Sicurezza in Internet

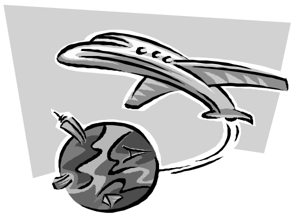
Terminologia e Virus
Tipi di attacchi e contromisure
Crittografia

Sicurezza in Internet

- Terminologia
- Virus
  - Classificazione
  - Evoluzione

Introduzione

- L'informazione è un bene prezioso e deve
  - Essere custodito
  - Protetto
- I sistemi informativi sono
  - Vulnerabili
  - Esposti agli attacchi
- Problema sempre più reale
  - Diffusione dell'informatica per la raccolta ed elaborazione dei dati
  - L'espansione sempre crescente di Internet



Sicurezza su Internet

- Espansione di Internet

e la Diffusione delle reti locali – aziendali

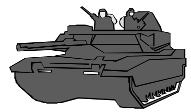
alla circolazione e allo spostamento in rete di dati importanti quali:
- Transazioni economiche
- Segreti industriali

Sicurezza

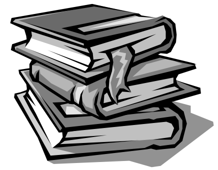
- Non solo in azienda …


- Ma anche sui calcolatori personali
  - Nootebook
  - Home computer (conti personali, codici di carte di credito)

Infowarfare e cybernetic warfare

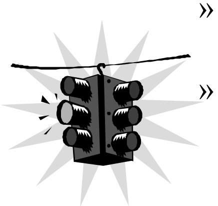


- Infowarfare
  - Termine coniato in ambito militare
  - "Serie di attività finalizzate a danneggiare il patrimonio informativo del 'nemico'
    - » Conoscenze
    - » Credibilità
    - » Immagine



Infowarfare e cybernetic warfare

- Cybernetic warfare
  - Insieme di azioni atte a tutelare il patrimonio informativo
    - » Tecnologie impiegate (firewall, anti-intrusione, antivirus …)
    - » Politiche di sicurezza interne (gestione accessi – responsabilità)
    - » Educazione degli utenti (conservazione password …)




Terminologia

- Abusi Tecnologici.
  - Insieme di azioni consistenti in un utilizzo distorto di una tecnologia ideata e creata per fini positivi.
- Attacker o Malicious Hacker.
  - Chi si occupa di violare i Sistemi informativi con l'intento di danneggiarli.
- Hacker
  - Idealista: viola i sistemi a scopo di "ricerca"
- Cracker
  - Viola i sistemi per fare danni

Terminologia

- Auditing Distribuito
  - Operazioni atte a verificare lo "stato di salute" di un sistema: più tipologie di verifica
- Backtraking
  - Operazioni per la localizzazione di un computer e se possibile del suo utilizzatore (in caso di violazioni)
- Information Security
  - Processo di protezione del patrimonio informativo a rischio (cybernetic warfare)
- Matching
  - Corrispondenza dei dati: tecnica utilizzata per rilevare la presenza di virus o l'attacco al sistema

Terminologia

- Security Policy
  - Regola che realizza una linea guida precostituita: di solito decisa dal management tecnico in collaborazione con un consulente legale
- Sensitive data
  - Non i dati sensibili previsti della legge sulla privacy, ma i dati sensibili di una transazione (è anche l'indirizzo IP)
- Sistemi aperti
  - Sistemi informativi eterogenei comunicanti grazie a una serie di regole standard, ovvero con un linguaggio di "connettività" comune

Terminologia

- Target
  - Obiettivo di un attacco:
    - » Singolo computer (*victim machine*)
    - » Rete (più calcolatori riconducibili ad un'unica entità)

Virus

- Un software (ovvero una porzione di codice) in grado di autoriprodursi e di trasferirsi "attaccandosi" ad altre entità del computer (programmi, disk sector, file di dati, …) e di "muoversi" all'interno del calcolatore

Catalogo/Caratteristiche Virus

- MacroVirus
  - veicolo: sfruttano le macro ovvero le funzioni presenti in programmi come Word, Excel ...
    - » macro sono oggetti che permettono di registrare sequenze di operazioni e di richiamarle velocemente.
  - attivazione: apertura del file infetto
  - effetti possibili: cancellare, rinominare e modificare file;

Catalogo/Caratteristiche Virus

- Polimorfici

  Caratteristica evoluta più che tipologia
  - Modificano la propria struttura per non essere identificati dai sistemi di difesa
  - usano crittografia
    - » versione base: mantengono unica funzione crittografica tramite la quale possono essere identificati
    - » versione evoluta: modificano anche le routine per la crittografia

Catalogo/Caratteristiche Virus

- Retrovirus
  - Attaccano gli antivirus cercando di disabilitarli
- Bombe a tempo (Timer Virus)
  - avvio solo a una certo evento: ora, data, azione ...
- Memory resident
  - si copia in memoria RAM rimane anche dopo la cancellazione se non si adottano tecniche opportune
- Size Stealth
  - nasconde le proprie dimensioni

Catalogo/Caratteristiche Virus

- Size Stealth
  - si nasconde completamente al Sistema Operativo, solo programmi specifici (antivirus) lo possono rilevare

Catalogo/Caratteristiche Virus

- Boot Virus e MBR
  - veicolo: si installano nella zona dei hard disk che viene letta all'avvio
  - attivazione: avvio del PC
  - effetti possibili: possono modificare la FAT criptandola e tenendone una copia altrove, cancellazione file, cancellazione intero HD.

Catalogo/Caratteristiche Virus

- File Virus
  - veicolo: sovrascrivono o si "attaccano" ai file eseguibili (com, exe, dll)
  - attivazione: avvio del programma infetto
  - effetti possibili: si attaccano ad altri file eseguibili, cancellazione file, hard disk
    - » anche danni fisici all HW.

Virus - Non Virus

- Worm
  - Codici indipendenti si diffondono in modo svincolato da eventuali file host
  - Possono essere multipiattaforma
  - Utilizzo risorse di rete (DoS successiva sezione)

Virus - Non Virus

- Trojan horse
  - Malware nascosti in file apparentemente "innocui" e utili
  - Richiedono intervento diretto per l'installazione: non si propaga autonomamente;
  - diffusi spesso tramite e-mail
  - scopo: interrompere il lavoro degli utenti o del sistema, anche con apertura backdoor
  - RAT (Remote Access Trojan) se installati permettono ad un attacker (cracker) di prendere possesso del calcolatore:
    - » due parti: server installato sulla macchina vittima e client su macchina remota (attacker)

Virus - Non Virus

- Hoaxes
  - falsità-burla
  - di solito tramite e-mail
  - chiede di cancellare file, di inviare e-mail
- Spam
  - messaggi di posta elettronica non richiesti
  - pubblicità prodotti o servizi

Scam

tutte le forme di comunicazioni utilizzate per ingannare gli utenti con il fine di produrre un qualche guadagno finanziario

- Phishing
  - Invio di e-mail fraudolenta
  - Richiesta dati personali di accesso (ad esempio Carta di credito, conto bancario).
  - esempio Fineco
  - esempio Bybank

Strumenti Hacker

- Rootkit
  - raccolta software per ottenere l'accesso remoto non autorizzato a un computer per poi poter compiere altri attacchi
  - monitoraggio pressione tasti (cattura password)
  - modifica registro di sistema o di applicazioni esistenti
  - creazione backdoor e avvio di attacchi contro altri sistemi

Altre ...

- Spyware
- Adware
- Cookie Internet

Requisiti Attacco

- Periferiche: tipo specifico
  - personal computer
  - computer Apple Macintosh
  - PDA (agenda elettronica)
- Sistemi Operativi: Windows 98, XP, Unix ...
- Applicazioni: Word, Shockwave Flash

Vettori

- File eseguibili: classico exe, com, sys, dll, ocx
- Script: Microsoft Visual Basic, PHP JavaScript, AppleScript, PerlScript
- Macro: script di macro di particolari applicazioni come elaboratore testi, applicazione database e foglio di calcolo
- Settore di Avvio

Meccanismi di trasporto

- Supporti removibili:
  - ieri floppy
  - oggi dispositivi USB o Firewire
- Condivisioni di rete:
  - alta potenzialità
- Scansione rete:
  - ricerca computer vulnerabili
- Reti P2P:
  - trasferimenti file su porte aperte sui firewall

Meccanismi di trasporto

- Posta elettronica: il prescelto due tipologie
  - Mailer (selezione indirizzi di posta)
  - Mailer di massa
- Attacco remoto: sfruttamento paricolare vulnerabilità in un servizio o applicazione per replicarsi:
  - esempio virus Slammer per SQL Server 2000 tramite un Buffer overflow (esisteva una patch poco installata)

Payload (azione intrapresa)

- Backdoor: accesso non autorizzato al computer
- Danneggiamento o eliminazione dati
  - immediato
  - ritardato a un certo evento: data o azione
- Furto informazioni:
  - credenziali accesso ad conti bancari
  - password in generale
- Negazione servizi di rete (DoS sezione successiva)

Attivazione Infezione

- Esecuzione manuale
- Individuazione persone vulnerabili
- Esecuzione semi-automatica: richiede intervento vittima
- Esecuzione automatica
- Bomba a orologeria: data
- Condizionale: esecuzione di una certa azione

Difesa dell'agente infettivo

- Armatura: tenta di confondere l'analisi del codice dannoso (rilevamento, funzionamento corretto aggiunta codice per sviare)
- Azione furtiva: si nasconde e fornisce informazioni false
- Crittografia: sempre stessa routine di crittografia, chiavi diverse
- Oligomorfico: cambia un numero limitato di routine di crittografia
- Polimorfico: motore di mutazione che genera una routine di crittografia casuale

Antivirus

- Scansione Firme
- Scansione Euristica
  - Falsi positivi
- Blocco Funzionamento:
  - come personal Firewall: blocco applicazione che cerca di comunicare in rete

Origini Problema

- Diffusione iniziale tramite supporti di massa (dischetti ...)
- In seguito, fino ad oggi Internete:
  - Internet nasce come sistema “aperto” ...
- Solo dopo l’avvento del Web primi tentativi di abuso su larga scala

Si parte dal MAC ...

- 1981 primo virus sull dell’Apple II tramite i dischetti.
- Quasi innocuo: visualizzazione al 50° boot di:

  “Tutti i tuoi dischi prenderà
  tutti i tuoi chip infetterà
  è proprio Cloner!”

  Come la colla ti si attacca
  dalla tua RAM non si stacca
  Diffondi Cloner!”
- Il nome assegnato a questo boot sector virus è Elk Cloner .

Nascita ufficiale

- 3 Novembre 1983
  - in otto ore Fred Cohen scrive un programma a cui Len Adleman darà il nome di virus.
  - lo stesso Cohen, negli anni succesivi pone le basi per uno studio scintifico dei virus perfezionando la loro definizione ancora valida oggi.
  - Parte la corsa verso la differenziazione e la moltiplicazione.

Eventi Significativi

- 1986: Brain primo virus per personal computer MS-DOS: scritto da due fratelli pakistani.
- 1987: Jerusalem (file infector virus), e poi l’Ibm Christmas Worm

... poi le reti ...

- 2 novembre del 1988 (Morris Worm)

un programma di sole 99 linee di codice scritto da uno studente della Cornell University, il ventitreenne Robert Tappan Morris mette in crisi la rete Internet

- il virus monopolizza le risorse dei computer infetti per la produzione e diffusione di propri duplicati
- effetto: intasamento linee di comunicazione e circa il 10% dei sistemi connessi in Internet in stallo

... evoluzione ... 1990-91

- 1990 nasce in Bulgaria la BBS VX (Virus eXchange):
  - gli autori dei virus si scambiano consigli e codici
  - viene reso pubblico "The Little Black Book of Computer Viruses": autore Mark Ludwig.
- 1990 Casper primo virus polimorfo
  - rischio basso: il 1 Aprile cancella MBR
- 1991 scocca l'ora dei virus polimorfici Tequila:
  - modifica le sue copie per non farsi individuare
  - rischio basso: mostra messaggio a video, perdite di archivi (inferiore 1%).

... evoluzione ... 1992

- 1992 vengono realizzati i primi programmi di utilità (toolkit) per creare virus e trasformarli in virus polimorfici.
- Più famosi (quasi delle IDE)
  - Dame (Dark Avenger's Mutation Engine)
  - Vcl (Virus Creation Laboratory)

1995 - 1998

- 1995: arrivano i Macro Virus per Word
  - Concept: disabilita menu macro e attacca i template.
- anno successivo:
  - Boza (per Windows 95): attacca file exe utilizzando kernel32.dll
  - Staog (per Linux)
  - Laroux macro virus per Excel
- 1998: Java ...
  - Strange Brew
- e Back Orifice (controllo remoto).

1999

- 1999: Melissa, Corner, Tristate e Bubbleboy.
- Utilizzo dell'e-mail per riprodursi: Melissa sfrutta la rubrica di Outlook (macro virus Word97)
- Corner disabilita macro in Word
- Bubbleboy: Internet worm richiede Internet Explorer 5, invio e-mail
- Tristate primo virus multi-programma:
  - file Word, Excel e PowerPoint.
  - cancella template

2000

- baco del millennio; Y2K è un bug, non un virus, ma ...
- esplosione programmi che infettano posta elettronica:
  - Love Letter, Timofonica
- Liberty: residente file .exe effetti:?
- Streams:
  - compressore sostituisce file originale, win2000
- Pirus: primo php virus
  - <?php include("FILENAME.PHP"); ?>

Esempio

- Il messaggio di posta elettronica contiene:

Subject = "TIMOFONICA"

Body =

"Es de todos ya conocido el monopolio de Telefónica pero no tan conocido los métodos que utilizó para llegar hasta este punto."

"En el documento adjunto existen opiniones, pruebas y direcciones web con más información que demuestran irregularidades en compras de materiales, facturas sin proveedores, stock irreal, etc."

"También habla de las extorsiones y favoritismos a empresarios tanto nacionales como internacionales. Explica también el por qué del fracaso en Holanda y qué hizo para adquirir el portal Lycos."

"En las direcciones web del documento existen temas relacionados para que echéis un vistazo a los comentarios, informes, documentos, etc."

"Como comprenderéis, esto es muy importante, y os ruego que reenviéis este correo a vuestros amigos y conocidos."

Attachment ="C:\TIMOFONICA.TXT.vbs"

- l'allegato contiene un internet worm

2001

- Gnuman:
  - Gnutella network users fa credere la presenza del file cercato
- Winux (o Lindos)
  - Windows: file 32 bit
  - Linux: file ELF
- worm
  - AplS/Simpsons: usa "deltree.exe"
  - PeachyPDF-A e Nimda: mass-mailing worm, network share propagation, backdoor

2001

- Nimda
  - primo a sfruttare vulnerabilità sistema operativo
  - Vulnerabilità IIS (usato nel 30% dei server del mondo; fonte NetCraft Web Server Survey)
    - » servizio Web Directory Traversal
  - Colpiva gli utilizzatori di Internet Explorer 5.5 senza patch;
  - chi usava Internet Explorer 5.0 riceveva la richiesta di download

2001

- BadTrans
  - » mass mailing worm che utilizza Microsoft Outlook con Inoltro delle email non lette
  - » attiva un remote access trojan (Backdoor-NK.svr)
  - » quando è attivo mostra un message box con titolo, "Install error" e messaggio "File data corrupt: probably due to a bad data transmission or bad disk access."
  - » si salva in copia nella directory WINDOWS come INETD.EXE e tramite WIN.INI si attiva all'avvio.
  - » KERN32.EXE (a backdoor trojan), and HKSDLL.DLL (a keylogger DLL sono posti nella caretlla WINDOWS SYSTEM e viene creata un apposita chiave di registro.

2001

- Goner
  - mass mailing worm che utilizza Microsoft Outlook si invia a tutti gli indirizzi trovati nel Outlook Address book.
  - prova a cancellare security software
  - può diffondersi tramiteICQ, e cancella IRC bot script e accetta instruzioni per iniziare un Denial of Service attack verso gli utenti remoti IRC che sono connessi allo stesso canale.

2002

- LFM-926
  - infetta i file Shockwave Flash
- Donut: Microsoft .NET architecture
- Sharp-A: Microsoft .NET architecture
  - scritto nei linguaggi C#, SQL
- Spider: invia log tasti premuti (banca brasiliana)
- Benjamin:
  - cambia parametri Kazaa software
- Perrun: Infected JPEGs scritto in vb6

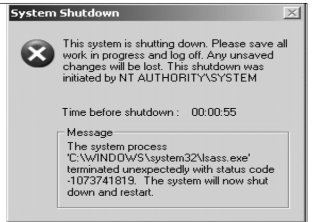
2003

- Worm Blaster
  - Windows NT 4.0
  - Windows 2000
  - Windows XP
  - Windows Server 2003
- riavvi del sistema

2003

- Bugbear
  - Mass-mailer
  - Network Share Propagator
  - Keylogger
  - Remote Access Trojan: TCP Port 1080
  - Polymorphic Parasitic File Infector
  - Security Software Terminator
- Sobig
  - diffusione attraverso condivisione di rete e e-mail. Il worm contiene un motore SMTP.

2004



- Netsky e Sasser
  - ideati da Sven Jaschan ragazzo tedesco di 18 anni
  - Sasser
    - » scansiona random indirizzi ip addresses se in ascolto sulle porte TCP porte dalla 1068.
    - » agisce come FTP server sulla porta 5554 TCP e crea una shell remota sulla porta TCP 9996.
  - Netsky
    - » sfrutta "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), to automatically execute the virus on vulnerable systems.

2004

- Sober
  - mass-mailing worm

  con proprio SMTP engine
  - doppio click su file infetti

- Zafi-B
  - mass-mailing worm con proprio SMTP engine
  - spoofing the From: address.
  - tenta propagazione via P2P copiando se stesso nelle cartelle che contengono nel nome share e upload
  - blocca antivirus

2005

- Mydoom.AK
  - mass-mailing worm con proprio SMTP engine
  - spoofing the From: address.
  - contains a backdoor apre la TCP port 3127 (se non riesce tenta le porte a partire dalla 3198)
  - Denial of Service payload
- Sober.V
  - mass mailing worm scritto in Visual Basic
  - oltre alla porta 25 per inviare e-mail, utilizza una porta non-standard (587) per connettersi a Yahoo servers,sempre per inviare mail.

2005

- Zar.A
  - mass mailing worm che utilizza Microsoft Outlook,
  - si invia a tutti gli indirizzi trovati nel Global Address Book.
  - Il virus è ricevuto con un e-mail con il seguente messaggio:
    - » Subject: Tsunami Donation! Please help!

2005

- Mytob
  - mass mailing worm
  - incorpora “Sdbot” functionalità
  - è progettato per contattare il server IRC irc.blackcarder.net su uno specifico canale e attendere istruzioni.
  - può accettare comandi per scaricare e eseguire altri programmi
  - contiene codice per diffondersi tramite LSASS exploit

2006

- SpamBot:
  - un trojan trasmesso via email da un falso avvocato, che vuole farvi causa per aver ricevuto email pornografiche da voi.
- Kamasutra, Grew.A o MyWife
  - mass-mailing worm on proprio SMTP engine
  - spoofing the From: address.
  - diffusione tramite condivisioni di risorse di rete
  - riduce configurazione sicurezza e disabilita software di sicurezza
  - sovrascrive file il 3 di ogni mese

Altre notizie

- 1991 (Guerra del Golfo) gli USA attaccano e infettano la rete militare irachena
- 1998 Aprile il Dod degli USA annuncia di aver subito in una settimana 250.000 attacchi
- Primo auditing su larga scala (1998) su commissione DoD
- Nello stesso anno l'FBI stima i possibili danni dai 100 ai 300 miliardi di dollari
- 1999 Amministrazione Clinton autorizza investimento 1,5 miliardi di dollari per studio del problema

Possibili cause del contagio

- L'utente avvia l'esecuzione del file allegato ...
- Il file di aggiornamento delle definizioni dei virus non installato ...
- I server non sono aggiornati periodicamente e frequentemente con le patch
- Individuazione persone vulnerabili: accreditarsi come amministratore di sistema o fornitore di servizi
- Appriazione indirizzi posta elettronica

Possibili cause infezione e diffusione

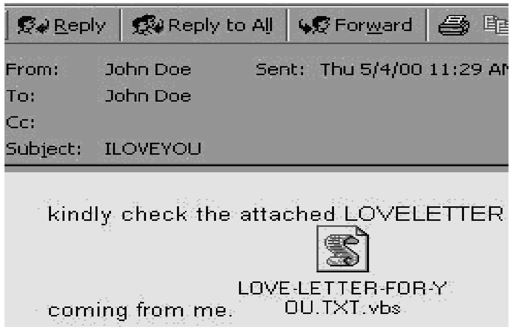
- Motore di posta integrato nel Malware per migliorare la propagazione dell'infezione
- Sfruttamento vulnerabilità prodotti
- Sfruttamento tecnologie Internet: nuovi strumenti come ad esempio i P2P

Soluzione ?

- Non e' possibile trovare una soluzione esaminando il problema a compartimenti stagni
- La soluzione è "Multilivello"
  - più componenti che interagiscono
  - molto importante il fattore umano
- Inoltre ad attacchi distribuiti si devono contrapporre difese distribuite

Contromisure

- Lo studio, l'intelligenza e la condivisione delle informazioni sono le migliori armi oggi a nostra disposizione
- Eesmpio:
  – Melissa
  – Loveletter



Tre Leggi

- Mai dire mai:
  – non esiste una metodica sicura e inattaccabile definitivamente
  – Ciò che appare impossibile oggi, domani sarà realizzato
- La sicurezza totale non esiste
  (postulato)
- Non si possono risolvere i problemi di sicurezza con il solo software
  (legge di Ranum)

Beni da proteggere

- Il primo elenco evidenzia tre categorie
  – Hardware
  – Software
  – Dati
- In dettaglio e non solo ...
  – Supporti di memorizzazione (software e dati)
  – Reti (scambio dati)
  – Accesso (possibilità utilizzo bene)
  – Individui chiave (amministratore sistema, operatore specializzato)

Sicurezza Informatica: Obiettivo

Garantire un adeguato grado di protezione dei *beni*, mediante l'attuazione di un progetto di sicurezza globale che, tenendo conto dei vari aspetti del problema, raggiunga un livello di protezione, organizzativo ed informatico che possa essere monitorato nel tempo.

Per realizzare ciò bisogna definire una politica di sicurezza in modo che il *bene* mantenga nel tempo le sue proprietà di disponibilità, integrità e sicurezza

C.I.A.

- Confidentiality (Riservatezza o Confidenzialità).
  - I dati non sono accessibili e/o interpretabili da chi non ne ha diritto.
- Integrity (Integrità).
  - Non deve essere possibile alterare in alcun modo i dati utilizzati in una transazione. (contrattualistica digitale, e-commerce, e-businnes …).
- Autentication (Autenticazione).
  - L'identità delle entità coinvolte nella comunicazioni deve poter essere verificata.

Sicurezza: più Livelli

Sicurezza totale è un astrazione ⇒ l'obiettivo diventa ridurre il rischio ⇒ si deve attuare una vigilanza a più livelli ⇒ separazione tra intranet e rete pubblica (WEB) tramite Firewall e introduzione di sistemi di identificazione fisici o logici.

Oggi il problema si allarga con la diffusione (costi contenuti) di Internet a Banda Larga (tramite la tecnologia ADSL) anche tra i singoli utenti che diventano a rischio.

Un'altra fonte di rischio sono le Reti mobili.