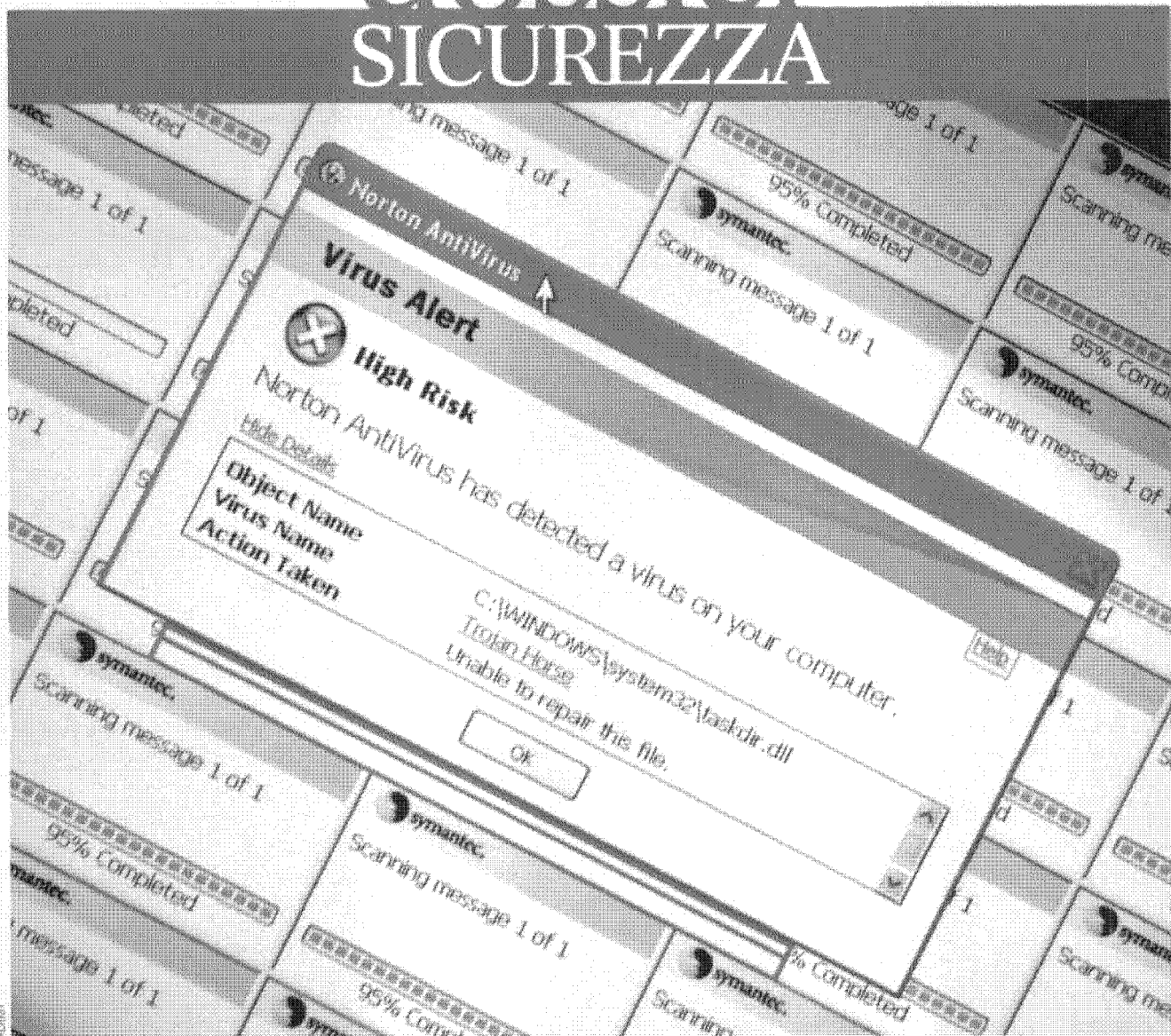


dossier SICUREZZA



Virus, la difesa inizia dall'informazione

Lo scorso anno sono stati bruciati 66 milioni di dollari, sottratti dai pirati informatici che hanno rubato password e dati sensibili dai computer aziendali. Anche se le soluzioni diventano sempre più sofisticate, la prima barriera è una corretta conoscenza dei rischi.

FRODI INFORMATICHE

Computer blindati per resistere a tutti gli attacchi

La stima dei furti informatici alle persone in Italia nel 2007 si è fermata a quota 5,5 milioni di euro. Con una forte riduzione rispetto ai 16 milioni dell'anno precedente. Ma il Paese resta nella «top ten» delle reti con le pagine più infette.

di Francesco Di Martile

■ L'amore tradisce e, se virtuale, è anche peggio. Gli analisti specializzati in attacchi di codice maligno informatico sono concordi: San Valentino, la festa degli innamorati di febbraio, ogni anno si trasforma in un improvvido trappolone per computer. Rispondere ai «valentini» di sconosciuti (le email di affettuose carinerie) è la via più sicura per beccarsi *malware*, ossia codici maligni che possono arrecare danni inenarrabili. Su Facebook, il popolare sito di social networking dove un milione di persone

si mostrano e discutono, Fortinet ha scoperto che c'è un programmino che miete vittime a man bassa: si chiama «Secret chush» (cotta segreta) e, se clicchi, scopri chi brama per te. In realtà scarica un worm che indirizza il computer su un sito

web pagato per numero di clic ricevuti e che, pertanto, sta rendendo ricchi i furbi inventori della «cotta segreta».

Furbate che sono un fiume in piena. Nell'Internet Security Outlook 2008 di CA si trae questo consuntivo del 2007: il 90% della posta elettronica è spam e più dell'80% dello spam contiene link a siti potenzialmente dannosi; addirittura il software di sicurezza fasullo pesa per il 6% di tutto lo spyware (codici per rubare informazioni) del 2007; da gennaio a ottobre il malware è cresciu-

to di 16 volte e i tipi più comuni sono stati *adware* (pubblicità non richiesta), *trojan horse* (codici maligni nascosti in immagini o allegati), *downloader* (mancano le parti più segrete del sistema operativo). E le previsioni per quest'anno sono pessime: incremento del flagello dei *botnet* (pc resi zombie all'insaputa dei proprietari), videogiochi e frequentatori di social network le vittime più facili, elezioni americane e Olimpiadi le date cruciali in cui si scatenano attacchi virali.

E l'Italia? «Le cose vanno molto meglio che in passato» dice Marco Riboli, country manager di Symantec (vende il 74% del mercato delle scatole antivirus per pc, 17 mila addetti nel mondo, 160 in Italia, con 5,20 miliardi di dollari di fatturato 2007)

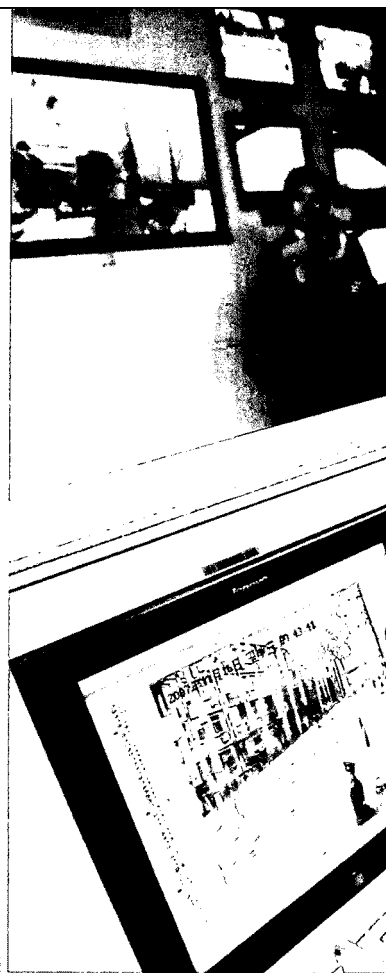
«L'impressione è che dalla sottovalutazione si è passati a una maggiore consapevolezza dell'importanza della sicurezza informatica. Semplicemente perché oggi gli attacchi sono molto più subdoli e toccano direttamente le tasche delle persone».

La stima dei furti informatici in Italia lo scorso anno è intorno ai 5,5 milioni di euro, molto meno dei 16,6 dell'anno prima. Dati che, però, non bastano a ribaltare la situazione generale come registrata da Sophos: l'Italia con-



LE INCURSIONI SONO PIÙ SUBDOLE E TOCCANO LE TASCHE DELLE PERSONE.

MARCO RIBOLI
SYMANTEC ITALIA



tinua a essere nella «top ten» delle nazioni con le pagine web più infette. Guida la classifica la Cina seguita dagli Stati Uniti, che ospitano un terzo delle pagine web infette al mondo, e poi Russia e Polonia.

«Non siamo più al folclore della pallina da ping pong che saltella o sulle lettere che precipitano sullo schermo dal documento» spiega Ottavio Camponeschi, regional director di McAfee (4 mila addetti nel mondo, 30 in Italia, con 1,2 miliardi di dollari di fatturato 2007) «Oggi il malware va a caccia dei conti correnti, delle password, delle chiavi d'accesso ai segreti industriali. Soldi, insomma. E i pc oggi sono pieni di questi dati sensibili: se viene smarrito o rubato, l'azienda o la persona è esposta a rischi enormi».

La tecnologia, nonostante tutti i progressi di antivirus, antispam, firewall, non può fare niente se non si educano le persone a comportamenti prudenti. Oggi si può, infatti, solo mitigare il rischio



ma non escluderlo al 100%. Ecco perché McAfee propone alle aziende *ePolicy Orchestrator*, uno strumento che aiuta a stabilire e far rispettare norme di comportamento rigide: sul pc di lavoro non si deve installare niente di insicuro, né film né musica; non si deve navigare in siti non sicuri, e via di questo passo».

SITI CON BUONA REPUTAZIONE. «Oggi le minacce colpiscono tutti e distinguere tra difese per l'utente finale e per l'azienda è un errore perché le aziende sono fatte di end user che portano il pc portatile a casa, navigano in internet e sono più facili vittime di frodi» aggiunge Rodolfo Falcone, amministratore delegato di Trend Micro (3 mila dipendenti, 27 in Italia, con 727 milioni di dollari di fatturato nel 2006). «Soprattutto sono vittime di bot, ossia il loro pc viene preso sotto controllo remotamente da hacker senza che il proprietario se ne accorga e viene utilizzato per inviare spam e diffondere mal-

ware. Ecco perché servono codici comportamentali aziendali molto rigidi per la sicurezza utilizzando, per esempio, il nostro servizio di *Web Reputation* che attribuisce una scala di affidabilità ai siti web e, quindi, può limitare la navigazione internet solo ai siti con buona reputazione. Un modo per navigare con più tranquillità».

Gartner stima che il fatturato Emea (Europa, Medio Oriente e Africa) sia stato nel 2007 di 2,4 miliardi di euro e, con tassi annui del 9,6%, toccherà i 3,4 nel 2011. Un business che attira grandi protagonisti come Ibm, Computer Associates, BMC Software, Hewlett-Packard che estendono la propria offerta con soluzioni centrate sul controllo dell'identità e la gestione degli accessi; e che vede Microsoft, Oracle, Novell espandersi nella sicurezza mediante acquisizioni.

La parte maggiore è delle tantissime imprese dedite anima e corpo alla sicurezza e alla preservazione dei dati. ©

DIFENDERSI DAL MALWARE

Lo spam è cresciuto del 100% nel corso del 2007 con una media di 120 miliardi di messaggi quotidiani a livello globale: insomma ogni persona al mondo riceve almeno 20 messaggi spam al giorno. Tramite lo spam si possono installare nel computer minacce capaci di recare infiniti danni. Che fare? Ecco dieci suggerimenti tratti da Ironport Systems, business unit di Cisco dedicata alla sicurezza

DIECI SUGGERIMENTI

1. Attivare i servizi per proteggere il furto dei dati personali (per esempio con avvisi via Sms quando avvengono operazioni sul vostro conto corrente bancario).
2. Quando si naviga e si deve lasciare online il proprio indirizzo email, indicarne uno secondario.
3. Per i pagamenti online usare una carta di credito temporanea o prepagata.
4. Non aprire messaggi sospetti o da sconosciuti.
5. Non rispondere assolutamente a email di sconosciuti.
6. Non cliccare su un link contenuto in una email di sconosciuti (anche l'unsubscribe).
7. Non comprare mai niente da un sito indicato in una email spam.
8. Non alimentate le «catene di Sant'Antonio»: sono un facile modo per intercettare indirizzi email validi.
9. I messaggi spam indirizzano a siti dove risiedono programmi spyware o malware. Se il vostro fornitore di connessione non utilizza filtri antispam e antivirus efficaci, cambiatelo.
10. Se un messaggio vi sembra uno spam o una frode online, probabilmente lo è: cancellatelo.