



## Symbolic

- Presente sul mercato da circa 10 anni
- Specializzata in Network Security
- Partner e distributore italiano di F-Secure Corp.

“La nostra mission è di rendere disponibili soluzioni avanzate per la sicurezza dei computer e delle comunicazioni. La strategia adottata si basa sull'analisi della sicurezza di un sistema informativo, l'offerta di soluzioni pratiche e affidabili, l'informazione e la ricerca.”

Martino Traversa, Founder e CEO

InfoSecurity 2003

## Ambiti Operativi

SYMBOLIC

- Anti-Virus
- IT Risk Mgmt
- PKI
- Content Security
- HSM
- Firewall

INTRINSIC

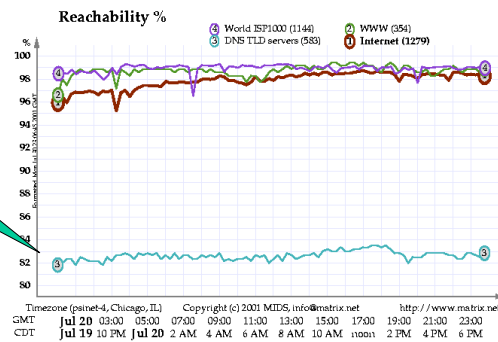
- Security Services
- Area Didattica: Informare

InfoSecurity 2003

# Salto di qualità: Code Red – 19/07/2001

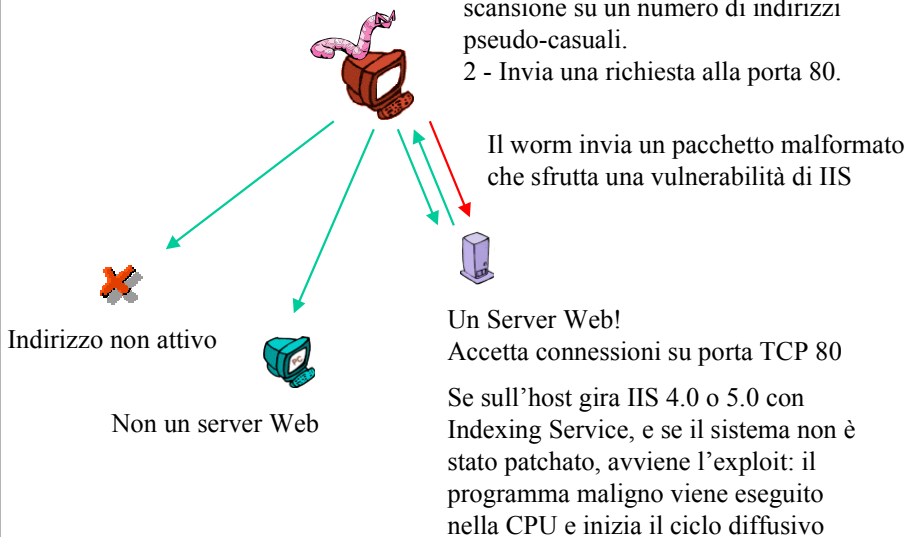
- Con 3 varianti rilasciate tra Luglio e Agosto 2001 è diventato il worm più diffuso al mondo, influenzando il comportamento dell'intera Rete

Indice di raggiungibilità media dei server DNS su Internet (20 Lug. 2001)



## Code Red 1

- 1 - Il computer infetto lancia una scansione su un numero di indirizzi pseudo-casuali.
- 2 - Invia una richiesta alla porta 80.



### Code Red.A (2 var.):

- Esiste solo come processo in memoria
- Non infetta nulla sul disco
- Il generatore di indirizzi casuali non funziona correttamente
- DDoS contro whitehouse.gov
- Defacement
- Propagazione Lineare, usa 99 thread

### Code Red II:

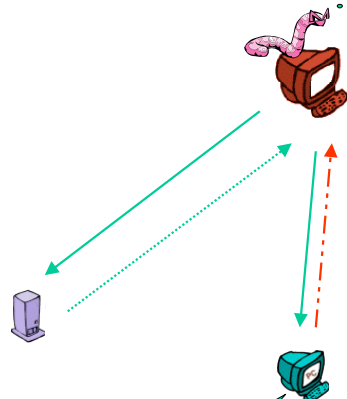
SYMBOLIC

- Scrive file su disco
- Installa una backdoor nel sistema
- I primi due HD sono condivisi e accessibili da Internet
- Propagazione Localizzata, usa fino a 600 thread
  - Con una probabilità di 3/8 scandisce un indirizzo di classe B dallo spazio dell'host infetto
  - Con probabilità 1/2 sceglie un indirizzo di classe A nello spazio dell'host
  - Con probabilità 1/8 scandisce un indirizzo casuale dall'intera Internet

InfoSecurity 2003

## Fattori mitiganti

SYMBOLIC



Ha un indirizzo pubblico, ma non è un server Web. Perciò ogni contatto su porta TCP 80 è uno scan o un worm

Ogni thread di Code Red “aspetta” una risposta dall'host contattato, prima di procedere con l'infezione o scegliere un'altra vittima, e non ha time-out: questo ne ostacola la propagazione se l'host di destinazione risponde lentamente.

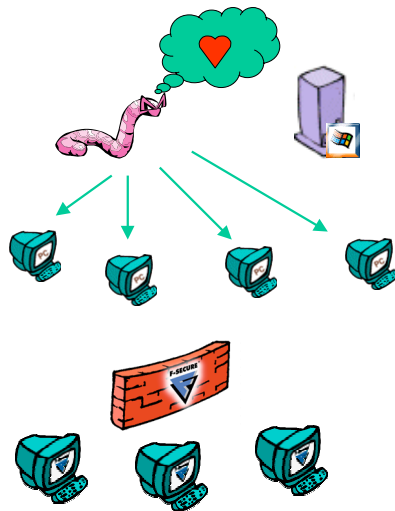
**LaBrea:** un bell'esempio di Judo informatico.

- Un host dedicato con indirizzo IP pubblico ascolta sulla porta 80
- Ad ogni contatto risponde con un acknowledge, ma mantiene l'altra parte in attesa prima che questo possa spedire un pacchetto
- L'attesa è infinita...

InfoSecurity 2003

## Un pericolo solo per i server?

SYMBOLIC



Code Red è stato chiaramente concepito per agganciare i Web server basati su MS IIS 4.0 / 5.0

Tuttavia è in grado di bloccare alcuni modelli di router Cisco non patchati. Inoltre, può generare traffico verso quelle workstation dotate di Personal Web Server che rispondono sulla porta 80.

Spesso, durante le prime decisive ore della diffusione di un nuovo worm, non se ne conosce l'esatta portata. Perché rischiare che un'intera rete di workstation si riveli vulnerabile?

InfoSecurity 2003



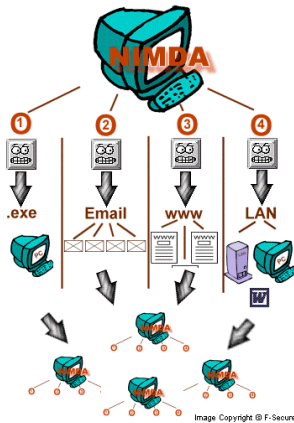
## Nimda, il supervirus – 18/09/2001

SYMBOLIC

- Nimda è il virus/worm che ha portato all'estremo il concetto di multivettorialità
- 4 metodi propagativi:
  - Infezione di file EXE
  - Mass mailing
  - Diffusione via server Web
  - Infezione tramite LAN

InfoSecurity 2003

## Multivettorialità



InfoSecurity 2003

- Infezione degli EXE: Nimda “assimila” gli EXE nel proprio codice. Eseguendo il programma, il controllo passa al virus in modo trasparente
- Nimda spedisce una mail con allegato README.EXE a tutti gli indirizzi trovati tramite il client di posta e nei file HTML
- Il Worm ricerca i server web IIS e sfrutta diverse vulnerabilità per eseguirsi sull’host e modificare le pagine web presenti. Chiunque si colleghi con un browser vulnerabile, viene infettato
- Effetto-trojan mediante RICHED20.DLL su share di rete: aprendo i file DOC e EML da quelle locazioni, si esegue il codice del worm

## Terra bruciata...

- La rimozione di Nimda è complessa e laboriosa
- La macchina è compromessa (dischi condivisi) e molti preferiscono formattare
- Nimda colpisce sia server che workstation
- La propagazione causa notevoli rallentamenti sulle reti

InfoSecurity 2003

## Prevenzione

- Un antivirus aggiornato a tutti i livelli della rete
- Patch sui server IIS
- Patch per Internet Explorer
- Eliminare gli share a livello workstation

## Durante la disinfezione

- E' necessario disconnettere le macchine dalla rete
- ...oppure utilizzare un programma che sia in grado di ottenere lo stesso effetto, magari controllabile tramite una Management Console 😊



## Slapper – 13/09/2002

- Si propaga su server Linux con Apache/SSL
- Ottima scelta di piattaforma: si tratta di una combinazione estremamente diffusa
- Anche in questo caso, exploit non recente
- Sorpresa: i server che implementano SSL non sono necessariamente sicuri e aggiornati

## Ritorno al passato

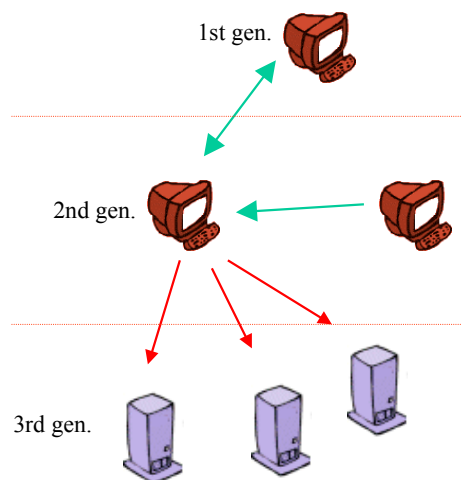
- Slapper si propaga in formato source code (è scritto in C)
- Si compila sull'host infetto, esattamente come lo storico "Morris Worm"
- Tuttavia, visto che sfrutta un Buffer Overflow, è specifico per alcune distribuzioni di Linux

## Private Infected Network

- Slapper è forse il primo worm “new type”
- Le istanze del worm comunicano fra di loro, “propagando” istruzioni
- Mediante la Rete-Slapper è possibile eseguire comandi di shell sulle macchine infette
- L’intuizione, purtroppo, è molto intelligente...

## Private Infected Network (2)

- La nuova istanza del worm si “registra” presso la macchina infettante
- Inizia una scansione random alla ricerca di nuove vittime (fino a 20 tentativi per ogni host che risponde)
- Intanto, si mette in ascolto sulla porta 2002: se riceve un pacchetto UDP, lo analizza per verificare se appartiene ad un’altra istanza di Slapper
- L’host esegue il comando contenuto nel pacchetto ricevuto



## Private Infected Network (3)

- L'host appartenente alla Slapper-Network è in grado di eseguire diverse operazioni:
  - Inviare informazioni ad altri host (uptime, indirizzo, versione)
  - Inviare un pacchetto a tutti gli host raggiungibili della rete
  - Eseguire un comando
  - Lanciare vari tipi di attacco DoS
  - Raccogliere indirizzi email sul disco della macchina infetta e spedirli a un altro host
  - Comunicare la propria esistenza alle altre istanze e ricevere una lista di host infetti

### WORM SPREADING

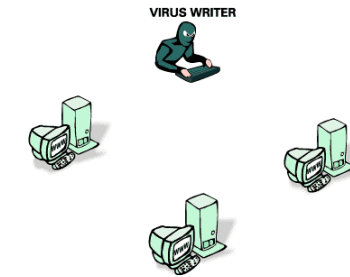


Image Copyright © F-Secure

InfoSecurity 2003

## Punto di forza e tallone d'Achille

- Il concetto di Rete Infetta è la vera novità di Slapper
- Potrebbe ispirare molti altri autori di worm
- Potenzialmente, è un metodo per controllare un numero enorme di host. Se il metodo funziona, la permanenza In-The-Wild è garantita
- L'autore di Slapper non ha pensato a proteggere il suo worm da se stesso
- Visto che è possibile lanciare un comando di shell e "propagarlo" sulla Rete Infetta, è possibile anche uccidere il processo del Worm sugli host contattati
- A giudicare dalla brusca interruzione delle nuove infezioni, alcuni Grey Hat Hacker hanno sfruttato questa caratteristica
- Il procedimento è discutibile sul piano legale e etico

InfoSecurity 2003



## Slammer (alias SQHell, Sapphire, NewSQL Worm etc.) - 24/01/2003

- Secondo alcune fonti, il worm più veloce della storia
- Impossibile sapere con esattezza quando e da dove è iniziata l'infezione
- Caida (www.caida.org) gli attribuisce 75.000 infezioni contro le 350.000 di Code Red
- Non sappiamo in che percentuale le workstation siano responsabili della propagazione

## Speed demon

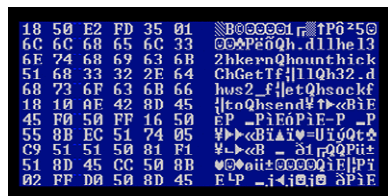


Image Copyright © F-Secure Corporation

- Slammer non usa il TCP, ma l'UDP, che non prevede handshake
- Questo significa che Slammer non ha bisogno di aspettare che un host gli risponda o preoccuparsi di impostare un timeout
- Deve solo inviare il suo pacchetto a quanti più host possibile

## Slamming Italy

### la Repubblica.it

"Sq Hell" in Italia, sarebbe l'attacco informatico più violento  
Infetta i server come un baco, ma non danneggia i file  
**Il virus colpisce le Poste  
in tilt 14 mila sportelli**

ROMA - Promette l'inferno e così oggi è stato, almeno per quanti avevano a che fare con gli uffici postali. Il virus Sq Hell (Inferno Sq) ha bloccato 14 mila sportelli degli uffici postali italiani, portando a segno l'attacco informatico più violento nella storia del nostro Paese. Il problema adesso è risolto, ha detto il responsabile dei sistemi informatici delle Poste, Paolo Baldelli, e domani l'attività riprenderà normalmente. Ma questa mattina sono stati sospesi i servizi online, come Postamat e il pagamento dei conti correnti con il bancomat. Sono invece state pagate regolarmente le pensioni così come sono stati regolati tutti gli altri servizi che non richiedevano l'utilizzo della rete. Pagare i conti correnti è stato invece possibile soltanto in contanti.



InfoSecurity 2003

- Slammer è diventato famoso in Italia per le disfunzioni causate al sistema delle Poste
- Il peggior incidente informatico accaduto nel nostro paese
- Recupero veloce della normale operatività

## Punti deboli

- L'infezione può essere eliminata con un reboot
- Il worm può essere bloccato applicando una patch già disponibile da tempo
- La prevenzione è decisiva per evitare l'attacco di Slammer
- La scansione casuale non è un metodo ottimale:
  - Ridondanza
  - Attacchi diretti contro obiettivi non vulnerabili
- Ogni istanza di Slammer è autonoma e isolata
- Nessun meccanismo di sopravvivenza
- Slammer è velocissimo, ma tatticamente debole

InfoSecurity 2003