Un anno di virus

di Stefano Toria (MC0170 su MC-link)

Con questo articolo, la rubrica «Virus» compie un anno. Vogliamo celebrare questa «occasione» ripercorrendo alcuni dei fatti salienti che si sono verificati in questo periodo nel settore della sicurezza informatica

Fuori l'autore!

Chi ha seguito queste colonne è senz'altro a conoscenza di un fatto, che abbiamo ripetuto più volte: è praticamente impossibile identificare l'autore di un virus. O meglio: era praticamente impossibile, prima che in questi ultimi tempi una serie di coincidenze tra ingegnose investigazioni e circostanze fortunose portassero alla scoperta di alcuni creatori di programmi maligni.

Ottobre: quattro virus per il Macintosh

La Polizia dello Stato di New York ha identificato e catturato l'autore di quattro virus per il Macintosh. L'autore dei virus, il cui nome non è stato comunicato, ha ammesso di aver creato i virus MDEF, MDEFB e CDEF, tutti ben noti ai ricercatori, oltre a una ulteriore variante di MDEF che non è mai stata rilasciata.

L'autore è stato identificato grazie alle investigazioni di Mark Anbinder, uno specialista di Ithaca, New York. L'autore dei virus sembra fosse uno studente delle locali scuole medie superiori.

Per una particolare coincidenza Ithaca è il luogo da cui Robert T. Morris ha attivato il celebre «verme» sulla rete Internet nel novembre 1988.

Gennaio 1991: Joseph Popp rischia l'estradizione

Molti lettori rammenteranno l'eco che ebbe, anche sulla stampa d'informazione, la diffusione su scala mondiale di un dischetto che apparentemente conteneva un programma di prevenzione dell'AIDS, ma che in realtà era in grado di danneggiare il contenuto del disco fisso del computer su cui veniva installato. Il foglietto che accompagnava il disco invitava inoltre a versare una consistente somma di denaro (oltre $300) a una non meglio identificata «PC CYborg Corporation» con sede in Panama, per ottenere un ulteriore disco contenente la chiave per ripristinare i dati danneggiati.

Il 1 febbraio dello scorso anno fu arrestato negli Stati Uniti un tale Joseph L. Popp, uno zoologo residente nell'Ohio. Poiché il caso dei dischetti «AIDS» fu portato all'attenzione della Polizia britannica, e le indagini furono avviate da quest'ultima, a seguito del suo arresto Popp avrebbe dovuto essere estradato in Gran Bretagna sotto l'accusa di ricatto ed estorsione.

Nel 1991 cresce il numero dei BBS dedicati alla prevenzione dei virus. Nella foto la schermata di apertura di «Excalibur!», uno tra i più noti di tali sistemi.

Analisi di un virus: Dark Avenger

«Dark Avenger», il «Vendicatore Oscuro»: nella foto è visibile il dump di un programma infetto da questo virus.

Iniziamo da questo numero l'analisi di alcuni tra i più noti e pericolosi virus conosciuti. Non è nostra intenzione fornire informazioni utili a chi si proponga di sviluppare nuovi virus, quindi i dettagli forniti saranno sufficienti alla comprensione del comportamento del virus ma non a replicarne le funzioni.

Il Dark Avenger è un virus parassita residente: agisce attaccando una copia di se stesso ai file .EXE e .COM, purché siano di lunghezza superiore a 1775 caratteri, e una volta che il programma viene eseguito una parte del virus rimane residente in memoria per infettare qualsiasi altro file .EXE o .COM venga eseguito, letto, aperto, chiuso o cambiato di nome. Il virus intercetta così praticamente qualsiasi funzione che agisca direttamente su un file, il che lo rende estremamente infettivo e pericoloso.

I sintomi della presenza del virus non sono visibili; tuttavia durante l'esecuzione di un programma infetto in un caso su sedici il virus analizza il disco da cui è stato prelevato il programma, sceglie un settore a caso e vi sovrappone caratteri anch'essi casuali, distruggendone il contenuto originario.

(Nota: un utente inesperto può essere indotto a ritenere che un virus che modifichi un solo settore per volta sia meno dannoso di uno che distrugga l'intero contenuto del disco. In realtà è vero l'esatto opposto. Infatti un programma che modifichi poco alla volta il contenuto del disco può passare inosservato per un periodo di tempo sufficiente a rendere praticamente impossibile la ricostruzione di un insieme corretto di dati; per contro la distruzione totale dell'intero contenuto del disco è talmente macroscopica da non poter passare inosservata, e se l'utente ha eseguito correttamente le operazioni di backup potrà rapidamente ripristinare il contenuto del disco, con una perdita minima di informazioni, e sarà inoltre avvertito della presenza di un virus, cosicché potrà provvedere a una immediata e radicale disinfezione del proprio elaboratore).

Il virus Dark Avenger si attiva e si trasmette nel momento in cui viene eseguito un programma infetto. La prima cosa che provvede a fare è verificare se una copia di se stesso è già presente in memoria. A tal fine prende in esame la parte offset del vettore INT 21H: se contiene qualsiasi valore all'infuori di 02EE procede con l'infezione; se contiene 02EE avvia una scansione della RAM per verificare se effettivamente una copia del proprio TSR è presente in memoria.

Se il Dark Avenger stabilisce che non è presente in memoria, rilascia il blocco corrente di RAM e richiede due blocchi, uno per il programma corrente, e l'altro (lungo 3680 byte) posizionato nella parte alta della memoria disponibile. Quest'ultimo blocco, destinato a contenere il codice del virus, viene nascosto. Il virus si trasferisce quindi nel blocco acquisito, si aggancia all'INT 21H e all'INT 27H e trasferisce il controllo al programma infettato.

È a questo punto che può verificarsi il danno. Infatti, ogni volta che viene eseguito un programma infetto viene incrementato un contatore; quando il valore raggiunge 0F viene riportato a 0, il virus identifica un settore nell'area dati del disco da cui è stato prelevato e lo ricopre. Per determinare da quale disco proviene, il virus esamina il parametro argv[0] e ne preleva il primo carattere.

Nella versione 3.0 del DOS e nelle successive, il parametro contiene il percorso completo del file da cui il programma è stato caricato. Nelle versioni precedenti non è così, e il comportamento del virus diviene imprevedibile.

Le due routine di controllo degli interrupt hanno il compito di mantenere il virus vivo e attivo in memoria (INT 27H) e di infettare altri programmi (INT 21H). Ci soffermeremo brevemente su quest'ultima funzione. Come è noto a chi conosca il funzionamento interno del DOS l'INT 21H consente, a mezzo di codici di funzione, di richiedere diversi servizi al sistema operativo. Alcune di queste operazioni vengono intercettate nel seguente modo:

AH=25 (Set interrupt vector): se un programma chiama l'INT 21H per ottenere il controllo dello stesso INT 21H o dell'INT 27H, il Dark Avenger trattiene l'indirizzo del nuovo vettore di interrupt in una variabile e restituisce il controllo al programma chiamante, mantenendo per se stesso il controllo dell'interrupt.

AH=35 (Get interrupt vector): un programma può chiedere informazioni sul valore corrente del vettore di interrupt per l'INT 21H o l'INT 27H; in questo caso, Dark Avenger restituisce il valore memorizzato in precedenza.

AH=4B00 (Load/execute program): Dark Avenger infetta qualsiasi programma venga eseguito.

AH=3C o AH=5B (Create file): se il file creato è un .COM o un .EXE, il virus trattiene in una variabile lo handle del file e pone a 1 un flag.

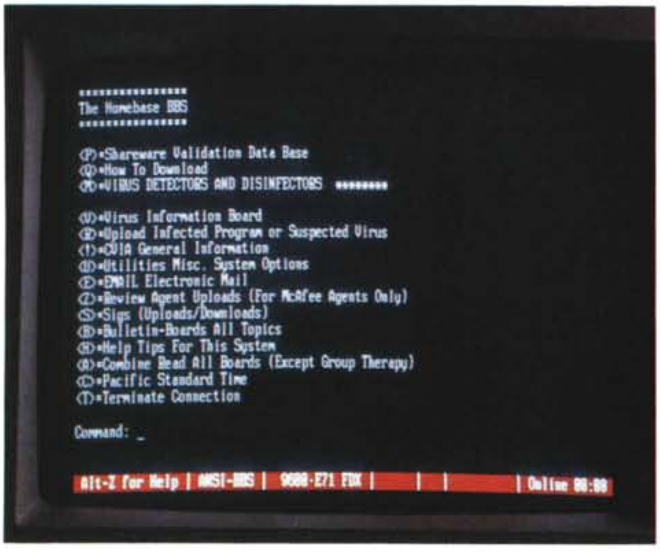
AH=3E (Close file): se il numero dello handle corrisponde a quello precedentemente archiviato, il virus infetta il file.

AH=3D (Open file), AH=43 (Chmod), AH=56 (Rename): in tutti e tre i casi, la richiesta della rispettiva funzione su un file .COM o .EXE ne determina l'infezione. Questa è la caratteristica più pericolosa del file: infatti, se l'utente ignora la presenza del virus in memoria ed esegue un programma di scansione per controllare se i propri programmi sono infetti, DETERMINA L'IMMEDIATA, TOTALE INFEZIONE DI TUTTO IL SISTEMA.

Un'analisi dei valori ASCII del corpo del virus rivela tre stringhe di caratteri, che hanno valso al programma il suo nome (Dark Avenger) e l'altro nome con il quale è noto (Eddie). Infatti negli ultimi byte del programma è contenuta la scritta «This program was written in the city of Sofia (C) 1988-89 Dark Avenger»; inoltre si trovano anche le frasi «Eddie lives... somewhere in time!» e «Diana P.». «Eddie» sembra riferirsi al simbolo del gruppo heavy metal «Iron Maiden», che nel luglio 1986 ha pubblicato l'album «Somewhere in Time». Non si sa chi sia Diana P.

Una lezione da non dimenticare

Dall'analisi del comportamento di Dark Avenger si trae la conferma di quanto più volte abbiamo ripetuto, e cioè che è importante disporre di un disco di sistema certamente privo di infezione e contenente una copia certificata di una versione recente di un programma di scansione. Infatti l'esecuzione di un programma di scansione, se è presente in memoria il Dark Avenger, causa più danno di quanto ne avesse fatto fino a quel momento lo stesso virus. In ogni caso è importante servirsi di un programma che sia in grado di rilevare la presenza del virus in memoria, e lasciare che come prima operazione venga eseguito il controllo della memoria.



«The Homebase BBS», il sistema telematico di John McAfee. I programmi antivirus prodotti da questo ricercatore sono stati fatti segno di diversi «hackeraggi».

Nel gennaio di quest'anno il giudice distrettuale Ann Aldrich ha accolto la richiesta di estradizione di Popp, rimettendo i documenti al Dipartimento di Stato per la ratifica della sentenza. Popp verrà quindi trasferito in Gran Bretagna, dove verrà processato e potrà essere condannato all'arresto fino a quattordici anni per ciascuno dei casi denunciati di ricatto ed estorsione.

Febbraio: Popp e Den Zuk(o)

A seguito del parere favorevole del Dipartimento di Stato, Joseph L. Popp viene trasferito in Gran Bretagna per essere processato.

Nello stesso periodo, una ingegnosa investigazione di Fridrik Skulason porta alla identificazione dell'autore del virus «Den Zuk», il cui nome si scopre in realtà essere «Den Zuko». Ne abbiamo parlato nel numero 108 di MCmicrocomputer (giugno 1991).

Maggio: Tequila in Svizzera

Il 20 maggio 1991 la Polizia svizzera ha arrestato due giovani di 18 e 21 anni nel villaggio di St. Hausen. I due ragazzi sono accusati di essere gli autori del virus «Tequila». Questo virus, identificato in diverse località europee, risulta essere stato scritto avvalendosi di molte tecniche già utilizzate da altri virus, e descritte in alcune pubblicazioni specializzate.

Come già si era verificato nel caso del «verme» della rete Internet, il cui autore Robert T. Morris è figlio di uno dei principali consulenti del Governo degli Stati Uniti per la sicurezza informatica, anche nel caso del virus «Tequila» è in gioco una sorta di conflitto tra padre e figlio: uno dei due giovani arrestati è infatti il figlio del titolare di un'impresa di distribuzione di shareware, e sembra che alcuni giochi distribuiti da tale impresa siano la causa dell'ampia diffusione del virus.

Fatti e persone

Novembre: il Governatore e «l'erba»

Grave imbarazzo per la diplomazia britannica: alcuni funzionari stanno cercando di capire come è potuto accadere che in un discorso del Governatore di Hong Kong, Sir David Wilson, comparisse un invito alla legalizzazione della canapa indiana. Il commento dello statista sul futuro della colonia britannica è stato infatti distribuito ai giornali sotto forma di un dischetto, il quale conteneva un sorprendente annuncio: «Your PC is now stoned. Legalise marijuana.»

Tra i più diffusi nel mondo, il virus «Stoned» è originato in Nuova Zelanda ed è diffusissimo in Asia e Oceania.

Dicembre: un attacco a McAfee

I programmi antivirus di John McAfee, disponibili praticamente su qualsiasi sistema telematico che offra il download di software, sono considerati tra i più sicuri rimedi antivirus per il mondo MS-DOS. Rimandiamo i nostri lettori ai precedenti articoli per un approfondimento dei motivi che ci portano a diffidare dei «sicuri rimedi» in materia di virus.

Ad ogni modo, lo scorso dicembre questi programmi sono stati fatti oggetto di una campagna denigratoria ad opera di sconosciuti: su alcuni sistemi è stato fatto circolare un file, dal nome SCANV70.ZIP, modificato in maniera da danneggiare i dati sui computer su cui veniva eseguito.

Marzo: le minacce del Vendicatore Oscuro

«Dark Avenger», il Vendicatore Oscuro, è il nome di un ceppo virale noto da tempo, che si ritiene abbia avuto origine in Bulgaria. In questo Paese, nel mese di marzo, numerosi BBS hanno ricevuto il seguente messaggio:

«Hello, all anti-virus 'researchers' who are reading this message...
I am glad to inform you that my friends and I are developing a new virus, that will mutate in 1 of 4.000.000.000 different ways! It will not contain any constant information, so no virus scanner could be detecting it...
The virus will have many other new features that will make it completely undetectable and very destructive!
the Dark Avenger»

Fortunatamente non esiste, né potrà mai esistere, un virus completamente «undetectable». Anche quando i limiti insiti nei programmi di scansione saranno stati raggiunti, resterà sempre possibile verificare, a mezzo di CRC e controlli sulle firme crittografiche, l'integrità dei file contenenti programmi eseguibili.

Giugno: ancora contro McAfee

Lo stesso caso verificatosi in dicembre si è ripetuto nel mese di giugno: stavolta la versione modificata porta il nome di SCANV78.ZIP, e contiene un file TB1.COM infettato dal virus «Whale».

Agosto: virus in Cina

La Repubblica Popolare Cinese era rimasta finora piuttosto al di fuori delle cronache mondiali dell'informatica. Alla fine dello scorso mese di agosto, tuttavia, una notizia viene distribuita dalla Agence France-Presse: riprendendo un comunicato dell'agenzia semi-ufficiale China News Service, afferma che sono stati riscontrati oltre venti virus nella provincia del Guangdong. La polizia sconsiglia l'uso di software di origine sconosciuta.

La zona più colpita dai virus sembrerebbe essere quella adiacente al confine con Hong Kong; tra le oltre 90 imprese che hanno denunciato l'infezione, alcune hanno subito danni ingenti per colpa dei virus che hanno colpito oltre i tre quarti degli elaboratori installati.

I virus più diffusi nell'infezione cinese appartengono ai ceppi «Venerdì 13», «Caterpillar» e «Pakistani Brain».

Con l'occasione è risultato che una vasta parte del software utilizzato in Cina è di provenienza piratesca e origina da Hong Kong.

Il laboratorio antivirus

Questo primo anno di vita della rubrica «Virus» ha visto anche la proposta di avvio di un laboratorio antivirus presso la redazione di MCmicrocomputer. Abbiamo più volte invitato i lettori a sottoporre alla redazione qualsiasi programma sospetto, e la risposta dei lettori non si è fatta aspettare, per lo più per posta ma in un paio di casi anche attraverso MC-link: abbiamo uno scatolone pieno di dischetti, per lo più con virus già noti della cui ampia diffusione eravamo già a conoscenza; ma in alcuni casi ci sono arrivati dei contributi utilissimi, che verranno ricompensati — come avevamo anticipato — con un abbonamento annuale a MCmicrocomputer.

Abbiamo stilato una classifica provvisoria dei virus che ci sono pervenuti. Per non distorcere le cifre, nei casi in cui abbiamo ricevuto più di una copia di un virus sullo stesso dischetto l'abbiamo considerato come copia unica. Ecco i risultati:

11 copie: Cascade (1701/1704)
9 copie: Jerusalem/Jerusalem B/Jerusalem II
6 copie: Ping-pong/Italian virus
5 copie: 801
4 copie: Brain/Pakistani, Italian file, Vienna; abbiamo ricevuto anche quattro casi di virus segnalati come «nuovi», che sono attualmente sotto analisi;
3 copie: Anthrax, Star Dot, Stoned, Yankee Doodle;
2 copie: 4096/Frodo, 512, Apoc II, Burger, Invader, Parity, Terror, Tiny;
1 copia: AIDS, Dark Avenger, Enigma, Vacsina.

Se da un lato possiamo esprimere soddisfazione per la buona riuscita di questa iniziativa, tanto che riteniamo di prolungarla invitando nuovamente i lettori a inviare eventuali programmi sospetti, dall'altro consideriamo piuttosto preoccupante il fatto che alcuni virus potenzialmente disastrosi (512, 4096, Anthrax, Dark Avenger) circolino tranquillamente anche in Italia.

Non ripeteremo mai a sufficienza quanto essenziale sia il premunirsi con delle semplici precauzioni contro i possibili disastri causati da uno di questi programmi. Il Dark Avenger, ad esempio (v. riquadro pubblicato nella pagina precedente) è estremamente infettivo, e si trasmette con una rapidità preoccupante.

Non è nostra intenzione fare del facile allarmismo, non lo è mai stata e non inizieremo certo ora. Tuttavia ogni nuova notizia che proviene dal fronte della lotta contro i virus conferma la convinzione che tutelarsi contro i virus non è impossibile: occorre una combinazione di sistemi di prevenzione, come abbiamo già visto negli scorsi articoli.

Ormai quindi chiunque abbia seguito questa rubrica sa bene come proteggere un singolo computer. Appare sempre più evidente che il problema non è proteggere un computer, bensì proteggere il patrimonio informativo di un'organizzazione che si avvalga di decine o centinaia di computer. Di questo tratteremo in un prossimo numero.

MB

Worldport.
Gli affari in tasca

Pensate a un modem, non più grande di un pacchetto di sigarette, che vi permette di collegare qualunque computer — portatile o da tavolo — con qualunque altro, ovunque sia. E pensate alla possibilità di dotare il computer della funzionalità del fax, per comunicare con chiunque da un comune telefono.
Tutto questo è WORLDPORT, un oggetto indispensabile quando la mobilità e lo scambio di informazioni sono strumenti del successo. WORLDPORT è compatibile con i più diffusi programmi di comunicazione e viene fornito con il proprio software o - volendo - con il famoso CARBON COPY. I modem WORLDPORT sono disponibili anche nelle versioni a correzione di errore MNP 5 e Videotel.
WORLDPORT: un piccolo modem, grande come il mondo.

SMAU'91 3-7 ottobre
Pad.17 - Stand C 29

Distributore per l'Italia:

D-P

Data Peripheral Italiana s.r.l.
20148 Milano - Italy
Via M. Civitali, 75 - Tel. 02/40090050 r.a.
Fax 0039-2-40090101