German
Data
Security

G Data Whitepaper 2009

Come si introducono i virus nei PC aziendali?

Ralf Benzmüller & Werner Klier
G Data Security Labs

Go safe. **Go safer. G Data.**

Sommario

1. A cosa serve il malware?

Negli ultimi anni, i motivi che inducono a creare e a diffondere software dannosi sono profondamente cambiati. Se agli albori dei virus la ragione principale era un'ambizione quasi sportiva, una sorta di gara tra specialisti del computer, oggi gli aggressori sono spinti principalmente da interessi finanziari evidenti.

Nel „sottobosco digitale" si è consolidata una vera e propria economia sommersa, la quale crea, perfeziona e diffonde malware professionali all'interno di strutture rigide, ben organizzate e impeccabili.

Nell'economia del cybercrimine si svolge un fiorente commercio di tutti i beni e i servizi digitali possibili. In alcune specifiche piattaforme commerciali, le informazioni sulle nuove falle di sicurezza appena scoperte si possono acquistare esattamente come i malware creati su misura. Gli autori forniscono agli acquirenti perfino una garanzia di funzionamento e durante il periodo di garanzia provvedono anche ad offrire gratuitamente le versioni modificate.

È possibile, inoltre, affittare eserciti di computer infetti, i cosiddetti PC zombie entrati a far parte di una rete Bot, su base oraria o giornaliera per lanciare campagne di spam o attacchi mirati contro siti web poco amati o server di posta.

E perfino l'ultimo anello della catena di creazione del valore, ossia la trasformazione in denaro contante delle informazioni rubate, come i dati delle carte di credito, viene realizzato nel mercato digitale dei cybercriminali. A questo scopo alcune false aziende arruolano come „agenti finanziari" gli ignari utenti di PC che mettono a disposizione i propri conti bancari privati per transazioni finanziarie di dubbia natura.

Da tempo l'obiettivo principale degli attacchi non è più la creazione di un software dannoso, creato unicamente per diffondersi. Anche le reti aziendali sono sempre più appetibili per gli aggressori, per carpire qualsiasi tipo di informazione che possa procurare denaro o per abusare delle infrastrutture della rete per scopi criminali.

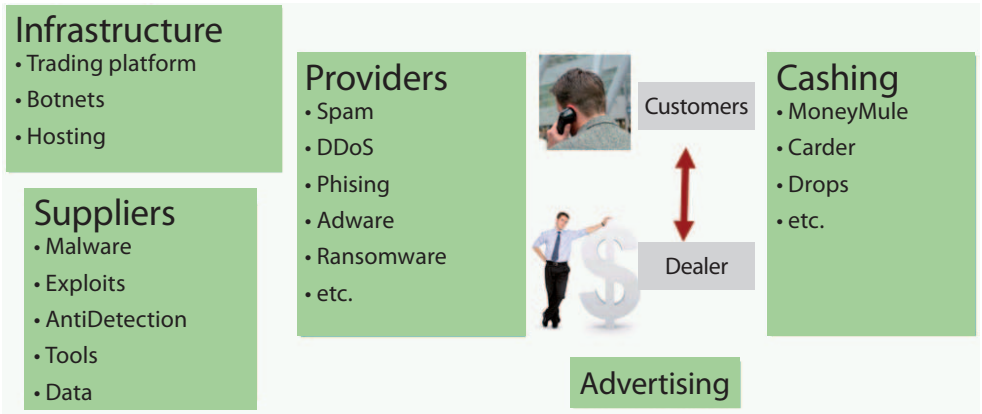

Fig. 1: Panoramica sui singoli settori dell'economica dell'eCrime

Come mostra la Fig. 1, l'economia dell'eCrime è strutturata come un'area nidificata di „settori economici" numerosi e diversificati. Sullo sfondo agiscono i reali attori che forniscono i programmi nocivi, le conoscenze sulle nuove falle nella sicurezza e smerciano i dati rubati. Questi vengono venduti o affittati da mediatori a „clienti" criminali in siti commerciali specializzati e infine trasformati in moneta sonante da intermediari generalmente inconsapevoli (cosiddetto cashing).

2. Come guadagnano i cybercriminali con il malware

I delinquenti online realizzano i profitti in vari modi. Un ruolo importante è svolto dalle armate di computer infetti controllate dagli aggressori. Le cosiddette reti Bot sono in grado di svolgere una serie di attività illegali che consentono di guadagnare molto denaro in modo occulto.

2.1 Reti Bot

Le reti Bot sono la chiave di volta dell'infrastruttura eCrime. Non servono solo per inviare spam o eseguire attacchi di tipo Denial of Service. I computer zombie vengono anche utilizzati per ospitare pagine di phishing e malware e per perlustrare gli indirizzi dei server di posta elettronica. Non deve quindi sorprendere se il numero di computer Bot sia aumentato notevolmente. Poiché le reti Bot sono state segmentate in unità più piccole di poche migliaia di zombie, anche il numero delle reti Bot è aumentato considerevolmente.

Il controllo avveniva principalmente via IRC (Internet Relay Chat: sistema di chat basato sul testo), quindi nelle fasi di sviluppo successive sono nate più reti Bot che utilizzano per il controllo altri protocolli. Le reti Bot più moderne, come la famosa Storm, sono state create come reti Peer-to-Peer (P2P). Anche la potente rete Bot Zunker comunica tramite HTTP. Dopo la chiusura dell'ambiguo Internet Service Provider McColo, alcune reti Bot hanno perso il proprio computer di comando ed erano quindi incapaci di agire. In seguito sono scomparse le reti Bot Srizbi e Storm. Ora nuove reti Bot, come Waledac e Conficker, generano varie possibilità di contatto per poter disporre delle reti Bot in qualsiasi momento. I meccanismi di mimetizzazione vengono costantemente perfezionati e i backdoor vengono nascosti efficacemente grazie a frequenti aggiornamenti e rootkit. I programmi e i dati necessari a un compito vengono trasmessi appena prima ed eliminati subito dopo.

2.2 Spam

Lo spam rappresenta un business importante. Con lo spam non guadagna soltanto chi offre i prodotti pubblicizzati. L'invio delle e-mail di spam avviene generalmente tramite le reti Bot. Per l'invio di 2 milioni di e-mail in 14 giorni, lo spammer Solomon ha pagato 195 $. 20 milioni di e-mail sono costati 495 $. Il commercio di pillole prive di efficacia, software rubato e copie scadenti è già lucroso di per sé anche con una percentuale di risposta minima, laddove le quote di risposta sono tutt'altro che esigue. I prodotti semilegali pubblicizzati qui hanno la loro clientela, che è maggiore di quanto comunemente si pensi. E non vi sono soltanto commercianti disonesti che truffano i clienti con l'acquisto della merce. Jeremy Jaynes, ai suoi tempi l'ottavo maggiore spammer del mondo, ha guadagnato in un mese fino a 750.000 $.

2.3 Estorsione

Quando il Web shop di un'azienda è molto remunerativo oppure quando un'azienda dipende da esso, tanto che le e-mail vengono elaborate in tempo reale, allora questa azienda è ricattabile tramite attacchi a questi servizi. I PC zombie di una rete Bot attivati contemporaneamente possono bombardare un sito Web o un server di posta con richieste prive di senso. A causa delle richieste inviate in massa al server, un sistema può essere sovraccaricato in modo tale da impedirne il normale funzionamento.

Con questi attacchi di overload distribuiti (in inglese: Distributed-Denial-of-Service, attacco DDoS) è possibile ricattare non soltanto agenzie di scommesse e casinò online. Chi guadagna importi a cinque o sei cifre in un'ora, o chi deve fornire i servizi a una comunità di giochi, è disposto anche a pagare un riscatto, che spesso ammonta a una cifra irrisoria rispetto alla perdita

del volume d'affari. In genere corrisponde ad importi a 4 cifre. La cifra stimata è molto elevata.

Gli attacchi DDoS vengono inoltre utilizzati per scopi politici. In Estonia tra la fine di aprile e l'inizio di maggio 2007 sono stati bloccati i server di ministeri, enti governativi, banche, giornali e imprese. La rimozione del monumento di un soldato russo aveva suscitato l'indignazione della popolazione russa. Mentre le manifestazioni venivano represse, le reti Bot sono state impiegate come strumento politico.

Oltre ai mezzi di ricatto mediante attacchi di overload, illustrati sopra, esistono altre possibilità di estorcere denaro alle vittime. Un ransomware, come ad es. GPCoder, crittografa determinati file di un computer. Chi vuole accedere ai contenuti dei propri file, deve acquistare un programma di decodifica il cui prezzo, a seconda dei casi, varia dai $ 12 ai $ 200.

Nelle aziende esistono ulteriori modelli. Un cavallo di Troia è riuscito a trasferire sul computer infetto di un dipendente immagini pornografiche, software illegali e/o file video e audio protetti da copia. L'aggressore ora può ricattare il dipendente, minacciando di rendere noto il fatto ai suoi superiori, o addirittura l'azienda stessa, minacciando di denunciarla alla polizia.

2.4 Furto di dati

Il commercio di dati rubati non si limita soltanto ai dati rubati di carte di credito e conti bancari. Con gli attacchi di phishing vengono rubati anche i dati d'accesso per eBay, social network, negozi online, account di e-mail e altro. Usando i keylogger, ossia programmi nocivi che registrano le immissioni da tastiera, è possibile rubare perfino più dati, ad esempio i dati di accesso a server aziendali, giochi di ruolo online, contenuti (riservati) di e-mail e documenti o dati di accesso a server, forum e VPN. Se un server web appena ripulito risulta nuovamente infettato dopo pochi giorni, è possibile che l'amministratore del sistema abbia perso le sue password in un keylogger. I file di log di questi keylogger vengono commercializzati nei forum illegali al prezzo di poche centinaia di euro per dozzine di gigabyte. Queste informazioni vengono poi sfruttate da altri gruppi e messe di nuovo sul mercato.

I dati rubati vengono utilizzati in vari modi:

- Le carte di credito vengono utilizzate per „stampare" carte di credito falsificate o per fare acquisti nei negozi online.
- I dati bancari vengono utilizzati per effettuare bonifici non autorizzati. Poiché nei conti bancari privati la somma ammessa per i bonifici è limitata (a partire da 5000 euro subentrano particolari misure di sicurezza), anche il bottino è limitato. Queste limitazioni non vengono applicate a molti conti bancari di aziende. Perciò i ladri di dati bancari online rafforzano le proprie attività per riuscire ad acquisire questi dati di accesso.
- Gli account eBay rubati servono per riciclare il denaro rubato mediante l'acquisto di merci.
- L'accesso ai giochi di ruolo online viene sfruttato per rubare valute e strumenti online.
- Con i dati di accesso degli account di e-mail e dei social network viene inviato spam a nome della vittima.
- I dati personali rubati vengono usati per aprire account Internet in determinati forum. Questi account verranno poi sfruttati per attività illegali e frodi.

2.5 Adware

Gli adware registrano le abitudini di navigazione dell'utente, visualizzano determinate pagine pubblicitarie o manipolano le ricerche. Il pagamento dell'adware avviene tramite il conteggio

del numero di clic prodotti (ad esempio, viene manipolata la pagina iniziale del browser dei computer infetti) oppure per versione installata. I programmi partner corrispondenti si trovano negli specifici forum online. Nonostante l'anno scorso anche grandi aziende del settore dell'adware abbiano dovuto incassare sconfitte legali, il numero di malware pubblicitario e programmi indesiderati è aumentato di oltre cinque volte negli ultimi due anni.

Conclusione: questi non sono gli unici business-model dei criminali online. Deve essere comunque chiaro che la criminalità online rappresenta un grosso business e che i danni provocati da queste attività sono nell'ordine delle decine o centinaia di miliardi, ossia più del mercato della droga. I settori commerciali menzionati mostrano gli ambiti principali usati da chi diffonde i malware. Lo strumento più importante sono le reti Bot. Esse costituiscono la base per l'invio di spam e per gli attacchi di phishing. Altri ambiti importanti sono l'estorsione, il furto di dati e la visualizzazione di annunci pubblicitari mirati.

3. Come si introduce il malware nel PC

Dopo avere illustrato le motivazioni di chi diffonde programmi dannosi, possiamo ora dedicarci al vero argomento di questo studio. Esistono vari modi per introdurre i malware nei PC aziendali. In alcuni casi può essere sufficiente collegare il computer a Internet o a una rete locale. Ma anche e-mail, siti di scambio P2P, Instant Messaging e perfino supporti dati possono contenere codici dannosi. Attualmente le più pericolose sono le pagine web appositamente preparate che scaricano direttamente i file o infettano il computer in background senza essere notati (i cosiddetti Drive By Download).

3.1 È sufficiente una connessione

Gli innumerevoli worm e bot che girano continuamente e autonomamente in Internet rappresentano una minaccia costante per i computer collegati a Internet. Essi generano senza pausa indirizzi IP più o meno casuali e verificano se nei rispettivi computer vi sono falle nella protezione. La scelta degli indirizzi IP è spesso limitata in modo da selezionare solo determinate aree della rete, ad esempio un particolare Internet Provider o una specifica area geografica. Le falle di sicurezza utilizzate variano con il tempo. Anche le falle chiuse da molto tempo vengono ancora interrogate, ad esempio da Blaster (2003) e da Sasser (2004). Qui di seguito vengono elencati gli obiettivi di attacco più frequenti:

- Plug'n'Play (MS05-039) tramite TCP/445, TCP/139
- RPC-DCOM (MS03-026/MS03-039) tramite TCP/135, TCP/445, TCP/1025
- LSASS (MS04-011) tramite TCP/445
- MySQL tramite TCP/3306
- Arkeia tramite TCP/617
- Veritas tramite TCP/6101
- Veritas tramite TCP/10000
- WINS tramite TCP/42
- Arcserve tramite TCP/41523
- NetBackup tramite TCP/13701
- Workstation Service (MS03-049) tramite TCP/135, TCP/445
- WebDaV tramite TCP/80

- DameWare tramite TCP/6129
- Backdoor MyDoom tramite TCP/3127
- Backdoor Bagle tramite TCP/2745
- IIS 5.x SSL PCT (MS04-011) tramite TCP/443
- Account con password banali (connessione tramite TCP/139 o TCP/445)
- Server MSSQL con password banali (ad es. account di amministratore del sistema con password vuota) tramite TCP/1433

In un'indagine sono stati misurati gli attacchi verificatisi in tre mesi su diverse architetture di computer. I computer Windows hanno subito di media un attacco ogni 38 secondi. Come alcuni amministratori di sistema hanno constatato, spesso un nuovo computer appena installato viene aggredito e catturato in pochi secondi, durante il download delle patch. Nelle reti con numerosi clienti finali, come T-Online, la frequenza degli attacchi è ben inferiore alla media di uno ogni 38 secondi. A questa situazione contribuisce anche il fatto che negli ultimi anni la creazione di codici exploit ha raggiunto un livello professionale. Talvolta i codici exploit per falle di sicurezza compaiono già pochi giorni dopo i primi rapporti su tali falle. Cresce costantemente anche il numero degli exploit che vengono scoperti mentre sono utilizzati dai malware, i cosiddetti exploit Zero-Day. L'esempio più recente è il worm Conficker, il quale, oltre a diffondersi automaticamente, si propaga sfruttando anche le condivisioni locali con password deboli e il meccanismo di Autostart dei supporti di dati USB.

Questo tipo di attacco non richiede alcuna azione da parte dell'utente del PC e nella maggior parte dei casi avviene a sua insaputa. Per proteggersi da questi attacchi è necessario un firewall o un router ben configurato.

3.2 Per e-mail

Come in passato, molti virus si diffondono per e-mail. Le grandi esplosioni di Loveletter, Melissa o Sobig e Netsky, che hanno parzialmente messo in ginocchio i server di posta, sono sempre più rare e non sono più previste dai diffusori di worm. Gli ultimi worm per e-mail che hanno suscitato grande interesse nei media sono stati Sober, Nyxem e Warezov. Al loro posto vengono lanciate piccole ondate, limitate a livello temporale e locale. Al contrario delle infezioni causate dai worm che si propagano in modo completamente automatico, i worm per e-mail diventano pericolosi solo quando il destinatario apre l'allegato. La ricezione di una e-mail infetta non rappresenta di per sé alcun pericolo e solo in rari casi è sufficiente visualizzare il messaggio sul client (ad es. Bubbleboy e Klez). La maggior parte delle e-mail necessita dell'intervento del destinatario, il quale viene indotto ad aprire l'allegato con svariate tattiche di persuasione (social engineering). A questo scopo vengono falsificati tutti i possibili dati dell'intestazione del messaggio. In particolare viene frequentemente rilevato l'indirizzo del mittente. Solo la prima generazione di worm per e-mail si diffondeva con il nome della vittima. Oggi quasi tutti gli indirizzi dei mittenti vengono falsificati dai worm per e-mail.

Poiché nel frattempo i file eseguibili contenuti nelle e-mail vengono filtrati (nel gateway o nel client) ed è aumentata anche la consapevolezza del pericolo nei destinatari di e-mail, gli autori di malware hanno cambiato strategia. Anziché allegare file, nei messaggi vengono inseriti link a file in Internet. Questi messaggi non vengono immediatamente riconosciuti come dannosi. Eventualmente si possono filtrare mediante il filtro antispam. Il comportamento dell'utente è tuttavia molto simile. Fa clic sul link e normalmente il browser propone di eseguire il file. Non passa molto tempo, che i link diretti al malware vengano riconosciuti come dannosi. Gli autori del malware ora indirizzano a un sito Web in cui il destinatario deve avviare di nuovo un down-

load o in cui il download si avvia automaticamente, talvolta mediante vari inoltri.

Come esca per indurre la vittima ad eseguire il file o a richiamare una pagina Web (il cosiddetto social engineering), viene utilizzato il mittente, la riga dell'oggetto e/o il contenuto della e-mail. Ma anche i nomi degli allegati, le doppie estensioni dei file, icone famose o nomi di dominio dei link servono per rendere plausibile questo tentativo di raggiro. Jordan e Goudey (2005) citano i seguenti dodici fattori psicologici sui quali si sono basati i worm di maggior successo tra il 2001 e il 2004:

- Inesperienza (inexperience)
- Curiosità (curiosity)
- Avidità (greed)
- Timidezza (diffidence)
- Gentilezza (courtesy)
- Amor proprio (self-love)
- Credulità (credulity)
- Desiderio (desire)
- Sensualità (lust)
- Minaccia (dread)
- Reciprocità (reciprocity)
- Cordialità (friendliness)

M. Braverman ha integrato:

- Conversazione generica (generic conversation): Brevi dichiarazioni, come „cool" ecc.
- Avvisi di virus e patch software
- Rilevamento di malware sul PC
- Rapporti di rilevamento di virus in fondo all'e-mail
- Informazioni o messaggi sugli account: ad es. il cavallo di Troia Telekom, che si spaccia da bolletta telefonica eccessiva
- Messaggi di errore di invio della posta elettronica
- Attrazione fisica (Physical attraction) (si sovrappone al punto Sensualità di Jordan e Goudey)
- Accuse (Accusatory): ad es. il cavallo di Troia BKA, che pretende di avere trovato file illegali
- Eventi di attualità
- Articoli gratuiti: alcune persone dimenticano le precauzioni non appena viene offerto qualcosa gratis

Tuttavia, i tentativi di inganno non si arrestano nel momento in cui il virus ha raggiunto il suo scopo ed è stato eseguito. Dopo un attacco realizzato con successo, occorre impedire che la vittima si accorga di essere stata infettata. Vengono quindi aperti messaggi di errore, immagini o documenti (spesso vuoti). Alcuni worm, come Sircam e Magistr, si associano a un file e quando si avvia il codice nocivo, viene aperto anche il file originale. In questo modo l'infezione passa inosservata.

3.3 Per Instant Messaging

La maggior parte dei worm per Instant Messaging invia messaggi di posta contenenti link a pagine Web. La possibilità di trasferire i file direttamente viene ora utilizzata di rado. Anche in questo caso, le e-mail ricorrono al social engineering. Alcuni worm di Instant Messaging possiedono perfino dei motori di chat in grado di condurre brevi conversazioni in modo da instaurare un rapporto di fiducia.

Chi utilizza l'Instant Messaging in azienda, dovrebbe scegliere un client che consenta la verifica dei file in entrata. Alcuni client permettono di lanciare un controllo antivirus tramite una riga di comando.

3.4 Attraverso i siti P2P

In uno degli studi condotti da G Data, è stata eseguita una ricerca di termini correlati ai 20 giochi online attualmente più utilizzati. All'inizio dell'indagine, dei circa 1000 file scaricati, il 33% era infettato da virus. Più dei due terzi (68%) dei virus sono stati identificati come adware, il 23% erano cavalli di Troia e il 5% backdoor.

Nel corso degli oltre sei mesi di indagine, già la metà dei file esaminati scaricati dai siti di scambio P2P conteneva codici dannosi. Questa cifra ha raggiunto il picco verso la fine del periodo di indagine, con un valore massimo di oltre il 65% di file infetti.

Queste cifre confermano il fatto che i siti di scambio P2P restano, come in passato, estremamente appetibili per gli autori di malware. Chi li utilizza in azienda, dovrebbe sempre tutelarsi al massimo.

3.5 Tramite i supporti di dati

Accade sempre più spesso che i supporti dati, come dischi rigidi, DVD e lettori MP3, escano dalla fabbrica già infettati con malware. Sono stati segnalati perfino dei casi in cui nel parcheggio davanti a un'azienda sono state „perse" appositamente chiavette USB. Alcuni dipendenti volevano sapere cosa contenesse la chiavetta e hanno infettato in questo modo i propri PC con programmi spyware.

Il worm Conficker, onnipresente nel 2009 negli articoli dei media, ha usato anche la funzione Autorun del sistema operativo Windows per diffondersi tramite supporti dati. I worm della famiglia Autorun sfruttano anch'essi questa „funzione" di Windows e dal secondo semestre del 2008 hanno dato vita a un vero revival dei worm. I consigli di disattivare la funzione Autorun sono inizialmente caduti nel vuoto poiché ciò si è reso possibile solo successivamente grazie ad una patch prodotta da Microsoft.

Questi casi mostrano che le aziende, soprattutto se custodiscono dati preziosi, possono essere attaccate anche tramite metodi inusuali e che le precauzioni non sono mai abbastanza.

3.6 Tramite le reti locali

Un'ulteriore via di propagazione è rappresentata dalle condivisioni nelle reti locali. Alcuni worm copiano sé stessi in tutti gli ambiti a cui si può accedere liberamente. In molti casi vengono usati gli elenchi delle password più comuni. Anche Conficker ha sfruttato questi punti deboli. Perciò nelle aziende è opportuno utilizzare password complicate e controllare periodicamente, meglio ancora se quotidianamente, l'eventuale presenza di virus nelle condivisioni. Alcune varianti di Rbot e Conficker utilizzato, tra l'altro, i seguenti login:

„ ADMIN", „ADMINISTRADOR", „ADMINISTRAT", „ADMINISTRATEUR", „ADMINISTRATOR", „ADMINS", „COMPUTER", „DATABASE", „DB2", „DBA", „DEFAULT", „GUEST", „NET", „NETWORK", „ORACLE", „OWNER", „ROOT", „STAFF" „STUDENT",

„TEACHER“, „USER“, „VIRUS“, „WWWADMIN“

e le seguenti password:

„ 0“, „000“, „007“, „1“, „12“, „123“, „1234“, „12345“, „123456“, „1234567“, „12345678“, „123456789“, „1234567890“, „12345678910“, „2000“, „2001“, „2002“, „2003“, „2004“, „ACCESS“, „ACCOUNTING“, „ACCOUNTS“, „ADM“, „ADMIN“, „ADMINISTRADOR“, „ADMINISTRAT“, „ADMINISTRATEUR“, „ADMINISTRATOR“, „ADMINS“, „BASD“, „BACKUP“, „BILL“, „BITCH“, „BLANK“, „BOB“, „BRIAN“, „CHANGEME“, „CHRIS“, „CISCO“, „COMPAQ“, „COMPUTER“, „CONTROL“, „DATA“, „DATABASE“, „DATABASEPASS“, „DATABASEPASSWORD“, „DB1“, „DB1234“, „DB2“, „DBA“, „DBPASS“, „DBPASSWORD“, „DEFAULT“, „DELL“, „DEMO“, „DOMAIN“, „DOMAINPASS“, „DOMAINPASSWORD“, „ERIC“, „EXCHANGE“, „FRED“, „FUCK“, „GEORGE“, „GOD“, „GUEST“, „HELL“, „HELLO“, „HOME“, „HOMEUSER“, „HP“, „IAN“, „IBM“, „INTERNET“, „INTRANET“, „JEN“, „JOE“, „JOHN“, „KATE“, „KATIE“, „LAN“, „LEE“, „LINUX“, „LOGIN“, „LOGINPASS“, „LUKE“, „MAIL“, „MAIN“, „MARY“, „MIKE“, „NEIL“, „NET“, „NETWORK“, „NOKIA“, „NONE“, „NULL“, „OAINSTALL“, „OEM“, „OEMINSTALL“, „OEMUSER“, „OFFICE“, „ORACLE“, „ORAINSTALL“, „OUTLOOK“, „OWNER“, „PASS“, „PASS1234“, „PASSWD“, „PASSWORD“, „PASSWORD1“, „PETER“, „PWD“, „QAZ“, „QWE“, „QWERTY“, „ROOT“, „SA“, „SAM“, „SERVER“, „SEX“, „SIEMENS“, „SLUT“, „SQL“, „SQLPASS“, „STAFF“, „STUDENT“, „SUE“, „SUSAN“, „SYSTEM“, „TEACHER“, „TECHNICAL“, „TEST“, „UNIX“, „USER“, „VIRUS“, „WEB“, „WIN2000“, „WIN2K“, „WIN98“, „WINDOWS“, „WINNT“, „WINPASS“, „WINXP“, „WWW“, „WWWADMIN“, „XP“, „ZXC“

Si dovrebbe dunque rinunciare a usare nella propria rete queste e simili password (anche nella loro traduzione italiana).

3.7 Attraverso i siti Web

Attualmente la principale porta di ingresso per i virus è costituita dai siti Web. I virus sfruttano un punto debole strutturale nel metodo di lavoro dei programmi antivirus. I programmi antivirus verificano i file non appena un componente di sistema desidera accedervi (OnAccess) oppure su richiesta (OnDemand). Quindi la scansione da parte del programma antivirus ha luogo solo quando il codice dannoso è già presente come file. Ora, quando i dati della pagina Web vengono trasmessi al browser via HTTP, i codici HTML e i comandi degli script ivi contenuti vengono inizialmente interpretati ed eseguiti nella memoria temporanea del browser. Ad un certo punto il browser decide di salvare i contenuti sul disco rigido. Probabilmente solo in quell'istante scatta l'allarme dell'antivirus. A questo punto, però, i codici dannosi sono già stati eseguiti. Un programma antivirus realmente efficace per proteggersi da pagine Web infette deve essere in grado di controllare il contenuto del flusso di dati HTTP prima che questo acceda al browser.

Nella sezione dedicata alle e-mail si è già spiegato che i file dannosi possono essere scaricati da siti Web. Ciò avviene direttamente tramite un link al file infetto, tramite inoltri o inducendo l'utente con l'inganno a fare clic su un pulsante o su un link e a scaricare ed eseguire il file sul computer.

Ora verranno brevemente illustrate due tipiche tattiche per indurre l'utente a scaricare e ad installare il malware. I cosiddetti scareware ingannano la vittima con falsi messaggi di avviso in merito a un'infezione del sistema. Per debellare l'infezione, alla vittima viene richiesto di fornire i dati della propria carta di credito al fine di acquistare per 50 dollari la presunta „versione completa“ di un falso programma antivirus.

Fig. 2: Una pagina Web di scareware in cui alla vittima vengono richiesti i dati della carta di credito

Viene adottata spesso e volentieri una tattica per attirare la vittima su una pagina Web che dovrebbe visualizzare un video. Può essere di contenuto erotico o anche correlato a un evento di attualità trattato proprio in quel momento dai media, ad esempio una catastrofe naturale, un incidente aereo, le elezioni presidenziali, un evento sportivo ecc. Per visionare il video tanto decantato, l'utente deve inizialmente installare uno speciale codec video o una nuova versione di Flash in cui è nascosto il software dannoso. Sotto questo link si nasconde sempre un malware, il quale viene installato sul computer al posto di Flash Player.

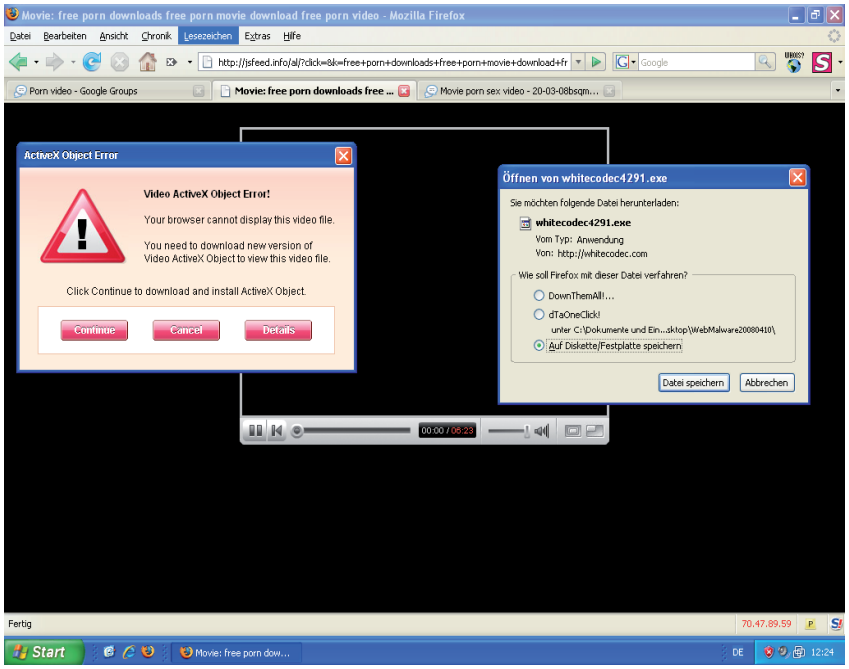

Fig. 3: Pagina Web di presunti video che invita a scaricare un codec infetto

Esiste un'altra tecnica di attacco nella quale l'utente non può intervenire: la cosiddetta tecnica drive by download. Mentre i download devono essere avviati dal visitatore, con la tecnica drive by download, come suggerisce il nome stesso, i download avvengono senza essere notati du-

rante la navigazione. Su un server controllato dal distributore di malware vengono creati alcuni script che controllano innanzitutto quale browser e quale sistema operativo vengono utilizzati nel PC del visitatore del sito Web. In base alla combinazione rilevata, viene quindi caricato un codice dannoso adattato in modo mirato che cerca le falle nella protezione del browser e dei suoi componenti. Se la ricerca ha esito positivo, viene trasmesso il codice dannoso, che sfrutta le falle nella sicurezza per aggredire il PC. Questi codici nocivi si chiamano exploit. La maggior parte degli exploit viene creata per i computer Windows con Internet Explorer. Vengono attaccati inoltre anche i punti vulnerabili di Firefox, Opera e Safari. Per l'installazione degli script sono usati tool come MPack IcePack e FirePack, i quali provvedono ad installare correttamente tali script. Attualmente, le falle nella sicurezza sfruttate più di frequente dagli autori di malware sono le seguenti:

- CVE 2007-0071 Adobe Flash
- CVE 2008-1309 RealPlayer
- ourgame_GLIEDown2 Internet Explorer
- CVE 2006-0003 MS06-01, MDAC
- CVE 2007-5601 RealPlayer

Quando il server è pronto, il distributore di malware deve soltanto attirare i visitatori sul sito. Vengono inviate a questo scopo e-mail di spam con messaggi interessanti, particolari offerte o vincite alla lotteria che invitano a collegarsi alla pagina. Sempre più spesso vengono manipolate anche determinate interrogazioni nei motori di ricerca più noti, come Google, Yahoo e Bing, in modo da visualizzare le pagine Web dannose in cima all'elenco dei risultati. Anche una digitazione errata durante l'immissione di un link può condurre a pagine infette. Ecco due esempi: „mircosoft.com", „goggle.com", „mcaffe.de" e altri domini, il cui nome assomiglia moltissimo a siti Web famosi, sono stati registrati già da anni per ospitare annunci pubblicitari. Ora con la diffusione di adware e malware si può guadagnare ulteriore denaro.

Molto più efficace, tuttavia, è quando si riesce ad integrare un codice dannoso nelle pagine Web di un dominio conosciuto. Se un aggressore riesce a mettere sotto controllo un server Web, utilizzando i toolkit degli exploit menzionati in precedenza, potrà inserire in ogni pagina Web una riga che scarica da un altro server il codice nocivo (ad es. per IFRAME o SCRIPT). Anche per le aggressioni a siti Web esistono ormai vari tool che tentano di carpire la password di accesso dell'amministratore mediante attacchi a dizionario. Per assumere il controllo sui server Web vengono sfruttate le falle nella sicurezza dei software per il Web, come sistemi di gestione dei contenuti, software per blog e forum e strumenti di amministrazione. Nella maggior parte dei casi, questi attacchi non sono limitati a singoli server Web, bensì eseguiti in massa e in automatico. Le conseguenze: i codici dannosi possono nascondersi in qualsiasi dominio, non soltanto nei luoghi più remoti di Internet.

Un'altra opportunità è offerta dagli annunci pubblicitari nei siti Web. Quasi tutti i domini più conosciuti sfruttano la possibilità di guadagnare pubblicando annunci pubblicitari nel sito. Generalmente i banner pubblicitari vengono visualizzati nella pagina tramite IFRAME, pertanto il gestore del sito non ha alcun controllo sui contenuti qui riprodotti. È compito dei responsabili dell'attività pubblicitaria verificare i contenuti degli annunci visualizzati. Tuttavia, è più facile a dirsi che a farsi. Gli script dannosi, creati con MPack o tool simili, sono altamente mimetizzati e codificati (la creazione di codici dannosi polimorfi si può realizzare anche con linguaggi di scripting). In questo modo si riesce ad integrare un codice nocivo in pagine Web legittime. Circa l'80% di tutte le infezioni drive by download avvengono in siti Web regolamentari.

Ma si può trasmettere un codice dannoso anche senza manipolare un server Web. I link a forum, blog ed e-mail possono contenere file pericolosi, che verranno poi eseguiti nella pagina richiamata. I siti Internet interattivi offrono numerosi forum di discussione e siti wiki che permettono ai partecipanti di contribuire con propri file e messaggi. In questi siti è possibile caricare virus o creare un link a una pagina dannosa. Una volta in Wikipedia, in un articolo dedicato al worm Blaster, un autore è riuscito ad inserire un link a uno strumento di rimozione che più tardi si è rivelato essere un cavallo di Troia. Questi forum sono frequentati attivamente anche da persone (e dai loro PC) che non hanno affatto buone intenzioni. E grazie alle innumerevoli identità rubate, possono accedere facilmente a gran parte dei forum e restare perfino mimetizzati.

Tuttavia, non è neppure necessario inserire un virus nel server. Già il link a una pagina Web preferita può contenere di per sé un codice dannoso, che verrà eseguito nella pagina di destinazione. Questo tipo di attacco viene definito Cross Site Scripting (XSS). Un attacco XSS è sempre possibile quando le immissioni di un utente vengono nuovamente visualizzate in una pagina successiva e non vengono controllate per rilevare l'eventuale presenza di contenuti eseguibili. Quando, ad es., il nome inserito in un modulo viene nuovamente visualizzato in una pagina successiva di un'ordinazione, è sicuramente un meccanismo utile. Tuttavia, quando un aggressore al posto del proprio nome inserisce un codice JavaScript, questo codice, se non viene filtrato dal browser, viene eseguito. Ecco un esempio di Cross Site Scripting: In un modulo viene richiesto di specificare il nome. Al posto del proprio nome, l'aggressore inserisce il seguente codice:

```
<SCRIPT>alert(„You're pwned")</SCRIPT>
```

Dopo l'invio del modulo, nella pagina successiva questo codice non verrà visualizzato, bensì eseguito. Nel caso precedente, verrà visualizzato un messaggio di avviso. Un vero attacco contiene un codice pericoloso.

Ma anche quando le immissioni in un modulo vengono filtrate, il codice può essere scritto direttamente nel link della pagina richiamata, in modo simile a questo:

```
http://www.myserver.dom/site.php?name=<SCRIPT>alert(„You're pwned")</
SCRIPT>
```

Un tale link può nascondersi in qualunque testo creato in un forum o un blog. Ancora più infido, tuttavia, è quando questi link XSS compaiono nei risultati di ricerca di Google. Gli autori di malware ottimizzano le voci dei blog corrotte per i motori di ricerca di Google e con un paio di trucchi di mimetizzazione riescono sempre ad infiltrarsi, nonostante Google tenti ogni volta con molti sforzi di rilevare questi link XSS e di eliminarli dai risultati della ricerca.

La situazione è simile con le molte nuove possibilità offerte da Web 2.0. Chi decidesse, a causa della situazione pericolosa, di non consentire più nel browser i contenuti attivi o i linguaggi di scripting, resterebbe escluso dal meraviglioso mondo del Web 2.0 e dalle sue innumerevoli opportunità. Molte di queste nuove funzioni offrono però anche un potenziale per gli abusi, aumentando così la quantità di possibili falle nella sicurezza. In Myspace, alla fine del 2005, il worm XSS di Samy si è creato mediante Cross Site Scripting (XSS) oltre un milione di amici in 18 ore. Tuttavia, finora il Cross Site Scripting è stato sottovalutato come pericolo.

I domini che propagano codici dannosi non si trovano soltanto negli angoli oscuri di Internet, nei popolari portali di download, come Rapidshare, e nella pagine Internet crackate, bensì anche nelle pagine legittime e nei risultati delle ricerche in Google. Conclusione: di fatto, in ogni pagina Web può esservi un file pericoloso in agguato.

4. Svolgimento di una tipica ondata di infezione

L'esecuzione di un attacco compiuto da cybercriminali avviene in genere secondo uno schema preciso. Nel corso degli ultimi anni, le caratteristiche di un'infezione tipica sono cambiate notevolmente. I worm come NetSky e MyDoom avevano allegati voluminosi che contenevano programmi dannosi monolitici, con molte funzioni integrate. Negli ultimi anni, invece, si sono trasformati in numerosi moduli piccoli, compatti e altamente specializzati, che possono essere caricati in modo flessibile in base alle esigenze. L'infezione si svolge in varie fasi. Dopo avere preparato il file dannoso e scelta la potenziale vittima, ha luogo l'aggressione vera e propria. A questo punto i sistemi infettati sono controllati dall'aggressore, che può abusarne praticamente per qualsiasi attività criminale.

4.1 Preparazione dell'infezione

Inizialmente viene sviluppato il virus che si intende diffondere. Tuttavia, non tutte le ondate di infezione si basano su nuovi virus. Se un autore di malware ha sviluppato un codice nocivo, può utilizzare questo modello e con l'aiuto di runtime packer, altri compilatori e strumenti vari per l'occultamento del codice, può creare per lungo tempo nuove varianti per altre ondate, finché queste varianti non verranno rilevate dai comuni programmi antivirus. Quando il virus prevede che il programma antivirus sia in grado di riconoscerlo nei computer infetti, è sufficiente presentare ai consueti antivirus una versione ancora sconosciuta del codice nocivo. Chi non vuole farlo da sé, può sempre trovare nei relativi forum le persone capaci, che offrono a prezzi lucrosi i servizi adeguati, corredati di garanzia.

Quando il virus è disponibile, l'aggressore deve scegliere uno o più metodi di diffusione. Ad esempio, può eseguire il virus tramite un attacco automatico a una falla nella sicurezza. In questo caso, la vittima non nota nulla né dell'attacco, né dell'infezione. Può anche scegliere una delle strategie di inganno per indurre l'utente ad avviare lui stesso il programma nocivo. Nel primo caso, l'aggressore necessita di un exploit che catturi il PC, nel secondo caso di un sito Web e/o di una e-mail o di un messaggio di Instant Messaging intrigante che induca l'utente a scaricare e ad eseguire il file. Quando il virus deve essere ospitato in una pagina Web, è necessario registrare i domini e salvare qui i file adeguati. Per molte di queste attività, esistono tool di semplice utilizzo.

4.2 Esecuzione

Dopo avere catturato il computer, di solito viene avviato un cavallo di Troia-downloader, il quale provvederà ad introdurre nel computer i file dannosi e quindi ad avviarli. Per prima cosa, l'autore degli attacchi viene informato del successo dell'infezione e del sistema catturato. Quindi vengono disattivate le impostazioni di protezione del PC infetto. In questo modo il computer viene esposto senza alcuna protezione ad ulteriori attività di malware. Nella fase successiva, vengono caricati sul computer ulteriori file nocivi. Per eseguire queste operazioni possono essere utilizzati più file infetti.

In molti casi il primo file nocivo che viene caricato è un backdoor, ad esempio nascosto con un rootkit, che viene eseguito in background senza essere notato. Attraverso questa porta secondaria, il computer infetto riceve un nuovo proprietario, che ora potrà agire con il computer a suo piacimento. Il backdoor consente, tra l'altro, di coordinare via IRC, P2P o HTTP il computer infetto con altri PC. In questo modo il computer entra a far parte dell'enorme esercito dei PC zombie. Dopo l'installazione del backdoor, il computer infetto viene ispezionato minuziosamente e l'aggressore decide cosa fare con questo PC. I PC crackati vengono esaminati mediante spyware alla ricerca di dati di valore e/o attrezzati con adware. Quando il computer dispone

di una buona connessione ad Internet, può essere sfruttato per l'invio di spam, per offrire file illegali da scaricare o per ospitare pagine Web di phishing o di malware.

4.3 Utilizzo del computer infetto

Se i PC zombie di una rete Bot devono essere usati per inviare spam, il gestore della rete Bot deve eseguire tramite un backdoor un pacchetto di malware sul computer infetto che contiene anche modelli di e-mail, un elenco di indirizzi di posta elettronica e il software per l'invio dei messaggi. Quando il file è configurato, viene avviato e la spedizione di spam comincia. Dopo avere inviato tutte le e-mail, il software si cancella dal computer insieme a tutti i dati. Ben nascosto, resta solo il backdoor, che attende ulteriori comandi.

5. Come proteggersi

La protezione dal malware dei computer aziendali è un ambito di competenza della sicurezza informatica, strettamente correlato alla sicurezza informatica dell'intera azienda. La sicurezza IT non è uno stato, bensì un processo. In ogni azienda sono determinati gruppi di utenti o reparti ad essere particolarmente danneggiati e che necessitano di una protezione speciale. In questo processo ogni singola azienda deve prendere delle decisioni sotto vari aspetti, che portano a soluzioni totalmente individuali.

Inizialmente si associa la protezione contro il malware con l'utilizzo di procedure tecniche che dovrebbero proteggere contro danni ben definiti. Le principali misure tecniche sono le seguenti:

- **Protezione antivirus**
  Deve essere installata sia sui server che sui client. Deve essere in grado di rilevare codici dannosi nei flussi di dati HTTP ed eventualmente nei dati provenienti dalle chat (ICQ, IRC).
- **Protezione antispam**
  Dato che le e-mail, anziché i file allegati, ora contengono solo link a pagine Web dannose, la protezione antispam funge contemporaneamente anche da protezione antimalware.
- **Firewall, rilevamento e prevenzione di intrusioni**
  I dati del traffico di rete possono essere utilizzati per scoprire ed impedire i più comuni attacchi da worm Internet.

Ma anche altri provvedimenti contribuiscono a proteggersi dai virus. Gestione delle patch, virtualizzazione del software, autorizzazioni per l'accesso degli utenti ai computer aziendali, controlli degli accessi per file e settori della rete nonché ulteriori provvedimenti integrano le consuete misure di sicurezza. Non verranno approfondite qui le singole possibilità. Una fonte esauriente su questo argomento è il Manuale per la protezione di base pubblicato dall'Ufficio Federale per la sicurezza della tecnologia informatica (BSI).

Purtroppo le misure tecniche da sole non sono sufficienti a proteggere efficacemente la rete di una società. Le misure di sicurezza devono essere accettate e rispettate da dipendenti e collaboratori. Le direttive stabilite dalla dirigenza aziendale forniscono le indicazioni in merito all'utilizzo di computer, supporti dati e altre informazioni critiche per la sicurezza. Sono inoltre da tenere presenti le condizioni generali legali ed etiche. Le misure di protezione devono rispecchiarsi nella struttura dell'organizzazione. Ad esempio, si potrebbe decidere di sanzionare le infrazioni a tali direttive. In ultimo, tutti i dipendenti e i collaboratori dovrebbero essere informati sulle fonti di pericolo in Internet e nelle attività aziendali di tutti i giorni. L'attenzione dei dipendenti associata a misure tecniche di prevenzione possono mantenere i computer di un'azienda liberi da malware.