Virus in Italia : quanti, quali e quale pericolo per le aziende

di Enrico Tonello

Il pericolo virus è perennemente in agguato. Ad elevato rischio di contagio sono sia i privati che utilizzano programmi di fonte incerta, sia le aziende che ricevono prodotti dimostrativi e visite periodiche del personale addetto alla manutenzione dei personal.

Tuttavia, mentre i privati possono, nella maggioranza dei casi, permettersi il lusso di perdere il contenuto del loro disco fisso, un'eventualità di questo tipo può risultare catastrofica in azienda.

Per rilevare quanti, fra gli oltre cinquemila virus circolanti nel mondo siano effettivamente presenti nel nostro paese, è stata organizzata nel 1994 - grazie alla collaborazione di alcuni giornalisti, del D.S.I. dell'Università di Milano e degli utenti della rete amatoriale FIDO Net - una raccolta di dati sull'intero territorio nazionale.

Il campione statistico su cui è stata condotta l'indagine è costituito sia da utenza aziendale che privata.

Secondo i risultati dell'indagine, la situazione virus in Italia si è radicalmente modificata nel corso dell'ultimo biennio. Da una situazione che vedeva, anche grazie alle inesistenti contromisure preventive ed alla relativa novità del fenomeno, codici virali di vecchia generazione quali FORM, Flip, Cascade, Stoned, Jerusalem e altri virus stranieri colpire i personal di mezza Italia, si è passati "all'utilizzo" di virus di produzione nostrana.

La maggior parte di tali virus hanno avuto per lo più una diffusione zonale che ha pregiudicato l'inserimento del codice di riconoscimento e rimozione specifico all'interno dei più noti programmi anti-virus di produzione straniera; altri hanno assunto l'onere della cronaca diffondendosi rapidamente al di fuori dei confini italiani.

I dati forniti da una recente indagine evidenziano la reale pericolosità dei virus Made in Italy

Fra i virus di produzione italiana più diffusi vi sono l'Invisible_Man.2926 (presumibilmente realizzato a Salerno), l'Arianna del quale sono note tre varianti (con ogni probabilità realizzate a Bari), il November_17th e le sue numerose varianti, Marzia e le sue svariate varianti (realizzate presumibilmente a Pisa) e il Bloody_Warrior (realizzato a Milano).

Abbastanza diffuso è anche HLLC.Crawen del quale sono note due varianti attive in particolar modo nel Veneto e in Friuli Venezia Giulia. Altri codici virali hanno una diffusione più ristretta, provinciale o poco più, come nel caso di Vota_DC.591 (provincia di Padova) e di RebelBase (provincia di Venezia).

Strategie d'azione

La fantasia degli italiani è come noto senza limiti, logico quindi che anche l'originalità dei virus writer di casa nostra sia superiore a quella dei loro colleghi.

Il più famoso tra i nuovi virus italiani è certamente l'Invisible_Man.2926. Questo virus è stato segnalato per la prima volta nel marzo 1993, epoca nella quale era già molto diffuso al sud. Rielaborazione del virus FLIP, Invisible_Man.2926 infetta i file .EXE .COM e il Master Boot Record ed è residente in memoria.

Grazie all'installazione in memoria il virus è da considerarsi Fast Infection (infezione veloce), risultano infatti infetti tutti i file che vengono utilizzati in una data sessione di lavoro.

Per cercare di sfuggire all'identificazione, Invisible_Man.2926 è dotato di un algoritmo di mutazione polimorfe sia per i file che per il Master Boot Record. All'interno del virus sono visibili (dopo la sua decrittografazione) le seguenti stringhe:

"The Invisible Man - Written in SALERNO (ITALY), October 1992"

"Dedicated to Ester: I don't know either how or when but I will hold you in my arms again..."

Questo messaggio non viene mai visualizzato a video.

Gli effetti visibili del codice virale si estrinsecano quando viene eseguito un file avente giorno e mese coincidenti con quelli correnti del calcolatore ma anno diverso. In questa situazione viene visualizzato a video, con appropriato sottofondo musicale, la prima e la terza strofa del motivo The Invisible Man del gruppo inglese QUEEN (voce solista Freddy Mercury). Concluse le performance video/audio il file viene sovrascritto con il testo della canzone.

Anche Marzia virus e le sue svariate varianti, oltre 14, sono state realizzate in Italia.

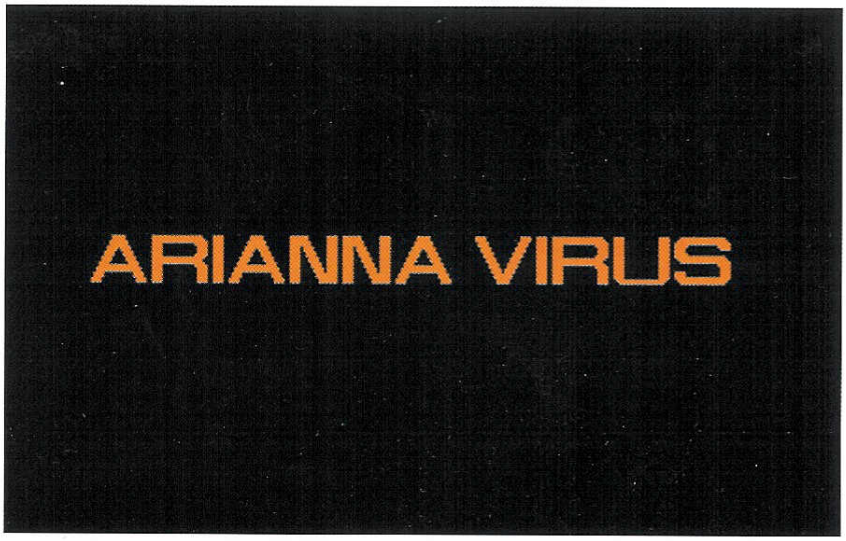
Marzia è anch'esso un virus multipartito residente in memoria. Marzia non è crittografato, ma utilizza tecniche Stealth per rendersi invisibile all'utente, e in molte occasioni riesce a rendersi invisibile agli scanner anti-virus, soprattutto quando questi non vengono utilizzati partendo da un dischetto di boot pulito.

Il nome del virus è dovuto alla presenza della stringa "Marzia" in una delle prime varianti ritrovate. Altre varianti di Marzia contengono la stringa "Virus Development Software", che dovrebbe identificare un gruppo di virus writer pisani che fanno riferimento a Willy Wonka autore anche di Minosse, un virus altamente polimorfica di difficile intercettazione. Alcune varianti di Marzia producono effetti disastrosi. Ad esempio, Marzia.B nei giorni 30 e 31 dei mesi che vanno da maggio a dicembre riscrive i primi 7 settori di tutte le tracce della testina 0 dell'hard disk 80H con valori casuali . Un'altra variante, dominata Marzia.D, contiene al suo interno la seguente stringa:

"PISello tenere fuori dalla portata dei bambini"
"PaxTibiQuiLegis.FaxFree!! WW20W3"

Mentre, Marzia.M contiene la seguente stringa:

"WW PASIPHAE(c)932Knosso"
"CX=5757-BX=CX-AX=3031-INT21H"



Un altro virus multipartito italiano è Arianna del quale sono conosciute fino ad ora tre varianti lunghe rispettivamente 2284, 3375 e 3426 byte.

La più diffusa delle tre è certamente la 3375, che deve la sua diffusione ad un periodo di permanenza sulla BBS italiana di un noto produttore internazionale di computer e macchine da scrivere. A causa di questa presenza, molti concessionari di zona che prelevano periodicamente upgrade di prodotti, driver e software shareware hanno, loro malgrado, contribuito a diffondere questo agente patogeno.

Arianna infetta i file .EXE e il Master Boot Record. E' un virus residente in memoria (Fast Infection) ed utilizza algoritmi per rendersi polimorfe ed invisibile (stealth).

Gli effetti visibili dell'infezione si manifestano dopo il quattrocentesimo boot del computer infetto. A seguito del quattrocentesimo boot viene visualizzata, in modalità grafica VGA/MCGA 320x200 pixel 256 colori, la seguente scritta:

"ARIANNA VIRUS"

Oltre alla scritta succitata, ve ne sono altre crittografate che non risultano essere mai visualizzate a video:

"BCoded in BARI ThanX to DOS UNDOCUMENTED See you for a new virus release. Bye !"

Naturalmente, non è possibile sapere se Arianna è un amore perduto o desiderato dell'autore del virus.

Decisamente più semplice a livello architetturale sono November_17th e tutte le sue varianti.

Alcune varianti di questo codice virale, soprattutto il November_17th.900.C, hanno avuto nel 1994 una grande diffusione.

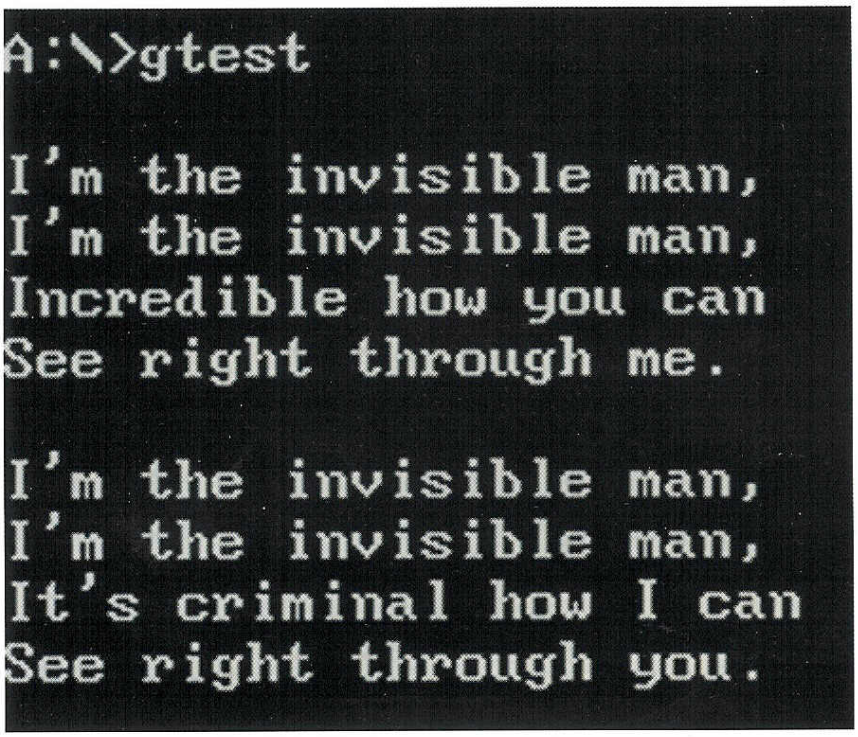
Ennesima variante del November_17th.855, che tanto fece strepitare negli anni scorsi la stampa specializzata ed i quotidiani, November_17th.900.C infetta "solamente" i file .COM e .EXE.

Quasi sicuramente non tutte le varianti del November_17th sono opera della stessa mano. Alcune di queste sembrano essere infatti prodotte da parte di virus writer improvvisati.

L'originale November_17th.855, è stato quasi sicuramente realizzato a Torino da uno sciagurato docente universitario che, ad un convegno SMAU di qualche anno fa, ammise di incitare i suoi allievi alla realizzazione di codici virali.

Non più Cracker_Jack

Come abbiamo avuto modo di vedere, la maggioranza dei virus circolanti in Italia sono interamente di produzione nazionale. Sono ormai passati i tempi dei vari Cracker_Jack, che "craccavano" maldestramente i virus, prelevati da BBS di virus exchange bulgare, e li distribuivano in Italia.



Le creazioni del "buon" Jack, per lo più virus overwriting quali il Milan.BadGuy, il Milan.New_BadGuy e altri, sono infatti praticamente estinte.

All'apice della sua "carriera" Cracker Jack, ebbe l'ardire di creare, prendendo come spunto alcuni virus prelevati sempre dalle BBS bulgare di virus exchange (probabilmente da quella che aveva sede all'interno dell'Università di Sofia, probabilmente capitanata da Todor Todorov), numerose varianti del virus Murphy. Queste ultime creazioni non sovrascrivono il file colpito, come i precedenti virus di Jack, , ma sono in grado di replicarsi mantenendo "funzionante" il file portatore. Queste "opere" furono create intorno al 1991, ed ebbero una scarsa se non irrilevante diffusione. Fortunatamente Jack da un po' di tempo a questa parte ha avuto la bella idea di abbandonare la scena, lasciando spazio ad altri creatori sicuramente più "dotati".

Nuovi codici virali

I nuovi codici virali italiani sono, da un punto di vista dell'originalità e della qualità del codice, molto validi.

Ad esempio, circa un anno fa sono stati rilasciati, o meglio scaricati, in vari BBS della rete FIDO Net, un gruppo di codici virali (24 per la precisione) creati con un generatore di virus chiamato I.V.P. (Instant Virus Production) firmato dal gruppo Youngsters Against McAfee.

Il pacchetto di 24 virus, veniva accompagnato da un file di testo che ne illustrava il contenuto e che viene riportato integralmente di seguito.

"This is the Italian Viral Labs family: Walky Replico, Executor, Infesto Replico NoTrace. These viruses were created just educational purpouse: none of them will annoy your datas!".

In barba alla legge sulla criminalità informatica, gli autori, o presunti tali, del pacchetto di virus (auto-definitisi IVL) hanno avuto l'ardire di darne notizia pubblica nella conferenza nazionale sui virus informatici VIRUS.ITA.

Di seguito vengono riportati alcuni stralci del messaggio pubblico degli IVL.

"IVL, associazione che si occupa di studi sui virus, nonché di produzione degli stessi ha deciso di rendere pubblica la sua attività di ricerca Anti-Virus. In quanto membri influenti di gruppi underground noi abbiamo accesso a dati che difficilmente cadranno nelle mani dei ricercatori senza la nostra intermediazione, e perché no, intercessione! Il nostro intento è dunque quello di far arrivare a ricercatori antivirus la nostra collezione di virus non ancora riconosciuti e dati in possesso di numerosi gruppi di Virus Writers."

Gli I.V.L. sono i presunti autori del virus Crepate, creato a Pisa, dove si firmano appunto con la sigla suddetta.

Fermare la diffusione dei virus

Molti si chiedono come mai queste distribuzioni a pioggia di virus non vengano fermate o per lo meno non si tenti di arginarle. Da un punto di vista pratico, i virus di nuova generazione possono essere tranquillamente scaricati nei BBS sia pubblici che privati ed anche nei siti INTERNET. Infatti, anche se il software viene controllato in automatico con le versioni più aggiornate di tutti i prodotti, i virus di nuova generazione, quindi non intercettabili, vengono tranquillamente messi a disposizione degli ignari utenti.

Dal un punto di vista legislativo l'Italia si trova in una situazione alquanto ingarbugliata.

Priva di una legge contro la criminalità informatica sino a fine 1993, l'Italia ha tentato di adeguare il Codice Penale per mezzo dell'articolo 615-quienques della legge n. 547 del 23 dicembre 1993 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

Tuttavia, principalmente a causa di una certa improvvisazione legislativa, è stata redatta una legge che colpisce più i diffusori (compreso quelli ignari) dei creatori di virus.

RAI: di tutto, di più

Una tra le più massicce diffusioni di virus in Italia è avvenuta ad opera del Televideo RAI, il quale grazie al servizio telesoftware inviava periodicamente software agli utenti.

Fra i vari software distribuiti dalla RAI, c'è un programma chiamato DIETA che conteneva un virus italiano.

Dopo una attenta analisi delle stringhe contenute al suo interno il virus venne identificato come Bloody_Warrior. Al fine di aggiungere la beffa al danno, i responsabili telesoftware distribuirono, qualche tempo dopo, un programmino singolo per la sua eliminazione creato in un paesino della Valle d'Aosta da una persona che sembra non esistere.

Un caso simile a quello RAI è stato segnalato anche in Germania con il virus Tremor inserito in PKUNZIP.EXE (uno dei più utilizzati software di compressione e decompressione dati). e distribuito via Etere attraverso il canale PRO-7 TV, di proprietà della German Company Channel Videodat, a circa 60.000 utenti tedeschi.

La schermata di benvenuto di una BBS italiana che distribuisce codici virali

Virus rari, pericolo vero

Esattamente come per i consueti prodotti software, anche fra i virus vi sono creazioni che non hanno avuto una diffusione a livello nazionale. Questi codici virali non hanno avuto la "fortuna" di infettare ampie zone, ma si sono limitati (e si limitano) a produrre infezioni a livello regionale o provinciale. Proprio a causa di questa scarsa diffusione, questi virus risultano più pericolosi in quanto vengono correttamente intercettati solamente da alcuni programmi anti-virus aggiornati direttamente in Italia.

Tra i virus più interessanti diffusi solo a livello locale c'è Vota_DC.591, segnalato attivo in provincia di Padova.

Vota_DC.591 è un virus propriamente a sfondo politico che visualizza, nel mese di aprile di ogni anno, il seguente messaggio: "Messaggio promozionale: Vota DC!".

Naturalmente, il messaggio promozionale che compariva proprio nel mese delle elezioni politiche poteva essere interpretato come una politica pubblicitaria intentata da sedicenti attivisti di partito. Ovviamente, non è chiaro per quale partito parteggino gli attivisti in oggetto, infatti essere colpiti da un virus che ti invita a votare un certo partito non può che dare risultati opposti. Potrebbe quindi trattarsi di un virus fatto ad arte dagli "oppositori" per screditare la fazione politica avversa.

Altro codice virale "politico" è il Berlusconi virus, noto anche come Berlusca o Slavery, creato nel periodo in cui il Cavaliere aveva minacciato di "scendere in campo".

Il Berlusca virus è un codice virale ad azione diretta che infetta i file con estensione .COM e che, il 27 Marzo di ogni anno, visualizza a video il messaggio:

"Freedom is Slavery: Berlusconi ti guarda"

accompagnato dal sottofondo musicale di Forza Italia.

Ad un ex presidente della Repubblica è invece dedicato il virus Cossiga.

Cossiga è un virus ad azione diretta che infetta i file con estensione .EXE, visualizzando a video ogni qualvolta venga eseguito un file infetto il seguente messaggio in modalità grafica CGA 40x25:

"COSSIGA ? No, grazie."
"By Amissi dee Panoce (c) 1991 Padova"

Il virus, oltre a propagarsi e a visualizzare a video il messaggio suddetto, non produce alcun effetto dannoso.

Sempre a livello provinciale è diffuso RebelBase, un virus ad azione diretta in grado di infettare i soli file con estensione .EXE. L'anonimo autore decanta, per mezzo di RebelBase, il suo amore per Kaori e tutte le ragazze giapponesi. Il novello virus writer è quindi un estimatore del fascino orientale, anche se in realtà Kaori (ragazza simbolo di una nota pubblicità di formaggi) è coreana e non giapponese.

RebelBase è un virus residente in memoria che, il 16 Aprile di ogni anno visualizza a video il seguente messaggio:

"Happy Birthday KAORY! Dedicato a tutte le meravigliose ragazze giapponesi. (C) BitLabs (The RebelBase) 1993, N. Italy"

Questo breve, e obbligatoriamente incompleto, excursus sui virus creati in Italia ha lo scopo di evidenziare una realtà che viene troppo spesso nascosta: il vero pericolo per le aziende è rappresentato dai virus di produzione italiana, virus che solo raramente vengono intercettati dai noti programmi anti-virus di produzione estera.

```
Happy Birthday KAORI!
Dedicato a tutte le meravigliose ragazze giapponesi
(C) BitLabs (The RebelBase) 1993, N. Italy.
```

L'autore
Enrico Tonello *è un consulente di sicurezza informatica in ambito bancario e aziendale.*