

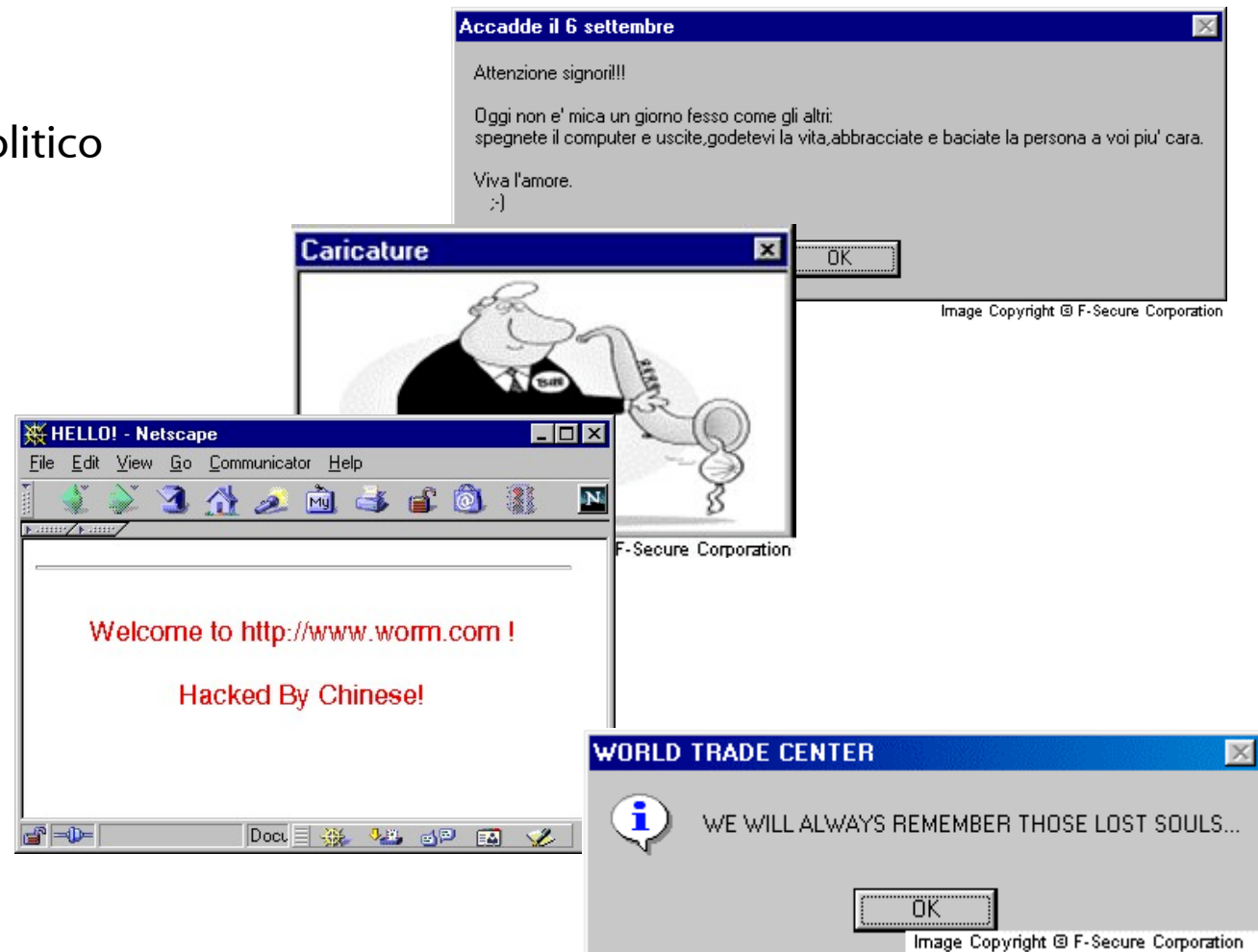
Situazione malware 2002-2003

Fabrizio Cassoni

Content Security Manager - Symbolic SpA

Una delle domande più frequenti

- Perché vengono scritti i virus?
 - Vandalismo
 - Mitomania
 - Attivismo politico
 - Goliardia



Cosa sappiamo dei virus writer

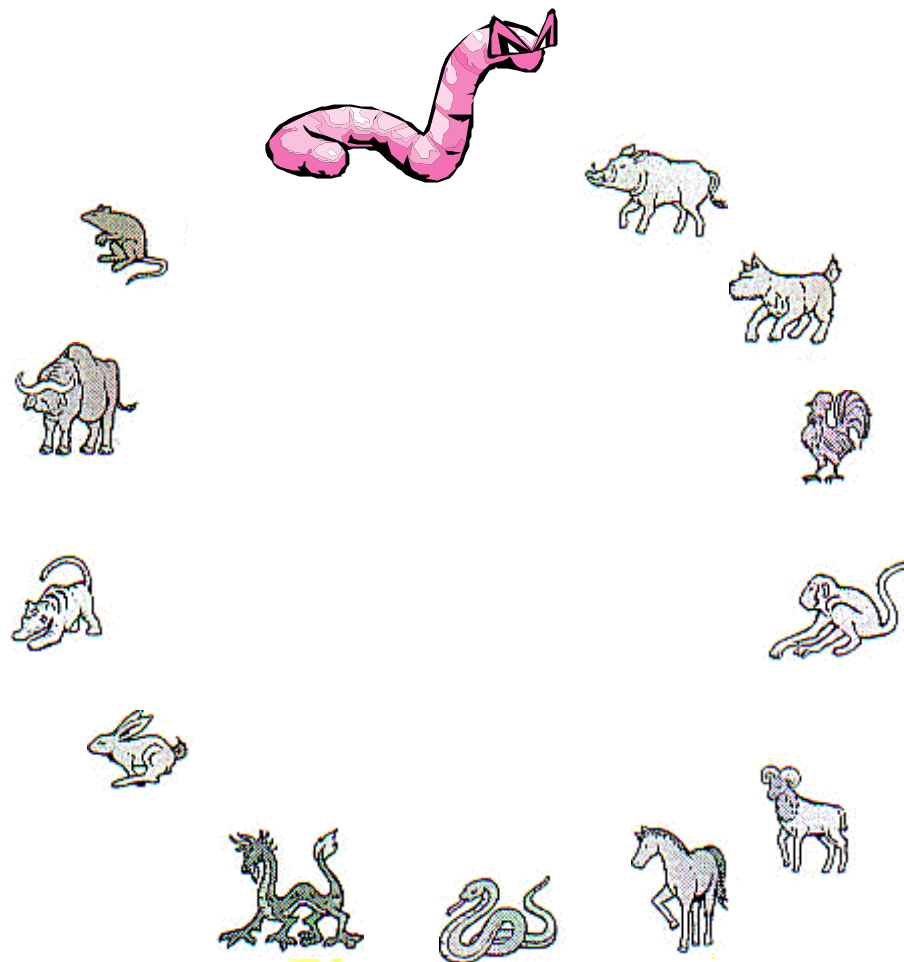
- Occasionalmente, gli autori di virus vengono identificati:
 - David L. Smith (“VicodinES”), ha scritto il macro-virus Melissa a 30 anni. Condannato a 20 mesi di carcere.
 - Chen Ing-Hau, autore di CIH a 24. Ha ammesso la propria responsabilità ma non ha subito condanne.
 - Non è tuttora chiara la posizione del presunto autore di LoveLetter (“Spyder”, 24 anni), in mancanza di una legislazione specifica nel paese di origine. L’accusato era un ex studente di informatica.

Che danni procurano i virus?

- Downtime
- Perdita di produttività
- Distruzione o furto di informazioni
- Perdita di immagine
- LoveLetter (2000): 875 M Euro
- CodeRed (2001): 2620 M Euro
- Slammer (2003): 750 M Euro

2001: l'Anno del Worm

- Il 2001 è ritenuto l'anno nero per la Security:
 - CodeRed
 - Nimda
 - Sircam
- Nel 2000 si pensava di aver toccato un picco irripetibile dopo LoveLetter...



Virus-Worm prevalenti nel 2002

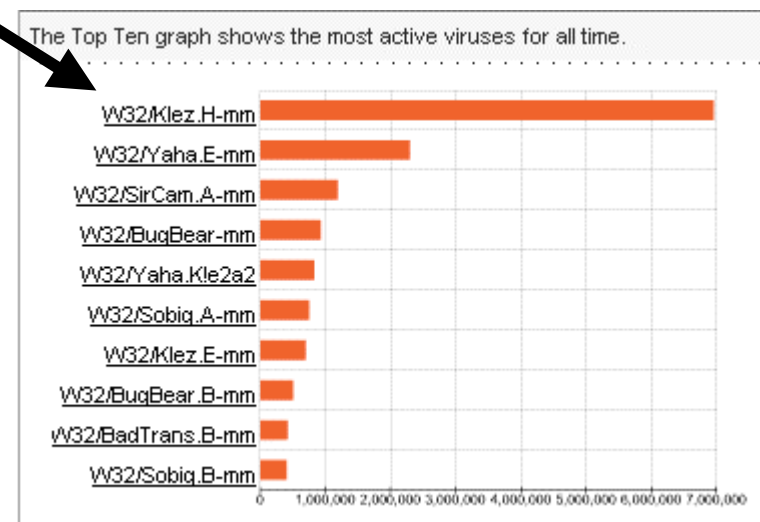
- Il 2002 è stato un anno più tranquillo rispetto al precedente, ma si sono verificati alcuni casi notevoli:
 - Slapper
 - Bugbear
 - Klez.H
 - Yaha.E
 - Yaha.K

Case Study: Klez.H

- E-Mail worm per Win32
- In grado di costruire mail con soggetti e nomi di allegati casuali
- Dropper per il virus Elkern
- Occasionalmente può “travestirsi” da Removal Tool
- Occasionalmente può allegare documenti esistenti alla mail infetta

I numeri di Klez.H

- MessageLabs.com conta 6.964.485 messaggi infetti rilevati finora
- Il mail virus più attivo e longevo di sempre
- La variante H, si è diffusa a partire dal 17 Aprile 2002

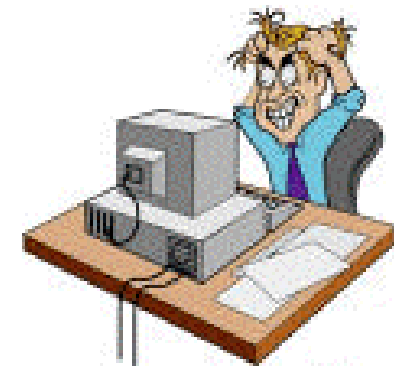


Ragioni del successo di Klez.H

- Infezione di file esistenti con meccanismo “Companion”
- Genera un ampio numero di mail per ogni sistema infetto
- La tipologia di mail (soggetto, testo, allegato) può variare enormemente
- Diffusione tramite share di rete
- Uso dell’ingegneria sociale

Utenti contro...

- L'ingegneria sociale induce molti utenti ad aprire l'allegato, confidando che provenga da una fonte nota
- Il mittente inserito da Klez è falsificato: molti utenti hanno ricevuto flaming ingiustificato da persone che li ritenevano "untori"
- Molte aziende impostano gli antivirus per gateway in modo da rispondere al sender di un messaggio infetto
 - Questo genera ulteriore traffico che congestiona la Rete
 - Spesso il sender è solo quello apparente



Bugbear (Tanatos)

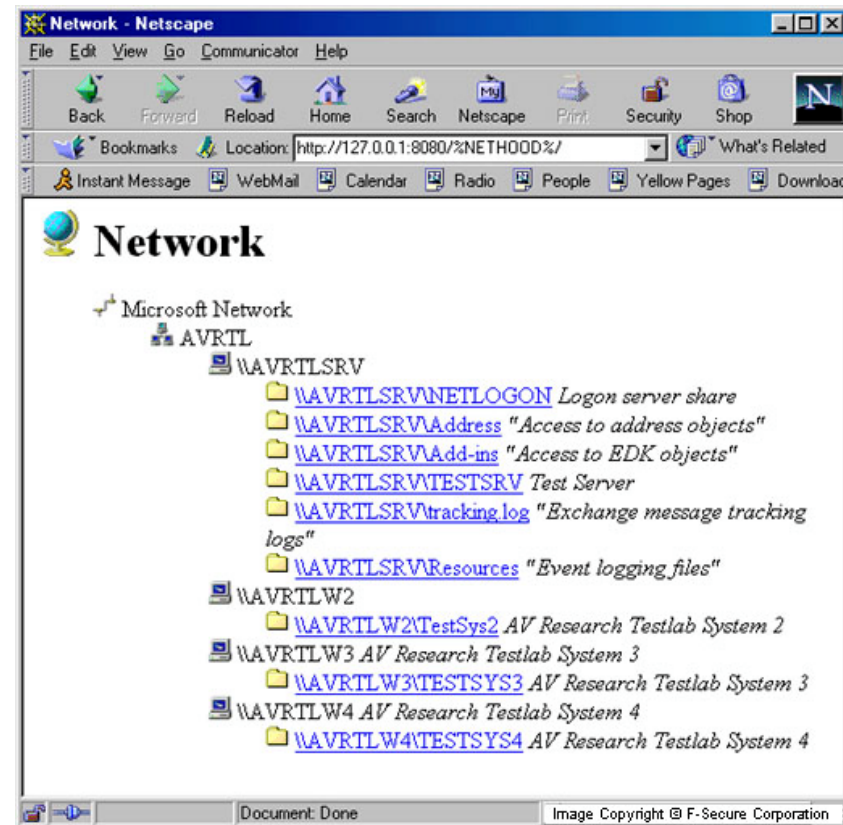
- Come Klez, si diffonde via mail e share di rete
- Come Klez, è in grado di creare e-mail con soggetto e nomi di allegati variabili
- Come Klez, su sistemi non patchati l'allegato può essere eseguito durante la lettura della mail

...inoltre:

- L'indirizzo del sender è falsificato
- Talvolta Bugbear "rispedisce" un messaggio già esistente, col proprio allegato

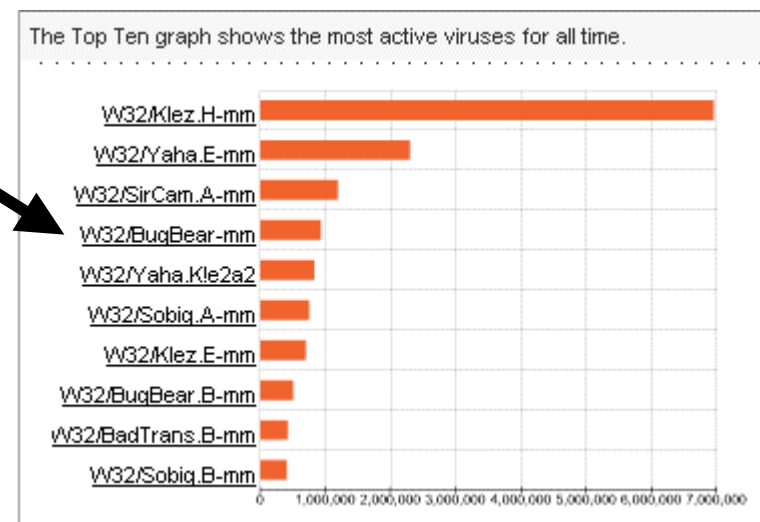
Il worm-spia

- Bugbear contiene una componente keylogger
- Installa una Backdoor sul sistema infetto
- La macchina infetta è perciò compromessa e accessibile via Internet tramite browser



Diffusione di Bugbear

- Secondo MessageLabs, Bugbear ha avuto il suo picco in Ottobre 2002
- 934054 mail intercettate



Slapper

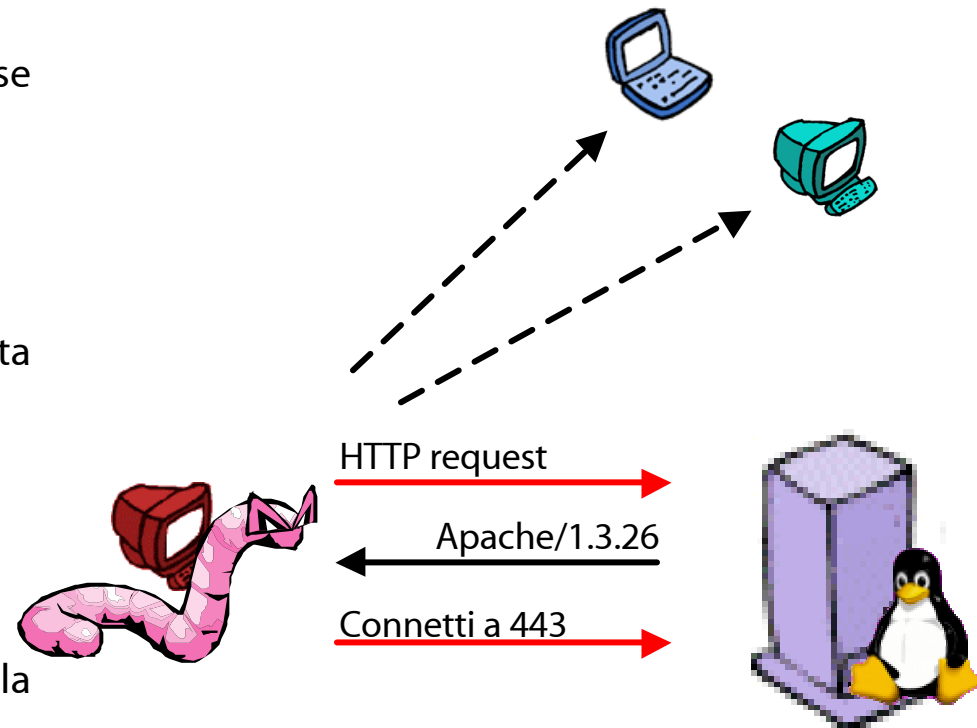
- Uscito Venerdì 13 Settembre 2002
- Scritto in C, gira su piattaforme Linux
- Sfrutta una vulnerabilità delle librerie OpenSSL
- Attacca i server Web basati su Apache con SSL (tipicamente siti di e-commerce, banche ecc.)
- Ispirato ai worm Scalper e CodeRed

Slapper: infezione

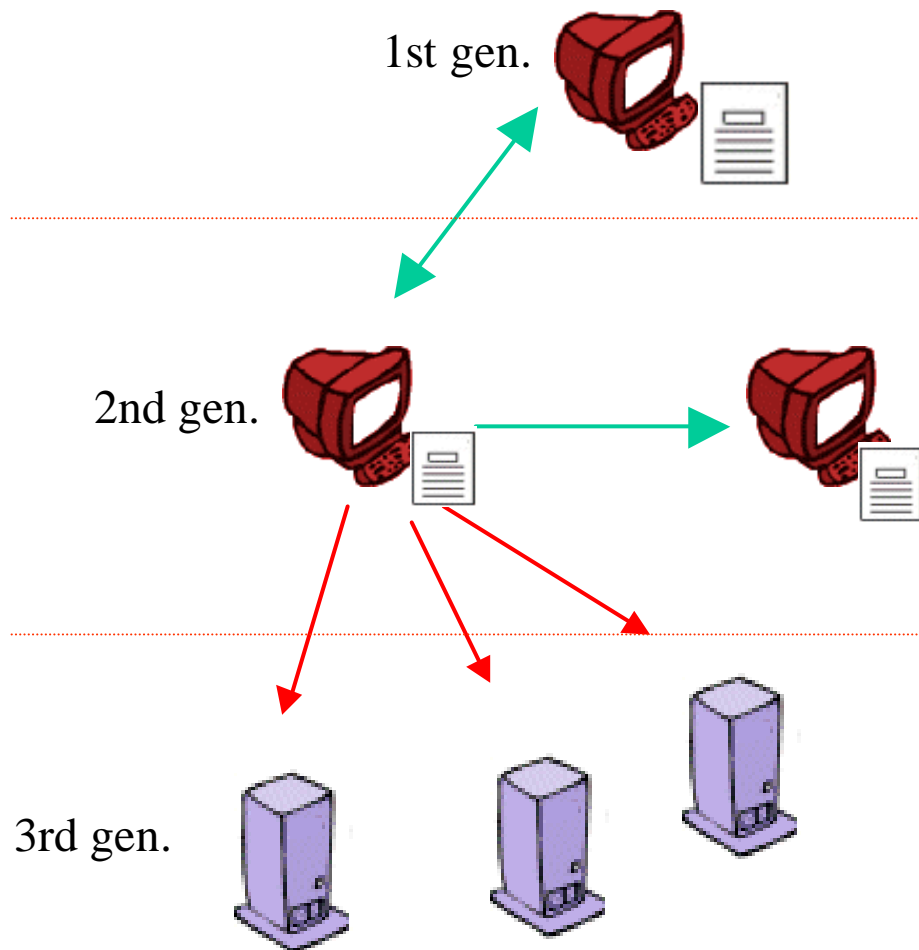
- Come alcuni worm storici (es. Morris Worm), Slapper si propaga in formato sorgente
- La vulnerabilità consente di uploadare un file sull'host e eseguire comandi
 - Slapper deposita il proprio sorgente UUEncondato in una directory
 - Compila il sorgente con GCC
 - Lancia l'eseguibile

Scansione

- Slapper utilizza una scansione sequenziale: sceglie a caso una classe B e ne scandisce tutto lo spazio di indirizzi
- Evita le classi private
- Per ogni host scandito, cerca di effettuare una connessione alla porta 80
- Invia una richiesta HTTP illegale ed analizza la risposta del server per verificare se è Apache e su quale distribuzione di Linux gira
- Slapper apre poi due connessioni alla porta 443 (SSL) e ne utilizza una per iniettare il proprio codice



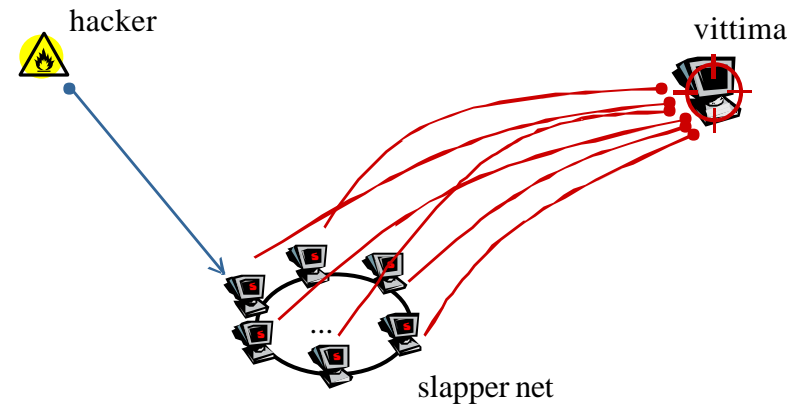
Backdoor



- Slapper crea una backdoor sugli host infetti (protocollo UDP, porta 2002)
- L'host appena infettato invia una notifica alla macchina da cui ha ricevuto Slapper
- La macchina "genitore" registra la presenza del figlio in una tabella
- Per ogni infezione, la presenza di una nuova vittima è notificata a parte delle macchine elencate nella tabella

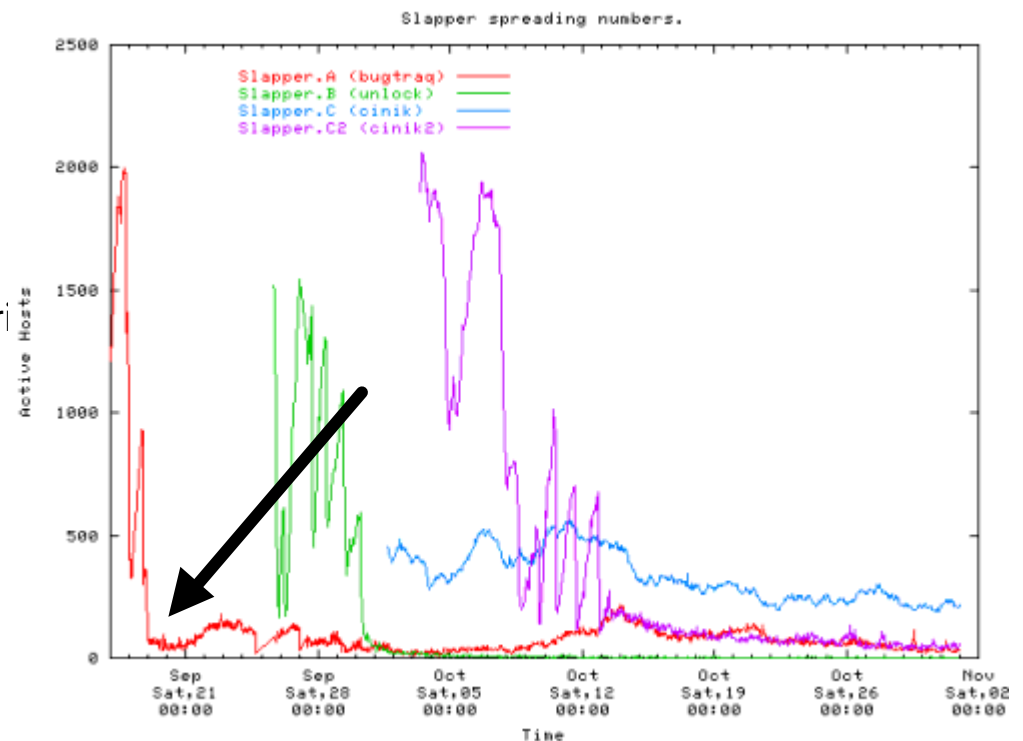
Infected Network

- Ogni istanza del worm “conosce” una serie di macchine infette
- La backdoor forma una rete peer-to-peer tra host infetti e permette di propagare diversi comandi su tutta la rete
- Quando si invia un comando a un host della rete, è possibile fare in modo che venga lanciato a catena su tutte le macchine
- La funzione principale della Slapper Network è di lanciare comandi DDoS
- E' però possibile anche lanciare comandi di shell



Una piccola dimenticanza

- Visto che la Slapper Network accetta comandi di shell e non prevede autenticazione, è possibile usarla contro se stessa
- Basta inserirsi nella rete, lanciare comandi che terminano il processo di Slapper e cancellare i suoi file. L'operazione viene propagata agli altri nodi tramite la rete
- Tecnicamente e legalmente, questo rappresenta un'intrusione su macchine altrui
- Alcuni Grey Hat Hackers lo hanno fatto, determinando la rapida disattivazione della Slapper Network



Altre tendenze del 2002

- Uso costante degli share di rete
 - Gli utenti aziendali hanno l'abitudine di condividere le directory sulle proprie workstation
 - I worm possono facilmente sfruttare questo mezzo per spostarsi tra i client di una rete (es. Opaserv)
- Propagazione sulle reti p2p
 - Diversi worm (Benjamin, Roron, Lolol) si sono diffusi tramite la rete Kazaa
 - E' sufficiente effettuare copie del worm nella directory di condivisione con nomi attraenti perché gli altri utenti si affrettino a prelevarle e lanciarle
- La diffusione delle connessioni always-on ha favorito gli attacchi contro i computer degli home users
 - Se il PC di un utente tipico è un pentium III con una connessione permanente ad Internet e un disco da diversi Giga, per un Hacker non è più necessario cercare di compromettere dei server ben protetti allo scopo di installare ad esempio una chatroom

Il 2003 finora

Fino ad oggi abbiamo osservato:

- Un limitato numero di incidenti
- La qualità e la diversità degli attacchi si innalzano
- L'Italia sembra più colpita che in passato
- Allarme per il possibile connubio tra e-mail worm e spam

Slammer (Sapphire, SQHell)

- Uscito il 24/01/2003
- Secondo Caida.org ha raggiunto le 75.000 infezioni contro le 350.000 di CodeRed
- Il risultato è impressionante, visto che ha come target i server SQL, meno diffusi dei server Web
- Forse il worm più veloce in assoluto

Slammer in breve

- Si propaga tramite i server SQL 2000 e MSDE
- Sfrutta una vulnerabilità nota da tempo per eseguire il suo codice sull'host di destinazione
- Nessun payload distruttivo, ma altissimo consumo di risorse
- Il codice è estremamente breve e scritto in Assembly
- Molte applicazioni incorporano l'engine SQL, anche sui desktop
- Molti utenti non ne sono al corrente

Speed Freak

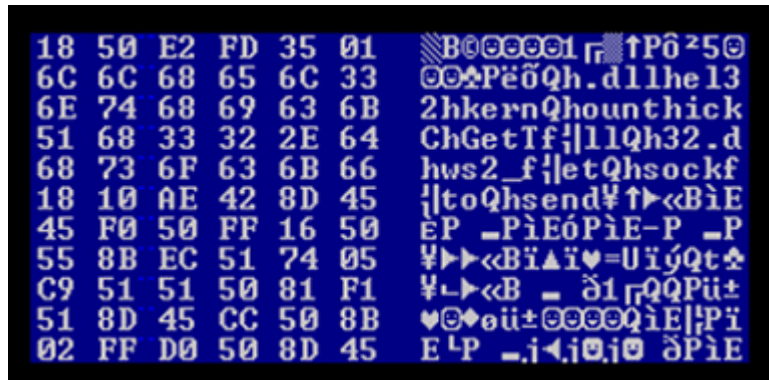


Image Copyright © F-Secure Corporation

Il meccanismo di scansione gli consente di contattare anche indirizzi di broadcast
 In questo modo, cerca di contattare tutte le macchine su una rete, generando traffico

Slammer non usa il TCP, ma l'UDP, che non prevede handshake
 Questo significa che 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
 Ciò lo rende più veloce di CodeRed e insensibile alle trappole come LaBrea

2Fast 2Furious

- Molti osservatori hanno registrato un intervallo di 5 minuti tra i primi report e la diffusione pandemica di Slammer
- Sembra una performance eccessiva, considerato che Slammer usa una scansione casuale
- E' possibile però che il primo stadio infettivo sia stato effettuato con una hitlist

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 regolari tutti gli altri servizi che non richiedevano l'utilizzo della rete. Pagare i conti correnti è stato invece possibile soltanto in contanti.



Slammer ha guadagnato gli onori delle cronache per le disfunzioni causate al sistema delle Poste Italiane

E' stato il peggior incidente informatico accaduto nel nostro paese finora

Veloce ma fragile

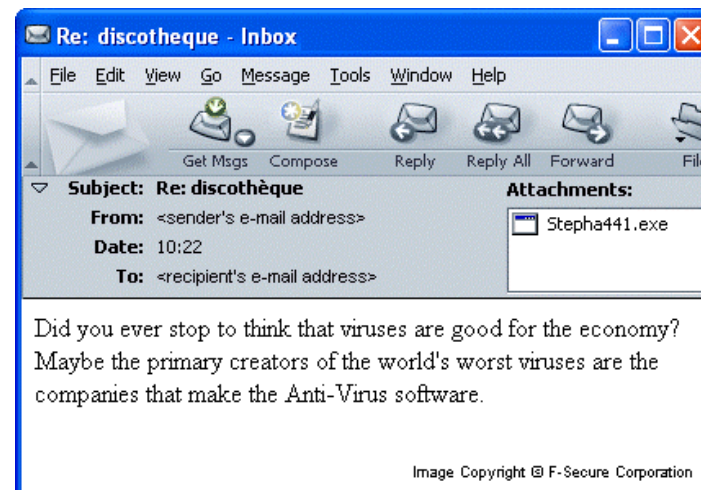
- Slammer esiste solo come processo in memoria → • Può essere eliminato con un reboot
- Usa una scansione casuale → • Non è un metodo ottimizzato (ridondanza)
- Il codice è molto breve → • Non ha feature che gli consentano sopravvivenza e non ha payload

Fizzer

- Fizzer è un mail/p2p Worm complesso e ricco di funzioni, tra cui:
 - capacità di auto-aggiornarsi
 - modulo per il keylogging
 - server HTTP
 - DoS tool
 - IRC backdoor
 - capacità di retrovirus

Diffusione via mail

- Fizzer ricava gli indirizzi a cui spedirsi dal Windows Address Book e dalla rubrica di Outlook
- Costruisce un falso indirizzo di provenienza utilizzando un lungo elenco di nomi contenuti nel proprio codice
- Dalla stessa lista ricava blocchi di testo con cui crea soggetto, testo e nome dell'allegato della mail
- Il nome dell'allegato può essere preso da un file su disco



- Fizzer inoltre può cercare indirizzi a cui spedirsi in vari tipi di file su disco, es. la cache del browser, la cartella dei cookies, la cartella personale dell'utente

Diverse Backdoor



- Fizzer installa una backdoor per il server AOL
- Cerca di connettersi a vari server IRC per registrarsi come "bot" e accettare comandi remoti
- Inoltre ascolta su 4 porte distinte, accettando comandi e permettendo trasferimenti di file
- Installa un server web per fornire un ulteriore accesso all'host infetto

Altre feature

- Infezione tramite la rete Kazaa
 - Il worm copia i propri file nella cartella condivisa del client per indurre altri utenti a prelevarli e lanciaarli
 - Fizzer contiene un keylogger:
 - può essere usato per rubare password, numeri di carte di credito ecc. sul computer infetto
 - Come già altri worm prima di lui, Fizzer è auto-aggiornante
 - Può aggiungere a se stesso altri moduli prelevati da alcuni siti web per aumentare le proprie capacità
 - Fizzer è un retrovirus:
 - E' in grado di bloccare i processi di alcuni antivirus
 - DoS:
 - Fizzer può effettuare attacchi DoS contro obiettivi scelti da un hacker che si connetta da remoto alla sua backdoor
- ...fortunatamente la diffusione di Fizzer non è durata a lungo. Il picco è stato il 12 maggio, ma dopo le 100.000 infezioni iniziali il worm ha rallentato vistosamente.

Serial Virus Writers

- Le varianti di uno stesso ceppo virale vengono spesso rilevate a mesi di distanza tra loro e a ritmo irregolare
- Raramente sembra esserci una vera strategia nella pubblicazione del malware
- Può però succedere che un virus writer si appassioni al proprio lavoro e produca nuovo malware con continuità
- Il caso Sobig

Sobig.A

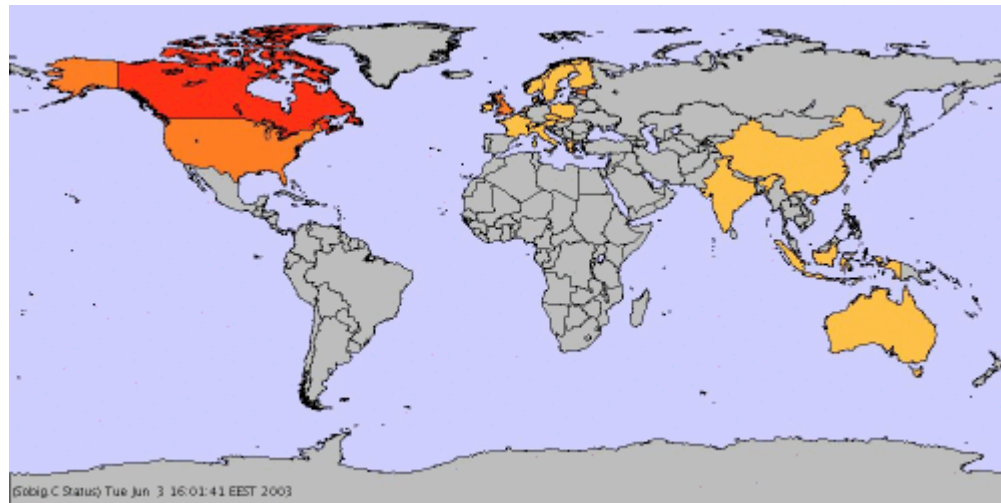
- Sobig.A è il tipico e-mail worm, che usa un indirizzo falsificato ma fisso e un allegato eseguibile dalla doppia estensione
- Si propaga anche sugli share di rete
- E' in grado di prelevare un modulo backdoor da un sito web
- Molto diffuso
- Uscito il 9 gennaio 2003

Sobig.B (alias Palyh)

- Il 18 maggio viene scoperta una variante di Sobig
- Le funzionalità di base sono simili alla prima variante
 - Massmailer
 - Diffusione su share
 - Capacità di prelevare e eseguire codice da siti web
- Il falso indirizzo di provenienza è diverso (support@microsoft.com)
- Questa variante diventa estremamente diffusa in tutto il mondo
- Il worm si auto-disattiva il 31 maggio 2003
- Dopo quella data, smette di propagarsi

Sobig.C

- Fra il 31 maggio e il 1 giugno viene rilevato Sobig.C
- Funzionalmente simile agli altri due
- Stavolta l'indirizzo del sender è variabile
- Il worm usa indirizzi ricavati dalla macchina infetta, oppure completamente inventati
- Molto diffusa, anche questa variante ha una data di disattivazione: 8 giugno
- Dopo quella data, non spedisce email e non attacca gli share



Sobig.D

- L'uscita di una variante D non fu una sorpresa
- Rilevata il 18 giugno
- Molto simile alla variante C, usa però l'indirizzo fisso admin@support.com come mittente
- Per auto-aggiornarsi, questa variante si mette in ascolto su diverse porte attendendo istruzioni remote (in forma di URL) dal suo creatore
- Si disattiva il 2 Luglio
- Poco diffusa, è la pecora nera della famiglia Sobig

Sobig.E

- Per ora, l'ultima puntata del serial Sobig
- Uscito il 25 giugno
- Il codice è più complesso dei precedenti, ma le funzionalità di base sono le stesse
- Stavolta l'allegato è zippato
- Il sender può essere support@yahoo.com oppure un indirizzo ricavato dal sistema infetto
- Una volta attivo, si mette in ascolto su diverse porte: attende che gli vengano passati URL di moduli aggiuntivi
- Si disattiva il 14 luglio

Le puntate del Serial

Sobig.A	inizio: 9 gennaio fine: mai	Sobig.D	inizio 18 giugno fine: 2 luglio
Sobig.B	inizio 18 maggio fine: 31 maggio	Sobig.E	inizio: 25 giugno fine: 14 luglio
Sobig.C	inizio: 1 giugno fine: 8 giugno		

Bugbear.B

- L'incidente virale più serio del 2003
- Virus/Worm polimorfico
- Nomi di sender e allegati variabili
- Diffusione via mail e share di rete
- Retrovirus (attacca antivirus e personal firewall)
- Keylogger
- Backdoor (non autenticata, chiunque può connettersi)
- E' particolarmente "cattivo" con le banche: cerca di spedire le password salvate in cache via mail se il dominio della macchina appartiene a una banca

Worm e Spammer?

- Abbiamo visto come diversi Worm contengano backdoor di vario genere
- E' possibile usarli per attaccare altre macchine, ma è da diverso tempo che non si verificano incidenti importanti legati al DDoS
- E' possibile che i Worm vengano usati per scopi diversi?

Ad esempio, un host sotto controllo remoto potrebbe essere usato per inviare Spamming, facendo ricadere la colpa sull'utente legittimo.

Tuttora non sappiamo molto sugli Spammer.

Teorie e scenari

- I worm più aggressivi, come CodeRed e Nimda, scandiscono attivamente Internet alla ricerca di nuovi “ospiti”
- Quest’operazione viene spesso fatta in modo localizzato, ossia scegliendo uno spazio di indirizzi prossimo a quello dell’host appena infettato
- Altri worm usano una scansione completamente casuale, su indirizzi IP generati a runtime
- Teoria e evoluzione dei “Warhol Worms” (da Nicholas C. Weaver)

Scenari

- E' possibile costruire un worm più veloce di Code Red, Nimda o Slammer?
 - La velocità di propagazione dipende da quanti host si riescono a contattare nel minor tempo possibile successivo all'infezione, prima che le difese entrino in azione
 - La scansione casuale (es. Slammer) implica duplicazione, quando più host infetti si mettono a scandire gli stessi indirizzi
 - Specialmente nel caso di worm che usano il TCP, la scansione casuale comporta una perdita di tempo quando il worm fa il probing di indirizzi non validi, non vulnerabili, irraggiungibili, ecc.
 - La scansione localizzata non può coprire tutto lo spazio della Rete
 - Ma ci sono altri metodi...

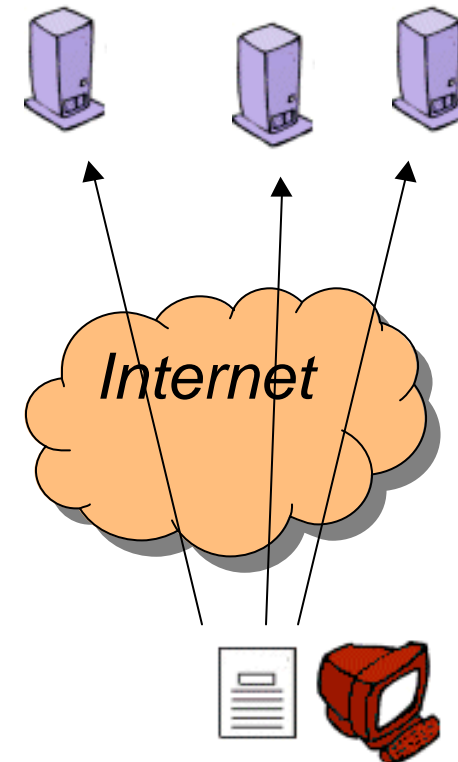
Hitlist

Agenda per un ipotetico worm anti-server web:

- Si ottiene una lista di server web potenziali vittime (es. tramite Netcraft)
- Si rilascia un worm contenente la lista in formato compresso
- Il Worm scandisce gli indirizzi della lista e poi inizia un random scanning

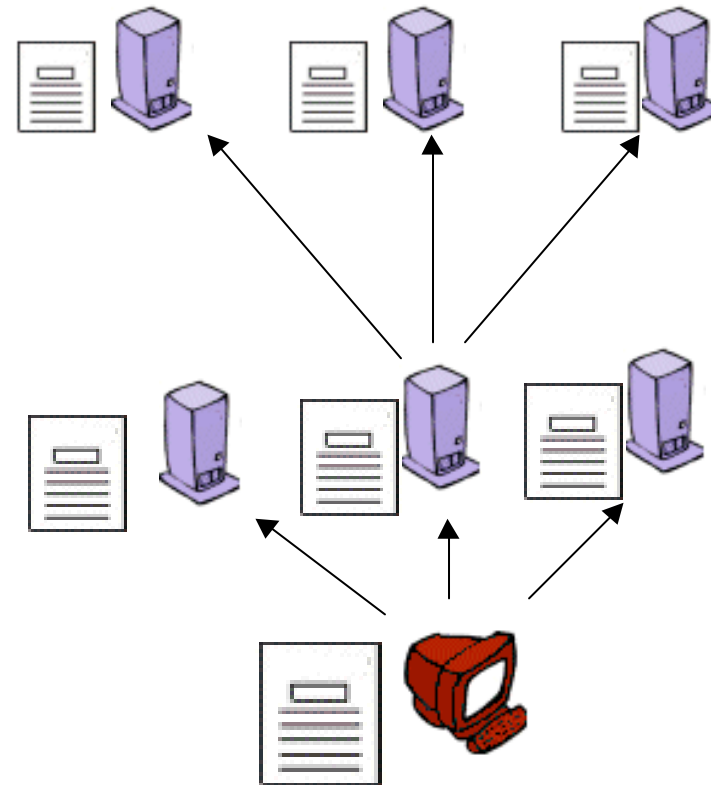
Svantaggi:

- Se la lista fosse uguale per tutte le istanze del worm, gli stessi indirizzi verrebbero contattati più volte e il worm perderebbe tempo
- La prima diffusione sarebbe sicuramente rapida, forse il worm non avrebbe vita lunga
- Gli amministratori dei server contattati più volte si accorgerebbero presto del traffico anomalo



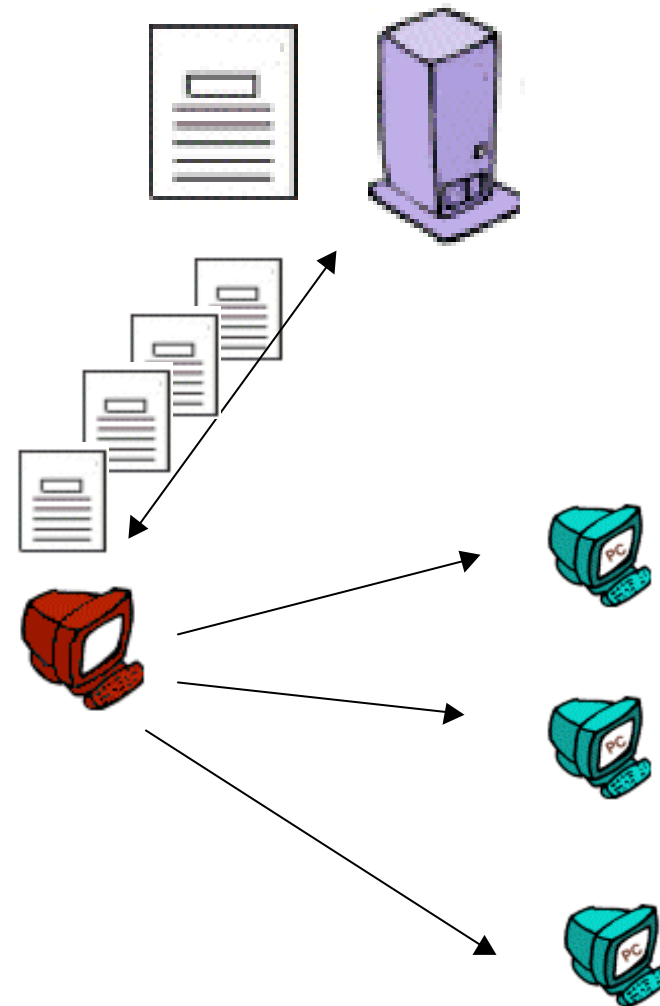
Hitlist migliorata

- La prima istanza del worm contiene la lista intera (compressa), ma ne processa solo una parte
- Ogni host infettato successivamente riceve una porzione della lista, con parziale sovrapposizione
- La seconda generazione di host infetti ripete la procedura, rilasciando a sua volta una ulteriore porzione della lista
- In questo modo un numero inferiore di potenziali vittime viene contattato più di una volta e il worm può tentare più host in meno tempo prima di passare al random scanning
- Meno "rumore"
- Non è un metodo error-free; se un ramo viene interrotto, molte potenziali vittime potrebbero non venire mai contattate



Hitlist centralizzata

- Un server ad alte prestazioni, accessibile via Internet, pubblica una lista enorme di indirizzi
- La prima generazione di worm viene propagata con una hitlist minima
- Dopo l'infezione, il worm si collega al server, preleva una porzione della lista e comincia a scandire gli indirizzi
- Ogni infezione successiva invia una query al server per ottenere un blocco della lista da processare
- Ma attenzione a non generare troppe richieste, altrimenti occorreranno più server!



Sopravvivenza del Worm

- Dopo essersi diffuso, il nostro ipotetico worm potrebbe auto-upgradarsi per cercare di sfuggire alla rilevazione e per aggiungere funzionalità
- “Rubiamo” l’idea di Hybris: plug-in scaricati da diversi siti Web controllati da noi
- Facciamo in modo che vengano accettati solo plug-in firmati elettronicamente per evitare che qualcuno inquina il nostro worm
- I moduli ci permettono di poter espandere le capacità del nostro worm, ad esempio con funzioni Retro-Virus per disattivare gli AV o rendere più difficile il patching del sistema.
- Potremmo aggiungere funzionalità di RAT per prendere il controllo delle macchine infette
- Potremmo far eseguire compiti specifici alle macchine controllate, come attacchi DDoS oppure spedire spamming via mail

Il ritorno della Infected Network

- Altra ipotesi: sviluppiamo l'idea di Slapper
- Ogni host infetto originale riceve una lista delle infezioni "figlie" (basta che inviino un installation check all'host da cui proviene il worm e che quest'ultimo salvi i loro indirizzi in un file)
- Ogni host infetto di seconda generazione conosce l'indirizzo della macchina che lo ha infettato e mantiene una lista di quelle da lui infettate
- Inoltre, il worm potrebbe memorizzare l'indirizzo di macchine da cui riceve un probing e che quindi sono verosimilmente infette
- Intanto che il Worm si diffonde, ogni istanza "conosce" altri host infetti sulla rete

Il Worm socievole

- Con le istanze del worm che comunicano fra di loro, abbiamo il Kazaa del malware
- Come Slapper, il nostro Worm “propaga” comandi e istruzioni su tutti gli host della rete...
- ...però ricordiamo di implementare l'autenticazione, in modo che solo noi possiamo prendere il controllo della Infected Network
- In modo simile a Bymer potremmo ad es. usare gli host per fare distributed computing
- Se gli host infetti si scambiassero fra di loro i nuovi plug-in, non avremmo bisogno di usare dei server Web che potrebbero essere smantellati o che potrebbero ricondurre a noi
- Anche in questo caso, ci troveremmo ad avere il controllo di una vasta rete di macchine che potremmo usare per attacchi distribuiti o Spamming su vasta scala

Difese

Che difese abbiamo contro Virus e Worm iperveloci? Ecco qualche idea:

- Misure preventive
 - Antivirus aggiornati
 - Firewall (Corporate e Personal)
 - Sistemi aggiornati con le patch corrette
 - Policy efficaci e adatte al nostro ambiente di lavoro
- Misure attive
 - Aggiornamenti automatici e efficienti per gli AV
 - Tiger Teams pronti a intervenire negli ambienti Corporate più complessi
- Educazione degli utenti
 - Fattore decisivo nel caso dei mail worm

Grazie per l'attenzione!