



Consorzio per la formazione e la ricerca in Ingegneria dell'Informazione
Politecnico di Milano

Virus e intrusioni automatizzate

Ing. Glauco Bigini
Cefriel - NS Unit

bigini@cefriel.it
<http://www.cefriel.it/ns>

© 2003 - Ing. Glauco Bigini



- Il mondo dei virus: definizioni, evoluzione, attacchi
- I software antivirus: tecnologia e limiti
- La difesa
 - ▶ L'informazione e le fonti
 - ▶ La creazione di un sistema di protezione dalle aggressioni da virus
- Case study e conclusioni



- Virus normalmente percepiti come entità più o meno “oscure” in grado di insinuarsi nei computer per distruggere i dati in essi contenuti
- Col tempo e con l’avvento delle reti i virus si sono evoluti e sono in grado di operare come un “cracker” in carne ed ossa, solo in modo più rapido ed insistente
 - ▶ **Hacker** è un concetto diverso da **Cracker**: un hacker è un soggetto che ama studiare e giocare con una tecnologia nei particolari, un cracker sfrutta questa capacità per compiere atti illeciti o fraudolenti
- Ciò che un moderno virus fa in realtà è un’intrusione vera e propria, in modo automatizzato



Alcune definizioni (1)

Virus

Un programma in grado di riprodurre autonomamente il proprio codice, inserendolo in quello di un altro programma, in modo tale che questo codice sia eseguito ogni volta che il programma ospite viene eseguito.

Macro Virus

Particolare forma di virus informatico scritto utilizzando il linguaggio di scripting fornito da programmi di Office Automation (principalmente Microsoft Office) che però presenta le stesse caratteristiche di un qualsiasi altro virus

Worm

Un programma in grado di esplorare autonomamente una rete di computer e di copiare se stesso, interamente o in parte, in zone dove possa essere eseguito, sfruttando vulnerabilità di sicurezza dei software che forniscono servizi di rete.

Ogni tipo di virus PUO' portare con se un "payload" contenente codice dannoso



Alcune definizioni (2)

Trojan Horse

Un programma, all'apparenza normale ed innocuo, che in realtà porta dentro di se codice in grado di svolgere azioni non documentate e potenzialmente dannose per il sistema su cui viene eseguito

Key Logger

Un programma in grado di raccogliere in memoria o in appositi file tutte le battute effettuate sulla tastiera. I dati raccolti possono essere spediti via e-mail o prelevati tramite altri mezzi da individui malintenzionati per estrarne informazioni utili

Backdoor

Un programma in grado di accettare connessioni dalla rete esterna, sia su porte note e utilizzate, sia non documentate, e di fornire un set minimale di comandi tramite i quali è possibile, in modo estremamente semplice per un malintenzionato, acquisire il completo controllo del sistema

Spesso i trojan horse sono costituiti da programmi molto utilizzati, modificati e spacciati per versioni ufficiali. Key logger, e Backdoor o virus possono essere parte di un Trojan horse o di un virus



Si sa ma spesso si dimentica...

Un Virus, worm,
trojan horse, ...
E' un
PROGRAMMA

I Virus sono pensati
per essere
INDELEBILI

I peggiori virus
Informatici sono
**INESPERIENZA e
DISATTENZIONE**

- I virus devono essere eseguiti in qualche modo per funzionare
- Prima cosa da fare in caso di attacco automatizzato: **capire da dove è partito, chi o cosa per primo lo ha eseguito**

- Una volta in esecuzione, un virus farà di tutto per
 - **nascondersi**
 - **replicarsi**
 - **essere eseguito al prossimo riavvio**
- Il virus non si rimuove solamente cancellando il singolo file infetto

- Mancata osservazione delle politiche di sicurezza
- Aggiornamento non regolare o del tutto assente
- Utilizzo di software di non sicura provenienza



Gli albori

Complessità
del codice

Primo trattato scientifico
sui virus informatici (Cohen - 1984)

Primo PC DOS "vero" sul mercato
(IBM PC XT - 1981)

Viene creato il CERT
(1988)

Backdoor
(BackOrifice)

Virus polimorfici ("Michelangelo")
Primi kit per creare virus

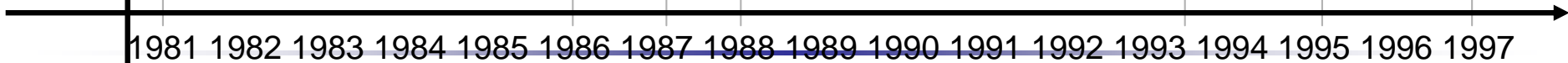
Macro Virus

Primo worm: il "Morris Worm" o "Internet Worm"
sfrutta una vulnerabilità dello stack
TCP/IP dei sistemi Unix

Primo "boot sector virus"
e primo trojan horse

Primo virus "vero"
(Elk Cloner)

Primi virus dei file
eseguibili DOS (exe)





2000

- I primi worm a larga diffusione via e-mail (I love you)
- Primi virus VBScript e Javascript
- I virus si spostano sui Palm
- Primo virus progettato per NTFS
- Primo virus in PHP/ASP

2001

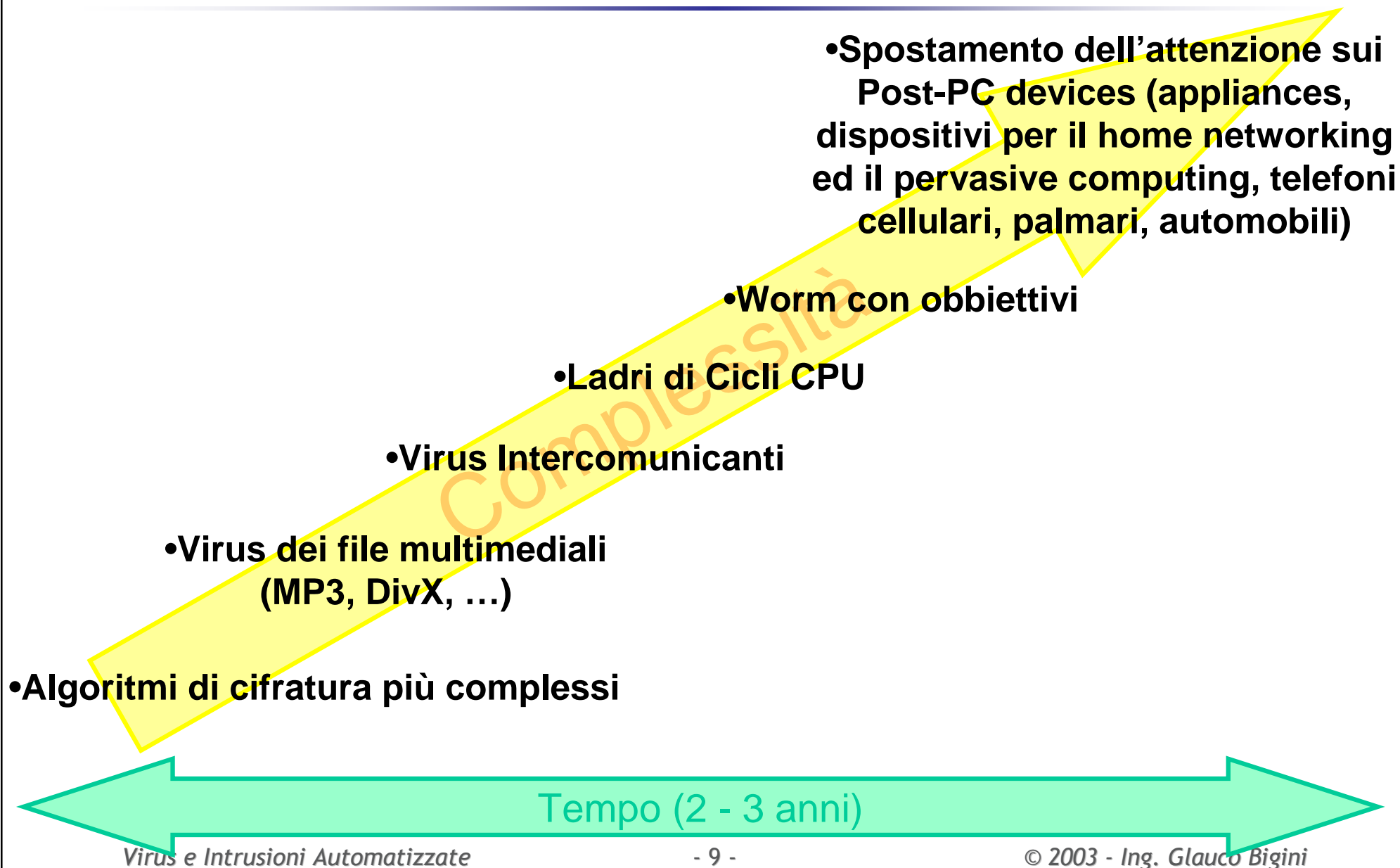
- Primo virus multiplatforma Windows/Linux
- Nimda/CodeRed, primo worm ad utilizzare più mezzi di propagazione

2002

- Primi virus in Java e C# per l'architettura .net
- Primi worm per sistemi di file sharing Peer to Peer
- Primi virus di file non contenenti codice (JPEG, animazioni Flash)

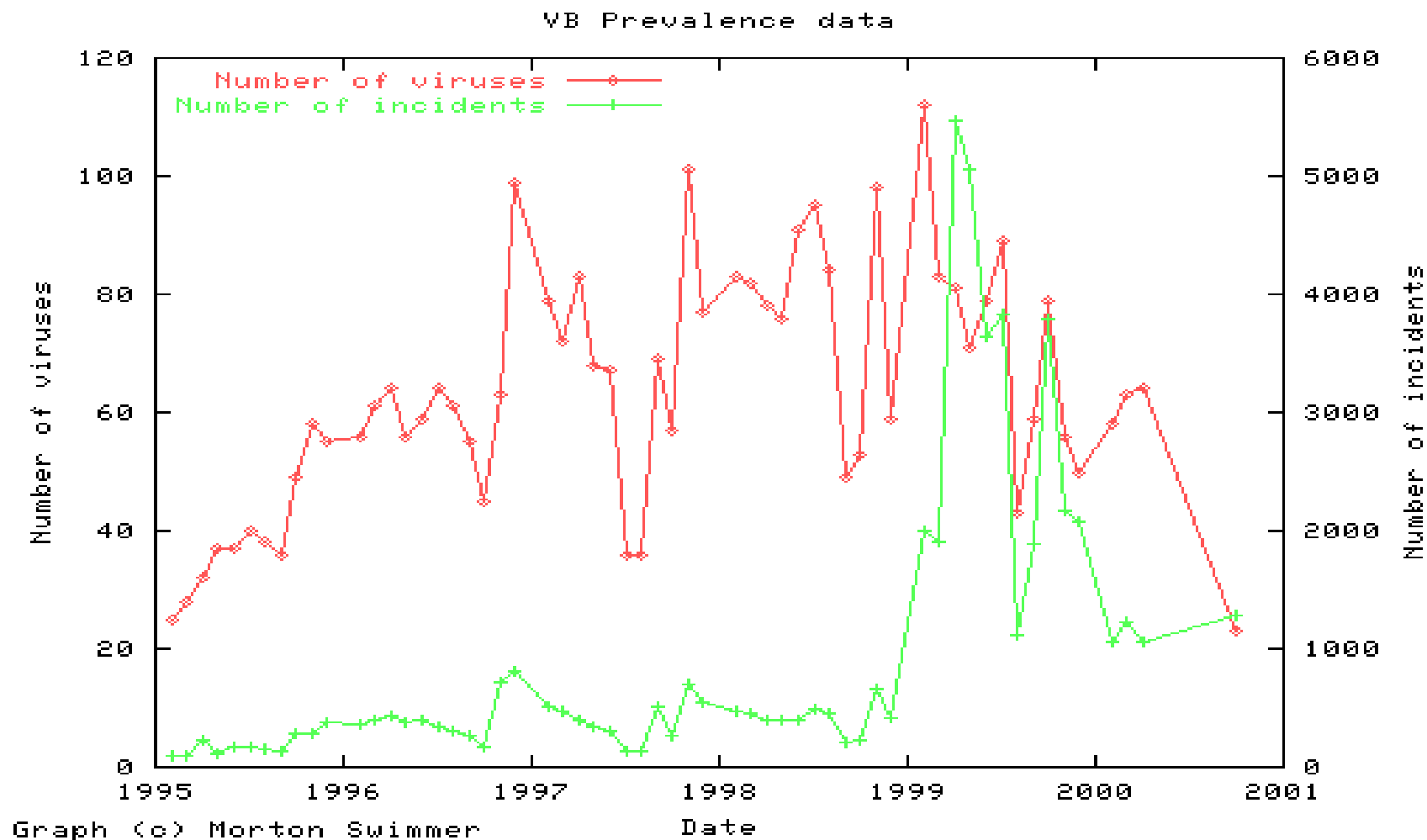


Il futuro





Evoluzione degli incidenti dovuti a virus



Fonte: <http://www.swimmer.org/morton/vstat.html>



Caratteristiche di un virus



- La bontà di un virus non si misura MAI dal danno che è in grado di causare
- Creare un buon virus è estremamente difficile
- Esistono tools per la creazione automatica di virus e motori di cifratura o polimorfismo



Scrivere un Virus - Conoscenze necessarie

Programmatore	Profonda conoscenza della programmazione ad alto livello (C, C++, VB, ...)	Profonda conoscenza della programmazione a basso livello (Assembler)	Notevole abilità nel maneggiare codice per ottimizzarne velocità e dimensioni
Ricercatore	Costante studio, aggiornamento e pratica nella programmazione	Capacità di applicare e sviluppare nuovi algoritmi e soluzioni	
Sistemista	Comprensione completa del funzionamento di un sistema operativo	Capacità di sfruttare appieno le caratteristiche del Sistema Operativo	
Hacker	Conoscenza dei protocolli e della programmazione di rete	Abilità e pratica nello sfruttare le vulnerabilità dei software	

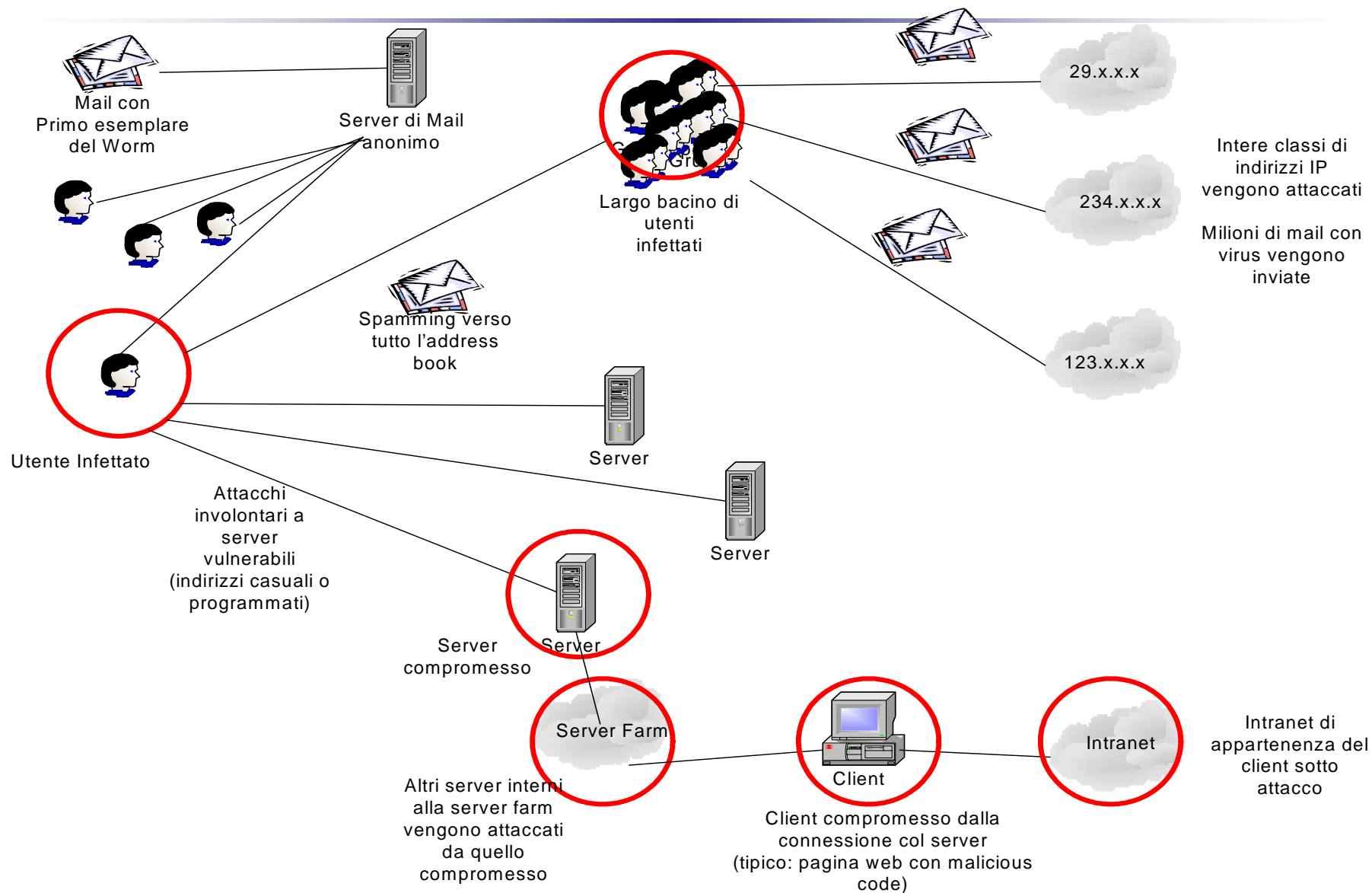


Come agisce un virus

- **Prima generazione di virus**
 - ▶ Metodo di infezione: attacco diretto dei file su una singola macchina
 - ▶ Attivazione: esecuzione di file infetto o utilizzo di supporti magnetici infetti
 - ▶ Propagazione: infezione all'interno della singola macchina, spostamento per "impollinazione"
- **Seconda generazione (network virus o worm)**
 - ▶ Metodo di infezione: multicanale, attacco diretto o ricerca di vulnerabilità in applicazioni internet e posta elettronica
 - ▶ Attivazione: esecuzione diretta o intrusione tramite sfruttamento di vulnerabilità
 - ▶ Propagazione: automatica, tentativi di intrusione da una singola macchina infetta a tutte quelle raggiungibili

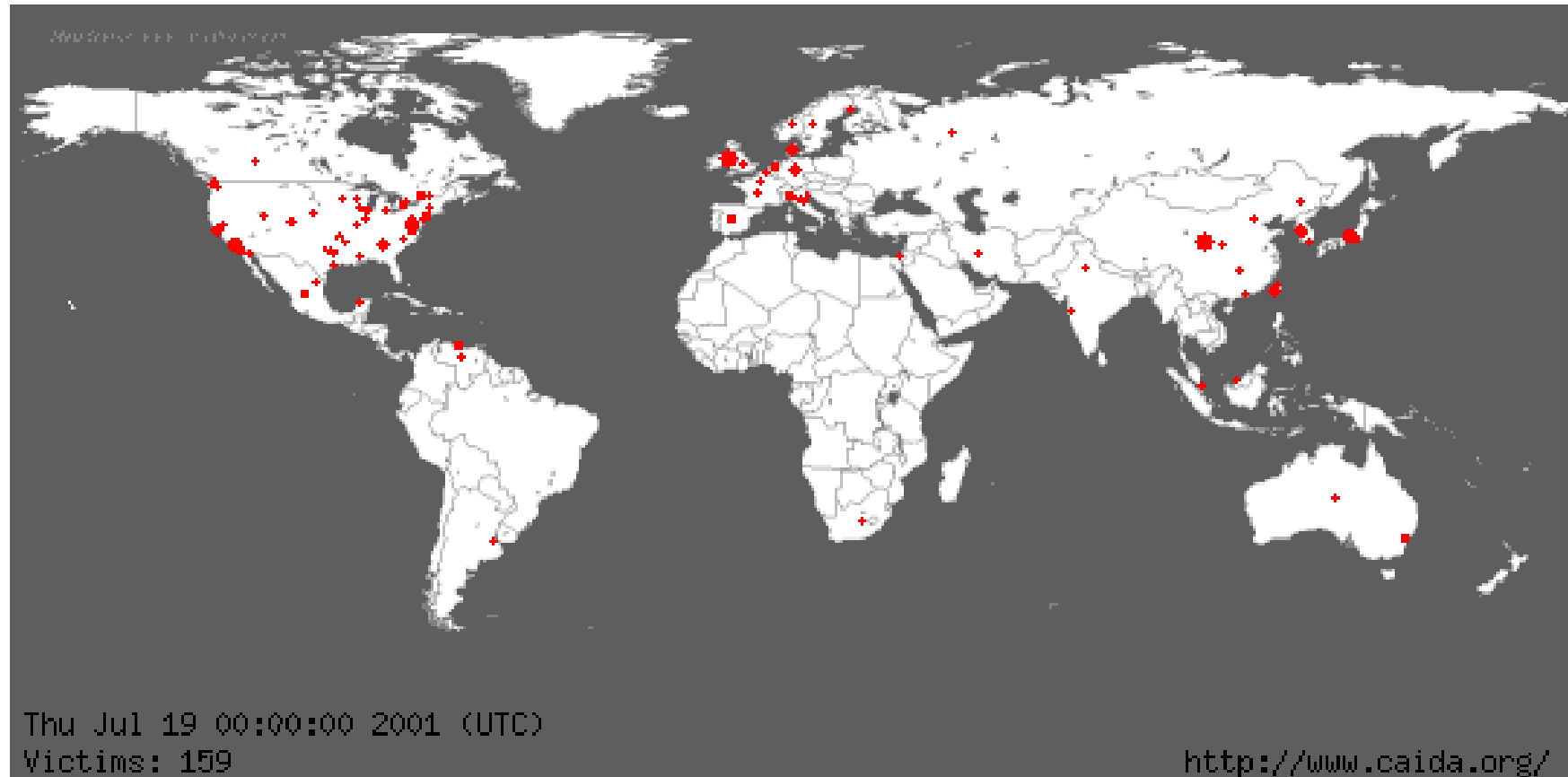


Struttura di un'aggressione di un worm





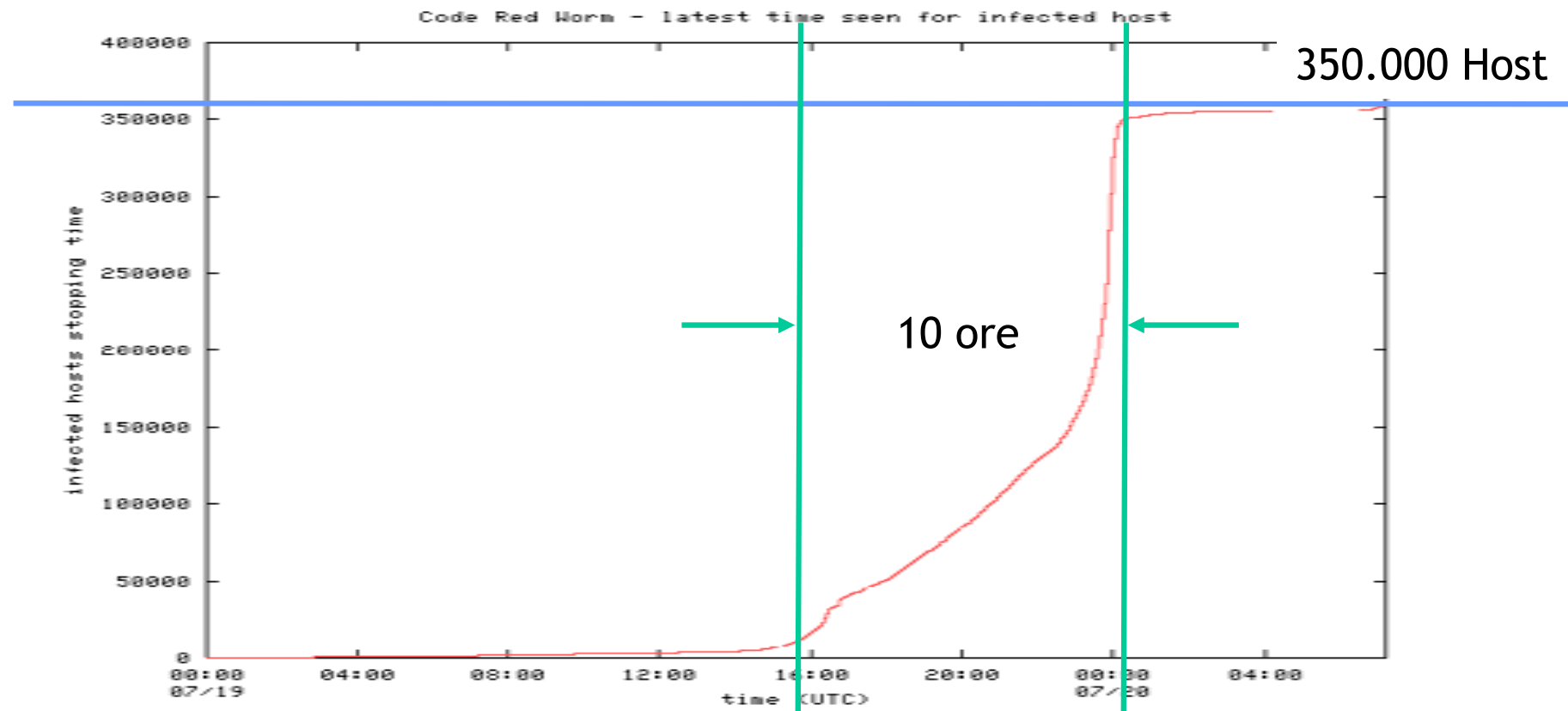
Rapidità e diffusione geografica infezione (Nimda Worm, 2001)



Fonte: CAIDA – 2001, <http://www.caida.org>



Numero di host irraggiungibili in seguito ad infezione (CodeRed worm, 2001)



Numero di host resi irraggiungibili a causa del riavvio dovuto alla necessità di rimozione del virus

Fonte: CAIDA (2001)

<http://www.caida.org>



Sommario

- Il mondo dei virus: definizioni, evoluzione, attacchi
- I software antivirus: tecnologia e limiti
- La difesa
 - ▶ L'informazione e le fonti
 - ▶ La creazione di un sistema di protezione dalle aggressioni da virus
- Case study e conclusioni



I software antivirus - Definizione e limiti

- Un software antivirus è un programma in grado di leggere il contenuto di un file, sia esso su disco o in memoria con l'intento di identificare possibili infezioni da virus informatici
- **Attenzione: è stato dimostrato analiticamente (Cohen, 1984) che non può esistere un programma in grado di determinare con una probabilità del 100% se un altro programma si può comportare da virus**
 - ▶ Le espressioni come "In grado di scovare tutti i virus noti e non noti" non sono vere
 - ▶ Nel caso dei virus noti l'individuazione è operazione relativamente semplice, per i virus non noti esiste invece **SEMPRE** un fattore di incertezza
 - ▶ Il trade-off tra falsi positivi e falsi negativi è uno degli indici di bontà di un software antivirus



Metodi di ricerca dei virus (1)

Scansione
per
“pattern
matching”

Ricerca di una
“firma” (signature)
caratteristica del
virus all’interno di
ogni file

Le signature
vengono lette da
un file (dat-file o
signature-file) che
deve essere
sempre aggiornato

Se il dat-file non
contiene la firma
per un particolare
virus, questo virus
non può in alcun
modo essere
individuato per
pattern matching

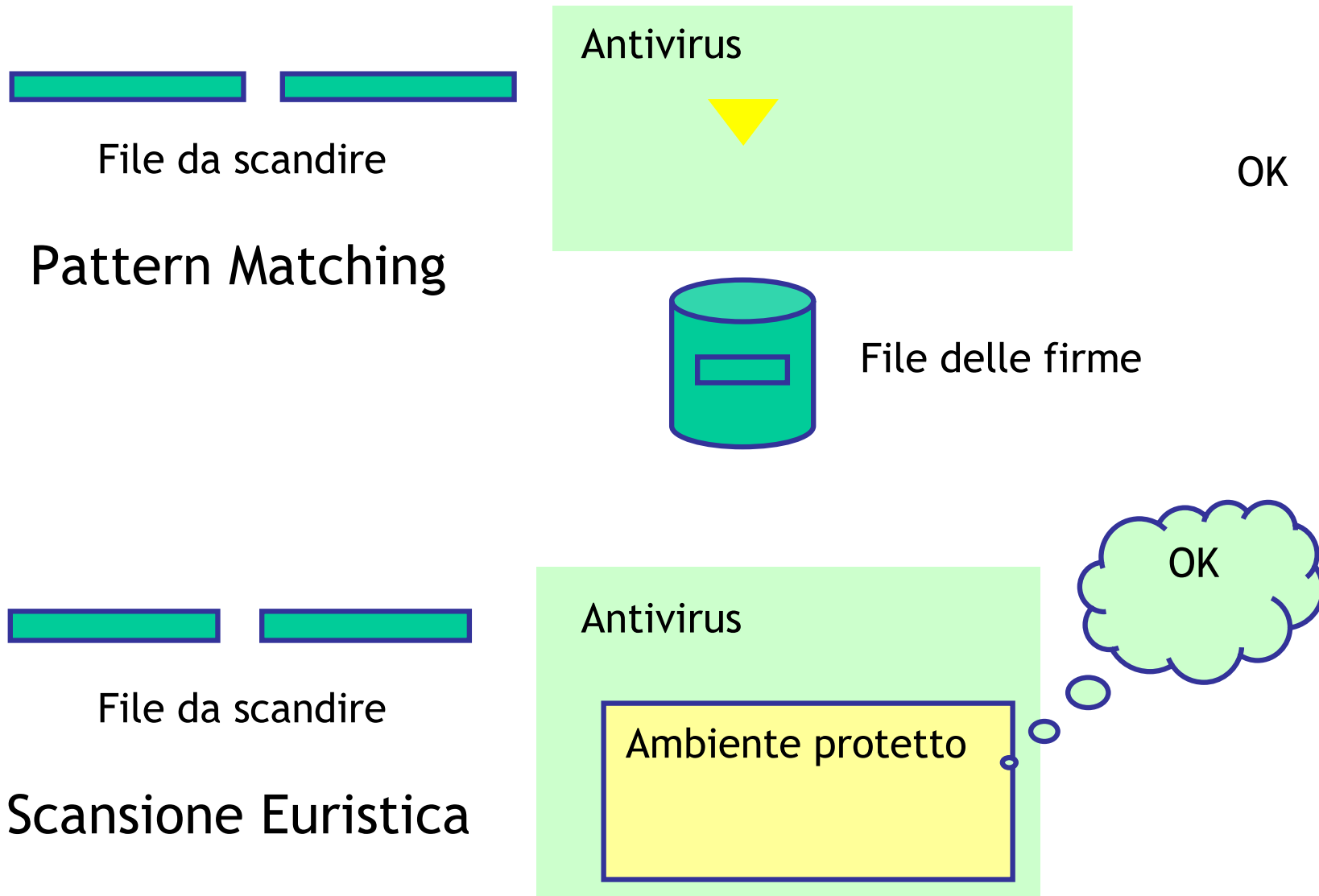
Scansione
euristica

Ogni file dal contenuto
“sospetto” viene messo in
esecuzione in un ambiente
protetto e monitorato
dall’antivirus

Se il file mostra
caratteristiche virali
viene isolato



Metodi di ricerca dei virus (2)





- Il mondo dei virus: definizioni, evoluzione, attacchi
- I software antivirus: tecnologia e limiti
- La difesa
 - ▶ L'informazione e le fonti
 - ▶ La creazione di un sistema di protezione dalle aggressioni da virus
- Case study e conclusioni



- La gestione dei virus informatici deve essere inserita in un sistema completo
- Un singolo prodotto non è assolutamente sufficiente
 - ▶ Aggiornamenti
 - ▶ Controlli
 - ▶ Monitoraggio continuo
- La quasi totalità dei virus sfrutta vulnerabilità NOTE DA TEMPO di sistemi operativi e applicazioni
 - ▶ Verifiche dello stato di salute della sicurezza in rete
 - ▶ Scelta di tecnologie con particolare riguardo alla sicurezza e allo “storico” di aggressioni e incidenti
 - ▶ La sicurezza deve essere il substrato su cui progettare un sistema informativo



Cosa dicono gli standard e le normative

- ISO 17799 / BS 7799
 - ▶ Policy per gli utenti contro utilizzo di software non autorizzato
 - ▶ Installazione e revisione di software antivirus
 - ▶ Periodica verifica di modifiche non autorizzate al contenuto dei dischi
 - ▶ Creazione di un team di gestione del sistema antivirus e formazione del personale
 - ▶ Reperimento di informazioni da fonti affidabili e certificate
 - ▶ Installazione di solo software proveniente da fonte attendibile e certificata
- Legge 547/93 (criminalità informatica)
 - ▶ Art. 615-quinquies. - (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico). - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni."
- DPR 318/99 (misure minime di sicurezza nel trattamento dati sensibili)
 - ▶ I dati sensibili devono essere protetti con misure adeguate
 - ▶ Deve essere prodotto un Documento Programmatico che illustri tutte le misure adottate



Sommario

- Il mondo dei virus: definizioni, evoluzione, attacchi
- I software antivirus: tecnologia e limiti
- La difesa
 - ▶ L'informazione e le fonti
 - ▶ La creazione di un sistema di protezione dalle aggressioni da virus
- Case study e conclusioni



Prima contromisura: Informarsi "BENE"

- (BENE = presto e tanto) Un worm o un virus non hanno tempi di reazione "umani"
 - ▶ La rapidità di reazione ad un'allarme è essenziale, tenersi quotidianamente informati sui virus in circolazione (10min al giorno)
 - ▶ Mantenersi costantemente informati sugli aggiornamenti di sicurezza e sugli incidenti accaduti
 - ▶ Avere sempre una visione precisa del software esposto ad Internet, delle configurazioni dei firewall e del comportamento degli utenti
- (BENE = nel modo giusto) Le informazioni stesse possono essere "virus"
 - ▶ Non prendere mai per vere le prime informazioni circolanti
 - ▶ Verificare sempre la PRIMA provenienza delle informazioni (diffidare di e-mail dalla provenienza non certa)
 - ▶ Diffidare assolutamente di informazioni non certificate da chi le fornisce
 - ▶ Servirsi solo di fonti ufficiali



- Alcune fonti, ufficiali o non, devono essere considerate come campanelli di allarme ma mai per nessun motivo come riferimenti autorevoli
 - ▶ Giornali, media e siti Web : il giornalista insegue la notizia, spesso ricevuta tardi e chissà da chi
 - ▶ Siti Web underground: spesso chi scrive virus (o millanta di farlo) ama vantarsi e ingigantire le proprie gesta
 - ▶ E-mail: possono essere contraffatte con una semplicità estrema, diffidare assolutamente da quelle senza firma digitale e verificare attentamente l'autenticità della firma
 - ▶ Passa-parola: diffidare ASSOLUTAMENTE di queste fonti, anche se chi parla è una fonte autorevole
- **VERIFICARE SEMPRE LE INFORMAZIONI ALMENO 2 VOLTE**



La mitologia dei virus

- Esiste un'amplissima mitologia riguardante i virus, si tratta dei cosiddetti "Virus Hoax" (hoax = "bufala"), le fonti:
 - ▶ Mail degli amici
 - ▶ Passaparola ("fw: i: fw: fw: re: fw: Attenzione virus!")
 - ▶ Sentito dire
 - ▶ Giornali non specializzati
- Ogni sito affidabile sui virus ha anche una nutrita sezione dedicata agli Hoaxes
 - ▶ <http://www.symantec.com/avcenter/hoax.html>
 - ▶ <http://vil.mcafee.com/hoax.asp>
 - ▶ <http://www.f-secure.com/virus-info/hoax/>
 - ▶ <http://hoaxbusters.ciac.org/>
 - ▶ <http://www.vmyths.com>



- I security advisory generici come utile fonte per la prevenzione prima della comparsa di un virus
 - ▶ I vari siti di CERT non osservano direttamente i virus ma le possibili fonti di incidente (buchi, vulnerabilità)
 - ▶ Utilissimi per la prevenzione: un baco può diventare un virus
 - ▶ I siti ufficiali dei produttori sono l'unica fonte accettabile per il reperimento delle patch, ma non sempre dispongono di informazioni tempestive
- Le uniche fonti in grado di essere rapide e precise nelle informazioni specifiche sui virus sono quelle di chi di virus si occupa
 - ▶ Per Incident Response: I siti dei produttori di antivirus e delle società di Information Security
 - ▶ Per informazioni: I siti di chi fa ricerca sui virus



Che informazioni cercare

- Virus attualmente in circolazione
- Virus più attivi nell'ultimo mese
- Virus recenti con maggior numero di incidenti all'attivo
- Vulnerabilità di software molto diffusi che possono indurre alla scrittura di un virus

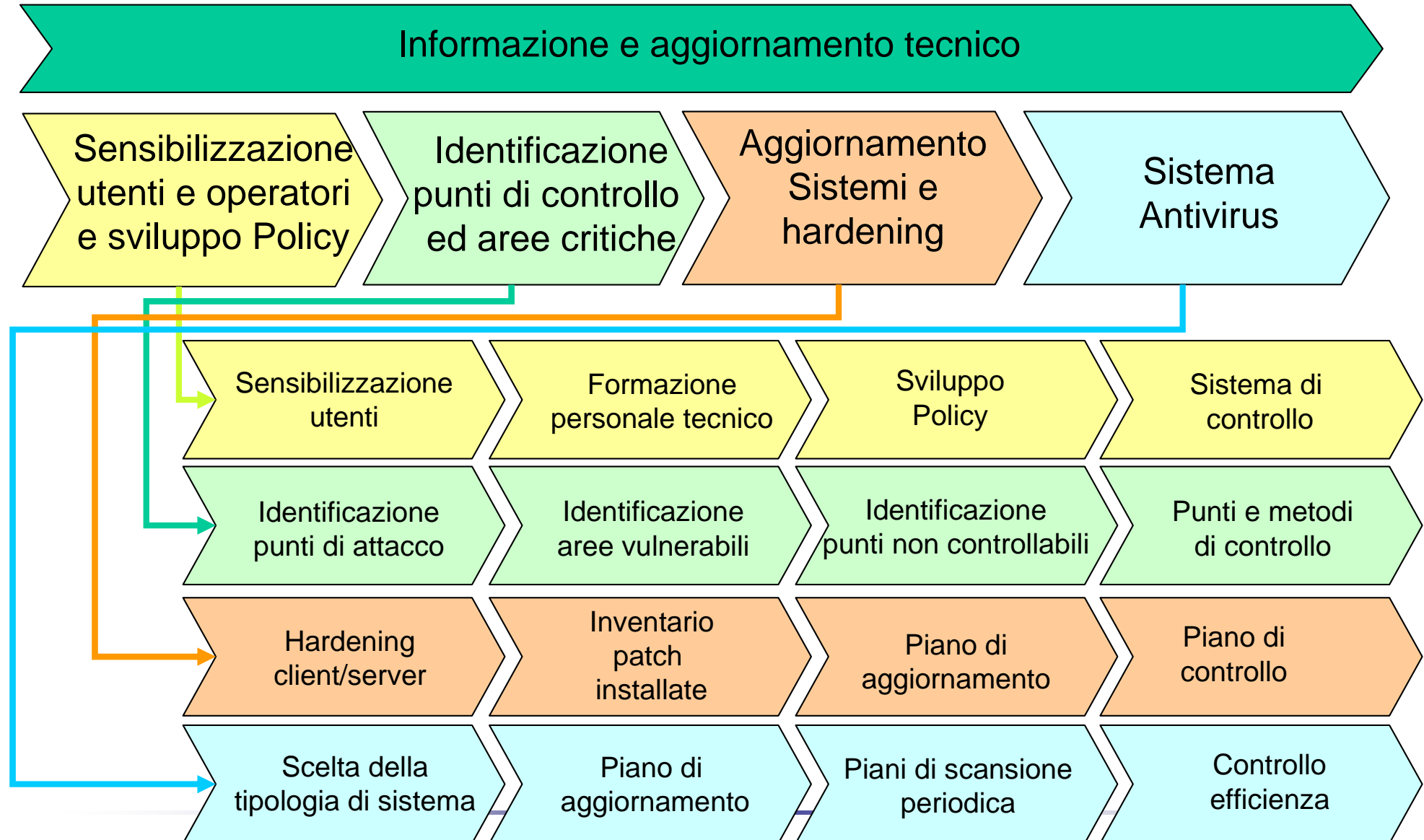


Sommario

- Il mondo dei virus: definizioni, evoluzione, attacchi
- I software antivirus: tecnologia e limiti
- La difesa
 - ▶ L'informazione e le fonti
 - ▶ La creazione di un sistema di protezione dalle aggressioni da virus
- Case study e conclusioni



Il sistema di difesa dagli attacchi di virus





Il Personale

Sensibilizzazione utenti

- Dare agli utenti la percezione corretta del rischio
- Renderli consapevoli delle fonti di infezione
- Prevenire le azioni incontrollate

Formazione personale tecnico

- Formare il personale tecnico con specifica attenzione al rischio di attacchi da virus
- Fare in modo che il sistema di gestione degli attacchi sia noto nel dettaglio

Sviluppo Policy

- Policy con contenuti specifici relativi ai virus
- Motivare sempre le prescrizioni previste

Sistema di controllo

- Controllare sia l'applicazione che la conoscenza delle policy
- Controllare la preparazione degli utenti e dei tecnici



Identificazione punti di attacco

- Programmi per posta elettronica
- Instant messaging
- ICQ
- Server Compromessi
- Portatili
- ...

Identificazione aree vulnerabili

- Server con informazioni sensibili
- Collegamenti di rete critici
- PC con informazioni importanti

Identificazione punti non controllabili

- Utenti esterni
- Accesso Wireless
- Accesso via modem

Punti e metodi di controllo

- Sistemi di monitoraggio della rete
- Analisi dei messaggi di errore dei server
- Controllo di integrità dei file più importanti



Aggiornamenti di sicurezza

Hardening
client/server

Patching

Piano di
aggiornamento

Piano di
controllo

- Controllo della configurazione dei programmi per la posta elettronica
- Impostazioni di sicurezza del browser
- Eliminazione programmi a rischio

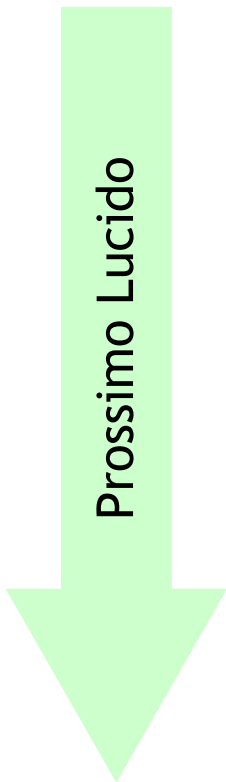
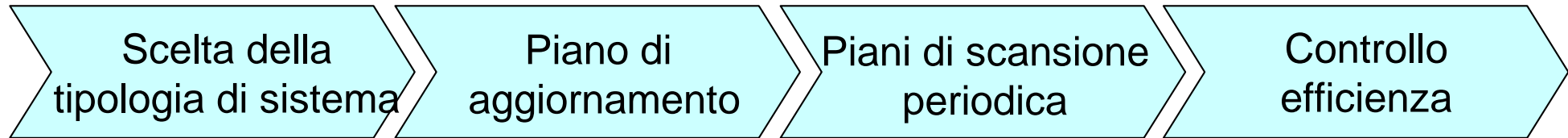
- Installazione di tutti gli aggiornamenti di sicurezza rilasciati
- Catalogazione degli aggiornamenti installati e delle vulnerabilità da essi corrette

- Redazione di un piano periodico di aggiornamento
- Codifica delle operazioni da svolgere
- Attribuzione delle responsabilità

- Redazione di un piano di controllo dello stato di sicurezza
- Redazione di un report periodico con le mancanze da correggere



Il sistema antivirus



- Redigere piano di aggiornamento del sistema antivirus
 - Aggiornare con frequenza elevata il file delle definizioni dei virus
 - Includere nel piano anche gli host non direttamente controllabili (portatili)
- Scandire periodicamente i sistemi
 - Raccogliere e catalogare gli output delle scansioni
 - Mantenere statistiche sulle aggressioni
- Verifica periodica dell'effettivo aggiornamento dei sistemi
 - Verifica dell'avvenuta scansione
 - Aggiornamento anche del motore di scansione, non solo del dat-file



Tipologie di Antivirus

Antivirus per Host/Server

Il più noto software antivirus:

- Controlla un singolo host
- Previene il caricamento in memoria di codice virale
- Consente scansioni delle unità disco
- Blocca le attività dannose di script e macro
- Scandisce la posta elettronica in entrata e uscita dall'host

Antivirus per applicazioni di rete

Antivirus per firewall

Antivirus per server Mail

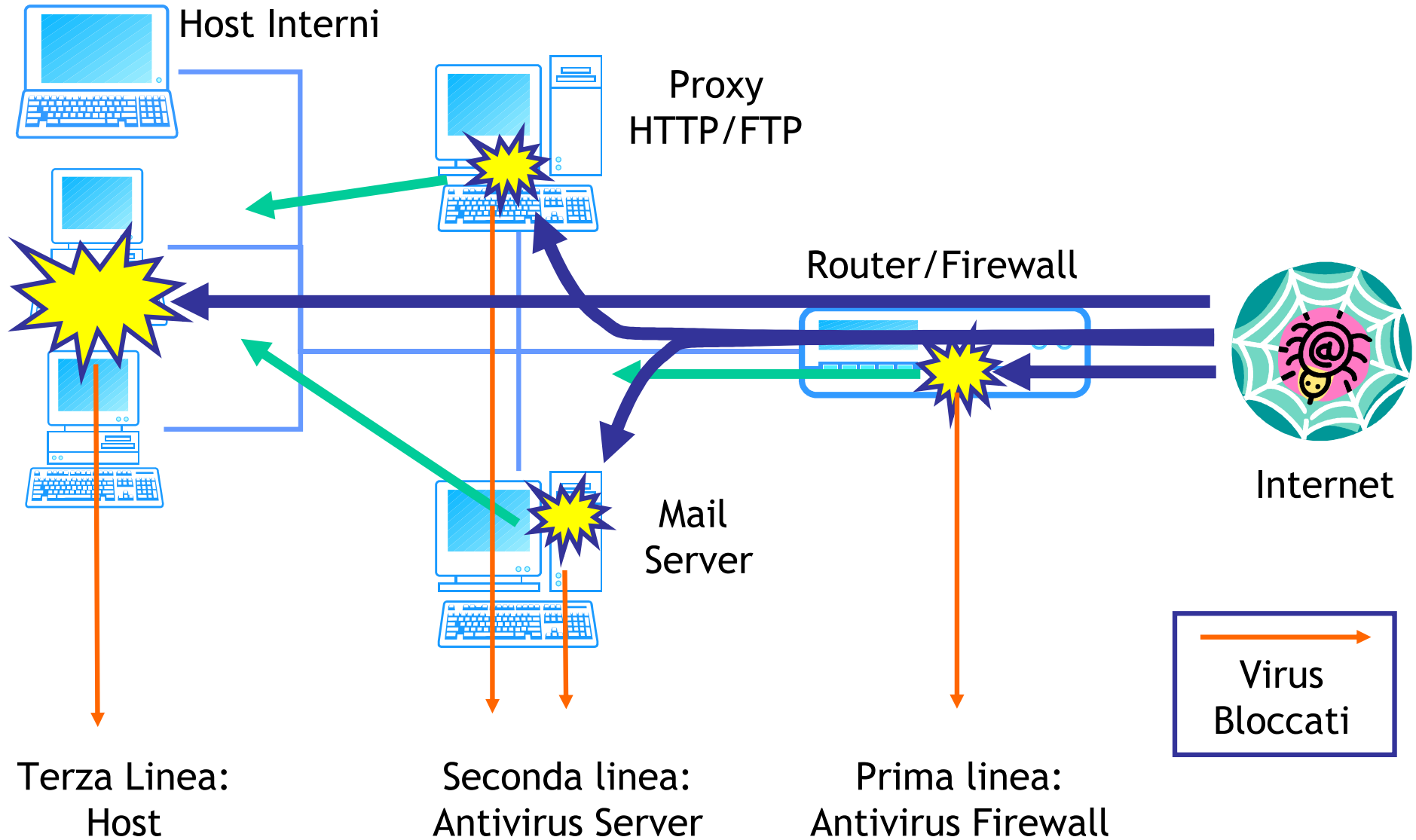
Antivirus per traffico Web

Software dedicati agli applicativi lato server o back-office

- **Per firewall:** Scandisce tutto il traffico in entrata bloccando quello dannoso
- **Per Mail server:** Scandisce tutte le mail in entrata ed in uscita, bloccando i contenuti dannosi e sostituendoli con avvisi di allerta
- **Traffico Web:** Funziona da proxy per traffici Web, FTP, Mail bloccando i contenuti dannosi

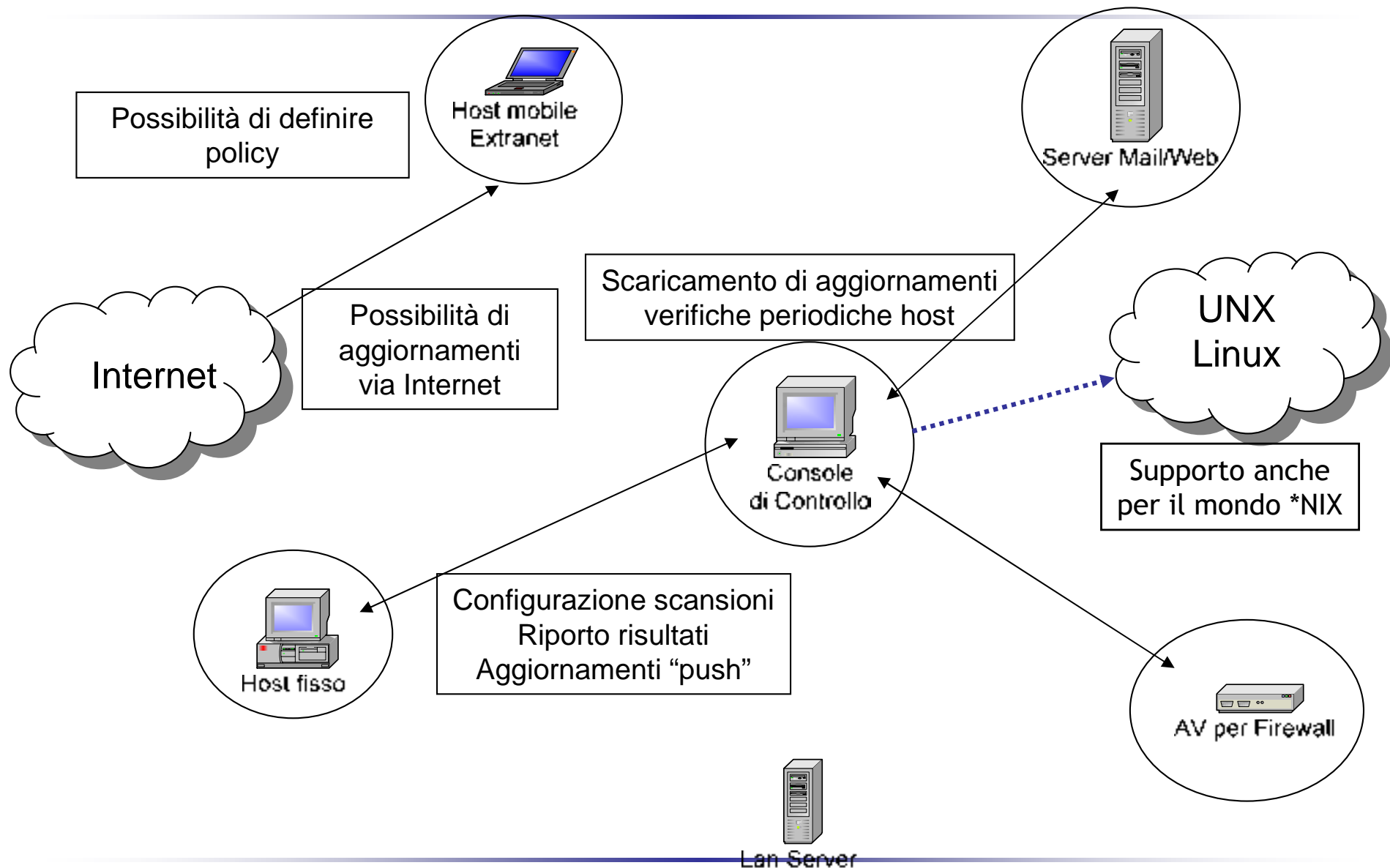


Tipologie di antivirus





Il software antivirus - caratteristiche minime





- Indice di azione di un virus è un comportamento anomalo della rete
 - ▶ Traffico eccessivo
 - ▶ Elevato numero di richieste ai server
 - ▶ Presenza di particolare traffico proveniente da host altrimenti poco attivi
- Spesso si viene attaccati da un virus senza saperlo e senza poter prendere provvedimenti
- La rete va monitorata costantemente con strumenti non direttamente collegati alla ricerca di virus
 - ▶ IDS per l'individuazione di tracce di attacchi da virus non ancora noti
 - ▶ Monitoraggio del carico di rete
 - ▶ Analisi dei log di sistema dei server o installazione di sistemi di notifica degli eventi



- Il mondo dei virus: definizioni, evoluzione, attacchi
- I software antivirus: tecnologia e limiti
- La difesa
 - ▶ L'informazione e le fonti
 - ▶ La creazione di un sistema di protezione dalle aggressioni da virus
- Case study e conclusioni



- Periodo di propagazione: Gennaio 2003 (1/2003)
- Sistemi affetti: Windows 2000/XP SQL Server
- Come si propaga: Tramite SQL Server (il server Database di Microsoft) mandando un apposito pacchetto contenente istruzioni che provocano una falla nell'applicativo DB del server
- Causa della falla: **una vulnerabilità nota da ben 6 mesi**, per la quale era da tempo disponibile un aggiornamento di sicurezza
- Danni ed effetti collaterali
 - ▶ Interruzione di servizio: la rete di appartenenza del server infetto è completamente saturata di messaggi del virus, il server deve essere scollegato per evitare blocchi prolungati
 - ▶ Il virus non provoca altri danni e non danneggia le informazioni contenute nel server
- **Nota: sebbene non particolarmente dannoso, questo virus ha causato il blocco di diverse grosse reti locali (in Italia il caso più eclatante è stata la rete delle Poste)**



Conclusioni

- Un moderno virus agisce come un cracker, ma è molto più veloce ed insistente
- La quasi totalità dei virus sfruttano vulnerabilità note di sistemi operativi e applicativi
 - ▶ Aggiornare i sistemi con frequenza e regolarità
 - ▶ Documentarsi e controllare regolarmente il sistema
 - ▶ In fase di progettazione, scegliere sistemi meno vulnerabili
- La gestione dei virus deve essere inserita in un sistema di sicurezza completo
 - ▶ Scegliere un software antivirus di buona qualità e adatto alla realtà aziendale
 - ▶ Non affidarsi solo al software antivirus (IDS, monitoring, ...)
 - ▶ Integrare la gestione dei virus con il sistema di sicurezza aziendale



- Produttori di antivirus e siti di advisory
 - ▶ Symantec: <http://www.symantec.com/avcenter/>
 - ▶ McAfee: <http://www.mcafee.com/anti-virus/default.asp>
 - ▶ Trend Micro: <http://www.trendmicro.com/vinfo/>
 - ▶ Computer Associates: <http://www3.ca.com/virusinfo/>
 - ▶ F-Secure: <http://www.f-secure.com/virus-info/>
 - ▶ Panda Software:
http://www.pandasoftware.com/virus_info/map/observatory.htm
 - ▶ Xforce: <http://bvlive01.iss.net/issEn/delivery/xforce/alerts.jsp>
 - ▶ Internet Storm Center: <http://isc.incidents.org/>
- Siti con informazioni tecniche e storiche
 - ▶ Virus Bulletin: <http://www.virusbtn.com/index.xml>
 - ▶ Wildlist International: <http://www.wildlist.org/>
 - ▶ McAfee VIL: <http://vil.nai.com/vil/default.asp>
 - ▶ Fred Cohen Associates: <http://all.net>
- Liste di Hoax
 - ▶ <http://www.symantec.com/avcenter/hoax.html>
 - ▶ <http://vil.mcafee.com/hoax.asp>
 - ▶ <http://www.f-secure.com/virus-info/hoax/>
 - ▶ <http://hoaxbusters.ciac.org/>
 - ▶ <http://www.vmyths.com>