virus possono anche indurre una formattazione automatica del disco rigido.

Propagazione parassitaria: meccanica di diffusione di un virus prevedente, la clonazione del codice maligno, all'interno di altri file eseguibili, nel momento di avvio dell'applicazione che lo ospita;

Protocollo: insieme di regole da seguire per la gestione di servizi offerti da internet, quali Web, email, ecc.

Protocollo MIME: (Multi-purprose Internet mail Extension).

Ransoware: particolari virus moderni, ricattanti, che in seguito all'infezione di un computer, bloccano con l'ausiolio di potenti algoritmi di crittografia, l'accesso a documenti all'utente, il quale viene costertto a pagare una certa cifra di denaro per poter recuperare i dati di sua proprietà, sono tra i malware più spietati, e tutt'oggi in continua evoluzione e diffusione.

RC4: algoritmo di crittografia progettato dalla RSA Data Security Inc. protetto per molto tempo dal segreto commerciale, è tra gli algoritmi a chiave segreta, quello che assicura un alto livello di sicurezza; la sua peculiarità sta nella capacità di accettare chiavidi cifratura a lunghezza variabile, infatti viene definito come “una generatore di numeri (chiavi) pseudo-casuali” usati poi nello XOR con il flusso dati.

Registro di sistema: registro nel quale sono memorizzate le impostazioni del sistema operativo e relative ai suoi rapporti con i componenti e periferiche hardware installate, il registro di windos è diviso in 5 categorie gerarchiche (ad albero): HKCR HKCU, HKLM, HKU e HKCC, cioè: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USER e HKEY_CURRENT_CONFIG; queste categoie suddividono quindi le informazioni registrate cioè le *chiavi di registro* (suudivise in più file, catalogati in base alle aree di competenza). Appare ovvia a quanto detto, l'importanza della sua integrità sia a fini di normale e ottimale funzionamento software, sia per quanto riguarda la sicurezza del computer, infatti sono moltissimi i virus che mirano alla sua modifica. Non è possibile identificarne tuttavia una posizione fisica sul disco, anche se la maggior parte dei suoi valori, (impostazioni) sono salvati nella cartella di Windows\System 32\Config.

RIR: Regional Internet Registry, o registri intenrnet regionali (relativi ai blocchi geografici) sono solo 5 a rappresentare appunto le regioni internet, quali:

AFRNIC: identifica l'Africa; *ARIN*: Nord America e Asia Settentrionale; *APNIC:* regione del Pacifico; *LAPNIC:* America Latina; *RIPE NCC:* Europa e Asia;

RSA: (Rivest Shamir-Adelmen) più comune algoritmi di cifratura a chiave pubblica, atto sia all'impiego di cifratura dati che per le firme digitali, il livello di sicurezza che garantisce è direttamente proporzionale alla lunghezza delle chivi, raggiungendo standard molto alti con chiavi a 1024 bit, il suo punto forte sta nella difficile fattorizzazione di numeri interi molto grandi.

RootKit: software malware atti all'introduzione, quindi alla diffusione, di spyware nei sistemi informatici apportando modifiche alle funzioni di sistema, le quali rallentano o fornirniscono risposte falsate, agli input dettati dall'utente; per questa loro capacità superano molte volte indenni i controlli di sicurezza, inoltre si rendono anche invisibili a software di gestione dei processi quali Task manager, process explorer ecc; per la loro rimozione servono dei tool specifici, di solito forniti dalle case produttrici di software antivirus.

Router: dispositivi di collegamento di reti, generlamente rappresentate da interfacce hardaware (ma possono essere anche di natura software) che consentono la connessione di reti Lan a reti di vasta scala (geografiche o Internet). Oggi i router per reti ADSL incorporano, modem per accesso a Internet e funzionalità di access point.

SAM: Security Account Manager, o manager di sicurezza degli account, è un'impostazione presente nel registro di sistema, che fornisce l'autenticazione al LSA e controlla gli accoutn catalogati per gruppi di utenti.

Scarewar: software malware, con sviluppo codice sorgente e programmazione, analoga agli spyware, la sua innovazione consiste nel mirare ad attaccare la parte psichica dell'utente, usando come mezzo di attacco, il pc infetto che lo ospita; la sua azione è sviluppata in modo da convincere l'utente di trovarsi in condizioni di imminente attacco

hacker, per irrilevanti misure di sicurezza installati nel pc, (con l'ausilio di riproduzione automatica e casuale di video o suoni di sistema angoscianti) inducendolo dunque in stato d'ansia che molto probabilmente lo porterà all'acquisto di una suite di sicurezza; è molto esplita la sua natura commerciale.

Screen routing: rappresenta il primo livello dello stack TCP/IP, di un dispositivo firewall; questo, prevede il funzionamento del firewall solo a livello data-link e rete, pertanto l'azione di filtraggio è basata essenzialmente in base a: numeri di porta, indirizzi IP, e flag TCP; tuttavia questo livello non è atto all'auditing, quindi a fini protezionisti, bisogna aggiungere dei filtri lavoranti a livello rete e a livello applicativo, sempre relativi allo stack TCP/IP.

Script: definisce il linguaggio di programmazione di una qualsiasi applicazione, è usato per eseguire automaticamente istruzioni all'inteno di un programma, per queste capacità posso essere usate per indurre l'esecuzione di codici maligni, comune è il caso in cui vengono contenuti all'interno del codice sorgente di pagine web, con lo scopo di arrecare danni ai visitatori, sfruttando per il loro fine, bug di sicurezza presenti nei browser.

Server: software atto all'offerta di servizi internet, a differenza dei programmi client esso mette a disposizione le prorpie risorse a chi li richiede (client), es: Web server, offrono agli utenti della rete il servizio di collegamento alla rete (internet); altra tipologia di software con funzioni server è rappresentata dai programmi peer to peer, i queli mettono a disposizione i files condivisi dall'utente.

Server Mixer: software (analoghi ai privoxy) che consentono la nagigazione anonima, grazie all'uso di algoritmi di gestione delle connessioni ad un server, che esplicano una funzione di mixaggio, instradando i pacchetti attraverso un identificazione resa possibile da algoritmi di cifratura, l'azione di criptaggio si basa su variabili dettate dalla posizione del computer nella rete, cosicchè, i computer collegati e mixati, possono decriptare i pacchetti basandosi sul posto occupato nella rete, e quindi in grado di legggere solo i dati criptati in base alle relative posizioni.

Servizi: risorse offerte da internet, quali: Web (visualizzazione pagine ipertestuali), FTP (trasmissione dati), email (posta elettronica), ecc. servizi comunque ragolati dai relativi protocolli, es. HTTP (protocollo per il web), SMTP (invio email), POP3 (ricezione email), IMAP (email, in ricezione, meno usato del POP3); ogni servizio, inoltre comunica con il client,attraverso determinate porte.

Sicurezza informatica: insieme di quelle tecniche e tecnologie usate per proteggere i dati e le impostazioni memorizzati su un computer, in modo da non essere violati, letti o modificati da terze persone non autorizzate.

Slack space: buchi nel file system, o meglio spazi rimasti vuoti, dentro il nostro disco rigido, in essi non sono presenti dati salvati, inoltre sono dispersi sul supporto in maniera casuale; questi cluster non usati, perchè non previsti dal file system, quindi non rilevabili, possono essere usati per riporvi i sorgenti di virus informatici in modocompletamente invisibile al sistema operativo. Comunque possono essere anche usati dagli utenti come luogo sicuro per riporvi dati sensibil, come password e altro.

Social engineering: Ingegneria sociale, da molti definito come il metodo più facile per l'acquisizione di informazioni riservate, essa studia l'architettura delle classi sociali focalizzandosi sui rapporti interpersonali e i comportamenti che ogni individui è condotto spontaneamente a fere nelle più svariate situazioni. Studiando quindi il comportamento delle persone, all'interno di particolari realtà sociali, è possibile prevederne la reazione con cui gli individui rispondo alle varie esigenze. Oggi su di essa si sviluppano oltre che progetti di marketing, particolari attacchi informatici, tra cui il phishing, ecc.

Es. invio richiesta di dati utili tramite email (scritta) telefono (voce) o fax, con particolare cura della forma e della dialettica professionale usata, al fine di indurre tranquillità e fiducia nel malcapitato di cui si vorrà violare la privacy, il quale crederà di interlocuiare o comunicare con persone serie e qualificate, con lo scopo di migliorgli il servizio (apparentemente).

Spyware: o programmi spia, semplici software malware, progettati con lo scopo di ricavare il maggior numero di dati sensibili relativi all'utente del computere infettato, adempiono il loro compito tracciando i siti web visitati, e i servizi internet usati, hanno scopo statistico a fini commerciali, la loro diffusione di norma è mediata da trojan o altri virus informatici, oppure distribuito come utility o addirittura come protezione antispyware.

SRM: Security Reference Monitor, controlla (negando o meno) l'accesso ai files o directory da parte dei vari utenti, fornendogli, in base alla precedente autenticazione, i privilegi previsti per quella tipologia di account, inoltre informa LSA dell'eventuali violazioni on messaggi di audit.

TCP/IP: protocollo di regole semplici che rendono possibile una libera comunicazione tra vari terminali e in vari ambienti (Lan, Internet); nato nel 1969, e a quel tempo non prevedeva requisiti per garantire la sicurezza delle trasmissioni (autenticazione, integrità e privacy), fu per sopperire a questa deficienza che si dovettero creare i dispositivi firewall.

TCP/IP-based attack: insieme, delle potenziali tipologie di attacchi informatici, resi possibili, quindi basati su bug di sicurezza del protocollo TCP/IP.

Tipologie virus: sostanzialmente due sono le tipologie di virus più diffuse: Virus che si insidiano in testa a programmi eseguibili, qui aggunngono le istruzioni che inducono un salto in coda, dove ripongono il loro codice sorgente vero e prorprio e l'istruzione di ritorno alla pima istruzione del programma leggittimo, non modificando quindi l'integrità del programma originale (metodo in disuso in quanto facilmente rintraccibile dagli antivirus); Virus che si diffondono attraverso pagine web o allegati mail, questa tipologia richiede il nostro involontario consenso, o sfutta falle del browser in grado di eseguire il codice automaticamente.

Transport Layer: (Livello trasporto): Nello stack dell'architettura a strati del protocllo TCP/IP, rappresenta il secondo livello subito dopo l'application layer. Essenzialmente la sua funzione è quella di permettere la comunicazione in rete fra due utenti (comunicazione “and to and”). E' a questo livello che i nostri dati trasmessi vengono divisi in pacchetti di circa 500 byte e associati all'indirizzo IP di destinazione, per poter passare al livello sottostante cioè Internet Layer; a tele livello inoltre, vengono specificate le porte di transito dati e specificato il programma che né ha richiesto la ricezione o trasmissione, (tale livello è in grado di accettare richieste da più utenti).

Trojan horse: o semplicemente trojan, software nocivi (malware), apparentemente inoffensivi contenenti backdoor, in mod da consentire l'accesso remoto al sisema attaccato.

Di norma, affinchè un trojan possa avviare la sua azione ha bisogno del consenso ignaro dell'utente, per questo motivo, questi malware vengono spesso inseriti in altri software utility, o condividendo software crackati (è addizionati di trojan) sulle reti P2P.

L'architettura semplice di un trojan, prevede la presenza di due elementi principali, il “server” e il “client”, il primo serve per effettuare l'infezione (in s.s.) il secondo è una semplice applicazione che permette la connessione al computer da parte dell'intruso. Una volta installato un trojan su un computer, il malintenzionato intrusore invia pacchetti di richiesta all'utente (nella stragrande maggioranza dei casi “agli utenti infetti”), interrogando la parte server del trojan, con il client, instaurando così un collegamento client-server diretto. Instaurato il collegamento, il controllo effettivo della macchina passa dall'utente al pirata informatico, e poiché tale connessione è stata voluta dall'utente stesso (nel momento delll'installazione del trojan), può riprendere il controllo del sistema in un solo modo ciòè attraverso la disconnessione dalla rete.

L'unico indizio dell'attività sospetta e quindi della presenza di un trojan, è cercare di monitorare il funzionamento del disco rigido, infatti se durante una normale sessione di lavoro al nostro pc, notiamo che l'hard disk gira costantemente alla max velocità, probabilmente qualche applicazione richiede la lettura o la scrittura su di esso, e se non siamo noi a richiederlo, chi sarà?

URL: acronimo di Uniform Resource Locator, esso definisce l'indirizzo sul Web.

UAP: acronimo di User Account Protection, è la tecnologia usata da Windows Vista, allo scopo di proteggere dalle violazioni degli account, si basa sostanzialmente nell'utilizzo di nome utente e password di amministartore, per permettere l'accesso e la modifica, di quelle zone di sistema, più delicate quali i files di sistema, registro ecc.

Virus: piccolo programma che si insidia in un altro programma ospite,avendo come obiettivo primario la sua duplicazione e diffusione, potenzialmente in grado di danneggiare i sistemi informatici infetti (tuttavia rarissimi sono stati i casi di virus in grado di apportare danni hardware, in passato si ebbe qualche virus in grado di apportare modifiche alle frequenze per la trasmissione segnali visivi al monitor, con lo scopo di rovinarlo oppure inducendo manovre errate alle testine di lettura HD in modo violento, manomettendone la sua integrità. Tecnicamente un virus è una qualsiasi porzione di codice che si aggiunge al codice sorgente di un altro programma al fine di dupliarsi e diffondersi. Attualmente è difficile catalogare questa grande famigli di malware, tuttavia è possibile una prima suddivisone in virus residenti e virus non residenti (in base alla tipologia comportamentale al momento dell'esecuzione).

Virus mutanti o polimorfoci: virus informatici frutto delle nuove tecnologie informatiche, questi, sfruttando complessi algoritmi sono in grado di ricodificarsi ad ogni duplicazione, con lo scopo di non essere rintracciabili (detti anche Stealth) e registrati nei database dei programmi antivirus.

Virus non residenti: tipologia di virus che al momento dell'esecuzione iniziano immediatamente la ricerca di files ospiti da infettare, li infettano e trasferiscono il controllo all'applicazione infettata. Per far ciò sono provvisti di un modulo di ricera e un modulo di replicazione, il primo esplica l'azione della ricerca dei files da infettare, ogni volta che la ricerca va a buon fine, ordina al modulo di replicazione di infettare quel file.

Per rendere più comprensibile questa tipologia comportamentale, passiamo a dettaglio le azioni che un virus non residente, esegue nel suo attacco dopo aver individuato il file da infettare, cioè le azioni svolte dal modulo di replicazione:

- Accesso al file aprendolo;

- Controllo dell'eventuale già prsenza del codice virale (in tal caso termina tutta l'operazione);

- Applicazione del codice virale al file .exe;

- Impostazione del punto di partenza dell'eseguibile modificandolo in modo che all'esecuzione del file, venga eseguito il codice virale e salvataggio;

- salvataggio della posizione iniziale del virus in modo che subito dopo l'esecuzione questo ritorni al suo posto;

- Salvataggio delle modifche apportate a tutto l'eseguibile;

- Chiusura file infetto e riavvio del modulo di ricerca.

Virus residenti: tale tipologia racchiude in sé tutti quei virus che vengono caricati in memoria solo al momento della loro esecuzione trasferendo il controllo all'applicazione che lo ospita; al contrario dei virus non residenti, avviata l'esecuzione, non cercano altri file ospiti, essi infatti rimangono sempre attivi e si duplicano in altri file quando questi vengono aperti dalle varie applicazioni ed in certi casi anche dal sistema operativo stesso, successivamente però all'apertura di un file già infetto. Detto in parole molto povere il virus viene caricato in memoria con l'apertura di un file infetto, questo risiede quindi sulla ram, e infetta i file targhet che successivamente vengono caricati su di essa. Anche questi virus contengono quindi un modulo di replicazione, ma al contrario dei virus non residenti, non viene richiameto dal modulo di ricera; Il sudetto modulo di replicazione, viene caricato in memoria solo apertura di un file infetto. Per questa caratteristica, questi virus tendono ad infettare i file di sistema in modo che essi vengano caricati all'avvio del sistema operativo. I virus non residenti tuttavia possono essere ancora suddivisi in base all'aggressività della loro azione infettiva in, virus residenti ad infezione lenta e ad infezione rapida.

Virus residenti ad infezione lenta: virus residenti aventi come targhet la non individuazione da parte dei software di protezione, questi infatti si replicano in modo molto lento e selettivo, cosicchè l'attività virale, ridotta al minimo, non richiami l'attenzione né dell'utente né dei sopracitati software. Tali virus di norma non infettano in modo apprezzabile le applicazioni, ipertanto non apportano né rallentamenti al sistema, né comportamenti anomali durante l'esecuzione delle applicazioni infettate.

Tuttavia tale tipologia non ha mai avuto larga diffusione.

Virus residenti ad infezione rapida: tipologia di virus che hanno come scopo l'infezione di più files possibili. Questi virus, nei casi in cui il sistema non è adeguatamente protetto e aggiornato, possono causare seri problemi, anche a carico dell'antivirus, infatti, questi sono in grado di usare i software di protezione come veicolo di diffusione, ciòè se il virus non viene rilevato prima che venga caricato in memoria, appena viene effettuata la scansione del sistema, cioè l'applicazione antivirus accede a tutti i files, il codice maligno si duplica in ogni files (attaccabile dal virus) che l'antivirus scansiona, con un'azione a “rimorchio”.

Come si può notare, lo scompiglio causato da un virus ad infezione rapida è molto notabile, e di norma questi hanno una vita relativamente corta, il tempo necessario per aggiornare il data base di riferimento del software di protezione. E' comune inoltre che tali virus prevedono misure di crash per le applicazioni antivirus o blocchi a carico delle procedure di aggiornamento delle protezioni.

WEP: o Wired Equivalent Privacy, metodo di protezione delle reti basato sull'autenticazione mediata da una chiave di rete che crittografa le informazioni trasmesse.

Wireless: o assenza di fili, tecnologia che permette la trasmissione e ricezione dati (pacchetti), basata sulla trasmissione di onde sonore (microonde) , quindi senza l'ausilio di supporti fisici quali cavi rameici o fibbre ottiche.

Worm: (definiti anche parassiti della rete)Virus di nuova generazione, che hanno rimpiazzato i classici virus, predisposto per la propagazione via internet o email(capacità di diffusione altissime), non si autoreplicano su sitemi locali ma usano la rete per inviare i loro cloni (consumando la banda), capaci di mimetizzarsi in altri programmi, che usano per diffordersi con il massimo della tempestività, col fine di aprire backdoor nel firewall, regalando al loro programmatore il dominio dei sistemi infetti, con accesso alle informazioni riservate; Una volta attivati essi si diffondono usando i sistemi di posta elettronica o direttamente tramite SMTP; Tuttavia sono programmi completi che non necessitano di collegarsi a software presenti; metodo usato per l'ottenimento dei dati è l'uso di keylogging.

Uno dei modi in grado di rilevare la presenza di un worm nel nostro sitema è il monitoraggio della rete locale, infatti appena il worm si attiva inzia a interrogare indirizzi a noi sconosciuti o non richiesti.

Il primo worm che disseminò panico nelle reti moderne fu “Melissa” (nome di una ballerina di lap dance conosciuta dal creatore del worm Kwyjibo), individuato il 26 marzo del 1999, questo bloccava, intasando con email infette, i sistemi di posta elettronica;

Il nome “worm” prende origine da un romanzo fantascientifico: “The Shockwave Rider”, di John Brunner nel 1975, in seguito fu introdotto nel campo informaticoda un gruppo di ricercatori di Xerox PARC nel documento del 1982 “The Worm Programs”.

WPA: o Wi-Fi Protected Access, protezione creata per eti Wi-Fi come aggiunta all'autenticazione WEP. Oltre a crittografare i dati esegue un controllo sulla chiave di rete in modo da analizzarne l'integrità terminando con l'autenticazione degli utent, in modo che solo l'effettivo destinatario sia in grado di dedodificare le informazioni trasmesse. Tale tipologia di autenticazione è stata progettata per affiancare dei server basati su autenticazione 802.1X, prevedenti l'identificazione degli utenti attraverso la distribuzione di chiavi univoche.

Esistono due tipi di autenticazione WPA cioè WPA e WPA2, quest'ultima rappresenta la più recente e la più sicura.