Informatica

Anche un PDF può essere pericoloso

di Nicola Bortolotti

Anche nel mondo dell'informatica esistono i cosiddetti "tormentoni" estivi: è ormai da qualche anno, ad esempio, che le creature dei "virus writers" – per volontà o per coincidenza più o meno fortuita – colpiscono con più efficacia nei mesi "caldi". È sorprendente il fatto che si tratti – a volte – di diffusioni improvvise di infezioni da tempo latenti e per le quali esistevano contromisure ignorate non solo per distrazione o negligenza, ma a volte per opportunità.
È – inoltre – un dato di fatto sempre più acquisito che la velocità di diffusione di virus e soprattutto "worm" sia sempre maggiore, un fatto che rende le contromisure tradizionali e obbligatorie (antivirus e firewall) temporaneamente e pericolosamente inefficaci. Nel contempo, i creatori dei virus sono sempre più solerti nello sfruttare ogni vulnerabilità di sistemi operativi e programmi.
Queste considerazioni, che meritano un approfondimento soprattutto in relazione in quanto sta succedendo proprio quest'anno in Italia e nel mondo, assumono un significato particolare per chiunque abbia a che fare professionalmente con anche un solo Personal Computer – alla luce della vessatoria normativa sulla privacy grazie alla quale operare su strumenti informatici è più pericoloso dal punto di vista legale del guidare un'auto con i freni difettosi – o addirittura si limiti a tenere in tasca un telefonino abbastanza "intelligente".

Dentro la notizia
Paradigmatica, a tale proposito, può essere la "prima pagina" del quotidiano "Punto Informatico" del 2 settembre (che si può leggere all'indirizzo Internet http://puntoinformatico.it/index.asp?r=PI&t=02%2F09%2F05): ben tre titoli riguardano virus e worm e sono tutti – per almeno un verso – assai allarmanti. Dedicato – ad esempio – a chi sostiene (come il legislatore e i tanti tecnici interessati che fanno da corifeo) che una effettiva e dimostrabile protezione nei confronti degli attacchi sia possibile (con inversione dell'onere della prova), ecco la clamorosa diffusione da parte di Creative di migliaia di lettori MP3 contenenti un worm: è chiaro che ci saranno uno o più responsabili e colpevoli; è altresì ovvio che la questione verrà in un modo o nell'altro chiarita e risolta affinché non si ripeta, perlomeno con la medesima modalità, ma qui si sta parlando di una breccia nel sistema di sicurezza e di controllo di qualità non dell'anonimo studio professionale di provincia bensì di un colosso mondiale la cui attività produttiva è situata in quella parte del mondo nella quale è stato inventato il concetto stesso di "qualità totale". E si sta discutendo di qualcosa che in Italia, da tempo immemore grazie all'ansia di arrivare primi – se non nella tecnologia – nel diritto, ha rilevanza anche penale; qualcosa che è sempre accaduto (celebre e risalente a svariati anni fa la pubblicazione di un file infetto per poco meno di una settimana su un importante sito istituzionale italiano, per debellare il quale si suggeriva successivamente l'utilizzo di un noto software... a pagamento) e che è destinato ad accadere anche in futuro inesorabilmente, così come inevitabili sono i "bug" del software.
Degna di nota anche l'infezione ai telefonini via Bluetooth o MMS (e peraltro da tempo annunciata, l'aspetto strano è solo che non sia successo prima) che sfruttano una sorta di "social engineering" giacché anche l'utente esperto (per non parlare del quasi sempre incolpevole profano – ma per la legge italiana perennemente responsabile) è portato ad "abbassare la guardia" quando utilizza un cellulare. E così, ad esempio, basta un distratto clic di troppo su un MMS per scatenare un autentico disastro fatto di credito e batteria prosciugati, violazioni della privacy, apparecchio inservibile, diffusione virale con l'ipotesi nemmeno troppo remota di vedersi anche citare per danni …

Nemmeno i migliori si salvano
Il vero temporale estivo nel mondo dell'informatica era però giunto – secondo tradizione – a cavallo di ferragosto. Perché – se l'utenza media ha da tempo alzato la guardia nei confronti di files eseguibili e messaggi malevoli ed ora si appresta a farlo anche nei confronti dei messaggini multimediali – ben diverso è il caso se l'allarme giunge da un tipo di file ormai tanto ubiquo da risultare indispensabile nella maggior parte dei contesti, il formato PDF.
L'utilizzo del "Portable Document Format" di Adobe da tempo non è più limitato al mondo dell'editoria elettronica ma è ormai strategico in molti campi; nel primo numero del 2003 di questa rivista, ad esempio, si metteva l'accento sull'importanza del PDF in relazione alla firma digitale e alla diffusione di modulistica. Oggi è pressoché impensabile riuscire ad utilizzare proficuamente per lavoro o per svago un PC sprovvisto di un'applicazione (sia esso il "reader" ufficiale e gratuito di Adobe o, invece, uno dei programmi alternativi prevalentemente diffusi in ambiente Linux, come KPDF) in grado di leggere e stampare documenti in questo formato altamente "porta-

bile" e "fedele", a dispetto delle differenti piattaforme hardware e software.
L'upgrade dei computer, una volta suggerito dalla "velocità di risposta" delle applicazioni di office automation, oggi viene sempre più indotto dal tempo impiegato ad aprire e gestire un file PDF. Dalle banche agli istituti pubblici, nella maggioranza dei casi l'interazione con il pubblico e i professionisti avviene tramite questo popolarissimo, potente e pervasivo formato; un formato dalle possibilità e dalla diffusione così ampi da stimolare la ricerca di vulnerabilità nei software – altrettanto onnipresenti – utilizzati per leggerlo.
Ed ecco arrivare il 16 agosto il fulmine estivo dallo stesso sito Adobe (all'indirizzo http://www.adobe.com/support/techdocs/321644.html), ripreso dal bollettino di sicurezza di Secunia reperibile all'URL http://secunia.com /advisories/16466, dall'ancor più autorevole sito governativo http://www.kb.cert.org/vuls/id/896220 e da una miriade di altri siti che hanno contribuito a diffondere l'allarme rosso: anche leggere un comunissimo e in apparenza inoffensivo file PDF proprio con i lettori ufficiali e gratuiti di Adobe – che ha inventato lo standard – può compromettere in modo assai serio il proprio sistema, sia esso Windows, Mac, Linux o Solaris.
Poco male, si potrebbe commentare, giacché all'atto della pubblicazione del bollettino di sicurezza erano subito disponibili le "patches" per correggere la vulnerabilità. Esistono invece ulteriori motivi di allarme poiché questa vicenda – per molti versi paradigmatica – offre diversi spunti di riflessione.
Analizzando innanzitutto le "patches", brilla per assenza quella a una versione per Windows ancor oggi diffusa, quell'Acrobat Reader 5.0.5 così apprezzato per la sua leggerezza, velocità e compatibilità anche con sistemi obsoleti. Non è peraltro facile capire dal "Security Advisory" di Adobe che l'aggiornamento 5.0.10, in grado di risolvere il problema di sicurezza della 5.0.5, riguarda solo la versione per Macintosh; la cosa è finalmente chiara dalla pagina che permette di scaricare manualmente gli ultimi aggiornamenti http://www.adobe.com/support/ downloads/new.jsp.
A ciò si aggiunga il fatto che i diffusissimi prodotti che possono essere colpiti dall'attacco abbracciano un arco di tempo di circa un quinquennio: Adobe Reader 5.1, 6.0-6.0.3, 7.0-7.0.2, Adobe Acrobat 5.0-5.0.5, 6.0-6.0.3, 7.0-7.0.2. Evidentemente tale "security hole" doveva essere ben celato non solo ai potenziali "pirati informatici", se non ha provocato seri problemi sino ad ora, ma anche agli stessi programmatori Adobe, il che non è confortante.
La raccomandazione, qualora non si aggiornino i software Adobe, è quella di aprire unicamente files PDF provenienti da una fonte "di fiducia". La cosa non è parimenti tranquillizzante, perché il meccanismo di diffusione di virus e worm prevede ormai quasi di routine la veicolazione tramite messaggi di posta elettronica in apparenza provenienti da un mittente conosciuto e del quale ci si possa fidare.
Il fatto che sua maestà PDF (ma sarebbe meglio dire: i più popolari software in grado di leggerli) abbia manifestato una tale debolezza sotto il profilo della sicurezza deve suonare come campanello d'allarme assordante, perché non ci sarebbe da sorprendersi se fra qualche mese una gran massa di utenti consapevoli – ma all'epoca in vacanza – non sapendo di dovere aggiornare con urgenza Acrobat Reader (o non volendo lasciare la vecchia ma perfettamente funzionante versione) non presterà troppa attenzione nell'aprirne di malevoli.

Luci ed ombre degli aggiornamenti automatici
Un'obiezione logica e lecita, a questo punto, è rappresentata dal fatto che ormai la maggior parte dei software (compresi i sistemi operativi) ha la possibilità di verificare automaticamente la presenza di aggiornamenti e di effettuarli, prassi da anni comune per gli antivirus.
Tale possibilità estesa a tutti gli applicativi e al sistema operativo, peraltro sottilmente e pericolosamente prevista dalla normativa sulla privacy, apre in realtà la strada a problemi talvolta non inferiori a quelli provocati da virus e worms. Questo perché gli "aggiornamenti automatici" non di rado creano malfunzionamenti e incompatibilità anche assai gravi, in grado di compromettere l'esecuzione di alcuni programmi vitali per il proprio lavoro o addirittura facendo fallire il caricamento del sistema operativo stesso.
L'esempio forse più famoso è rappresentato dal "Service Pack 2" per Windows XP, tanto che una prestigiosa newsletter come quella della CNET Community titolava ancora il 2 settembre: "Upgrading to Windows XP SP2: yes or no?".
Ma – rimanendo in casa Microsoft – esistono molti casi ancora più insidiosi: ad esempio, in un ambiente di rete misto, la patch – definita "critica" – KB885250 dedicata alle macchine Windows 2000/XP crea enormi problemi

Figura 1

nell'accesso a condivisioni in rete Windows 9x. Problemi tutt'ora irrisolti, tanto che in siffatti contesti – caratteristici di piccole reti – l'unica soluzione è la rimozione (forzata e manuale) di questo aggiornamento.
Ma anche ritornando al caso degli antivirus – per i quali un update almeno giornaliero è davvero consigliabile, a prescindere dal risibile obbligo di legge di svariati mesi – le insidie non mancano. Rimarrà come eloquente "case history" quanto accaduto lo scorso 22 aprile ad uno dei produttori più seri, Trend Micro, con un aggiornamento del "Pattern File" (le cosiddette "firme") che ha causato problemi a non finire (con una paralisi dell'attività del PC) a svariate migliaia di clienti. La storia è ampiamente documentata anche sullo stesso sito di Trend Micro all'indirizzo http://www.trendmicro.com/en/support/pattern594/overview.htm.
È infine da sottolineare il fatto che l'obbligo di aggiornare il software per proteggerlo da attacchi implica la sua immediata obsolescenza e potenziale inutilizzabilità qualora il produttore – per volontà o forza maggiore – non rilasci più le necessarie patches. La questione, anche visti i costi e i termini di licenza, non è affatto di poco conto. Non a caso i produttori di antivirus prevedono abbonamenti annuali assai economici per l'update delle firme virali; nel caso di programmi applicativi e sistemi operativi gli aggiornamenti sono di norma gratuiti, ma solo per un periodo limitato a discrezione della politica sul "ciclo di vita" del software decisa unilateralmente dal produttore.

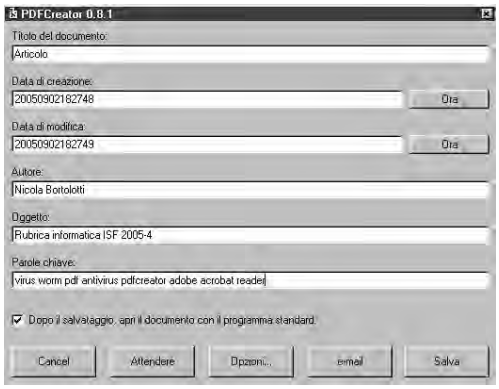

Figura 2

Creare PDF senza problemi
Dopo avere parlato dei pericoli connessi alla lettura dei files PDF, è opportuno spendere qualche parola anche sulla creazione dei files in questo formato perché – pur esistendo numerose altre alternative disponibili per chi non voglia acquistare il potente ma costoso prodotto ufficiale Adobe – la scelta ottimale a costo zero è rappresentata da un progetto open source ormai consolidato (a dispetto della versione 0.8, che sembrerebbe indicare una immatura prerelease) e di grande interesse dal nome autodocumentante: PDFCreator.
All'indirizzo http://sourceforge.net/projects/pdfcreator si possono scaricare programmi di installazione e sorgenti. In realtà PDFCreator fornisce un'interfaccia amichevole a vantaggio di tutti gli utenti Windows (da 95 a XP) al famosissimo e collaudato GhostScript; a quest'ultimo, in effetti, è delegato tutto il lavoro di generazione del PDF.
Da tantissimi anni, anche prima di PDFCreator, era possibile creare ottimi PDF con GhostScript installando (e configurando) un printer redirector come RedMon; si trattava tuttavia di una operazione non sempre immediata per un non addetto ai lavori, come ben sanno i clienti Infocamere che hanno aperto la strada all'utilizzo della firma digitale in Italia.
PDFCreator, però, rende il tutto (compresa l'installazione di GhostScript) veloce e alla portata di chiunque – e senza sgradite sorprese finali – come documentato dalla sequenza di immagini riportate in Figura 1. Alla fine comparirà una nuova stampante (virtuale) denominata PDFCreator, scegliendo la quale verrà generato un file in formato PDF.
A questo si aggiunge anche la possibilità di controllare agevolmente alcuni parametri "occulti" del file PDF, come le date, il titolo, il soggetto, l'autore e le parole chiave per l'indicizzazione (Figura 2).
È bene chiarire che, se lo scopo è quello di generare PDF destinati non alla semplice visualizzazione e stampa bensì alla realizzazione di moduli di richiesta dati con campi da riempire a video, questo non è il prodotto adatto, così come del resto gli altri software non Adobe – assai più economici o gratuiti con restrizioni – sul mercato.
L'utilizzo di una stampante virtuale consente di generare PDF a partire da qualsiasi applicativo in grado di stampare.
È bene ricordare che è sempre preferibile diffondere un documento "finito" in formato PDF piuttosto che "proprietario" (come ad esempio Word, Excel, e così via); non solo perché – in tal modo – non si obbliga il ricevente a dotarsi di un programma per la visualizzazione, ma anche poiché esso sarà visto e stampato su qualsiasi piattaforma esattamente così com'è stato creato dall'autore (entro certi limiti) e – qualora firmato digitalmente – ci sarà assoluta garanzia della sua conformità all'originale, cosa questa che non potrebbe essere garantita nemmeno utilizzando formati non proprietari (come quello di OpenOffice).
Avendo citato OpenOffice, è bene ricordare che – per generare PDF a partire da questo potente pacchetto di office automation gratuito – è anche possibile utilizzare la funzione di generazione interna che non ha bisogno né di PDFCreator né di GhostScript ma – ovviamente – consente di generare files solo a partire da documenti aperti da OpenOffice.