Le minacce
del 2007

e previsioni
per i prossimi 6 mesi

TREND MICRO
Securing Your Web World

Indice

In breve

Lo scorso anno, il report *2006 Annual Roundup and 2007 Forecast* (*The Trend of Threats Today)* di Trend Micro aveva previsto come principale minaccia di sicurezza per il 2007 un'ondata preponderante di minacce veicolate tramite il Web. Queste minacce includono un ampio ventaglio di attacchi perpetrati attraverso Internet, sono tipicamente costituite da più componenti, generano un elevato numero di varianti e mirano a un target relativamente ristretto. Una previsione fatta su una base di continuità rispetto alle caratteristiche di “focus elevato/diffusione limitata” registrate con alcuni attacchi sferrati nel 2006.

Trend Micro aveva inoltre previsto che la crescita e l'espansione delle reti bot durante il 2007 si sarebbe prevalentemente nutrita di metodi innovativi, tecniche ingegnose di social engineering e sfruttamento delle vulnerabilità software. I dati indicavano anche che il crimeware sarebbe cresciuto a tal punto da diventare la causa prevalente di minacce dal 2007 in avanti.

Mettendo in evidenza le minacce circolate nel 2007 risulterà evidente che tutte le previsioni fatte sono diventate realtà, alcune delle quali anche con modalità interessanti.

La capacità di trasformazione dello scenario delle minacce richiede un passo avanti rispetto al concetto tradizionale di codice pericoloso. Oggi le minacce digitali sono più che mai diffuse: possono colpire un utente semplicemente perché possiede un PC vulnerabile, perché si collega a siti Web affidabili che in realtà sono stati compromessi, perché clicca su un link apparentemente innocuo, o perché fa parte di un network che subisce un attacco di tipo Distributed Denial of Service.

Nei dati presentati di seguito, Trend Micro riassume tutte le minacce, le tendenze del malware e gli eventi salienti inerenti la sicurezza verificatisi nel corso del 2007. Le vittime di tali attacchi includono gruppi di interesse, singoli utenti e, in alcuni casi, anche intere nazioni. Tutti questi esempi dimostrano chiaramente la necessità di adottare metodi più performanti per combattere le minacce del Web. Tutti i dati forniti in questo report sono stati raccolti da TrendLabs, l'organizzazione di ricerca, analisi, esame e supporto di Trend Micro specializzata nelle minacce globali.

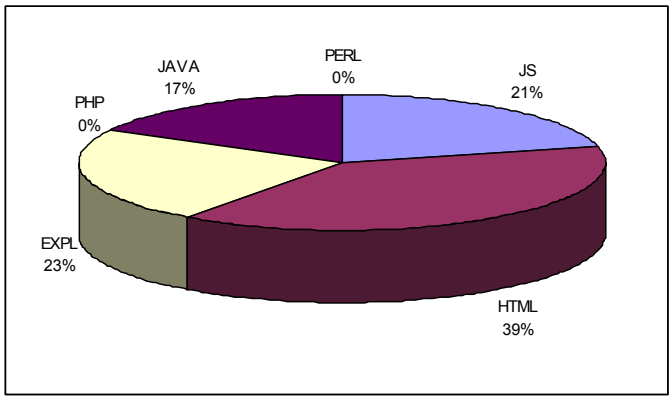
Vulnerabilità del software e delle infrastrutture

Le vulnerabilità del software e delle infrastrutture riguardano il modo in cui i programmi (sistemi operativi o applicazioni software) o le infrastrutture (come le architetture di rete, gli abilitatori di comunicazioni mobili ecc.) sono stati progettati o configurati per gestire determinati dati. Spesso esistono all'interno del programma buchi causati da sviste di programmazione, da configurazioni errate o da altri fattori che mettono a rischio di utilizzo illecito alcune parti del programma o del sistema. In genere queste vulnerabilità sono quelle che consentono ai cybercriminali che agiscono da remoto di creare exploit in grado di eseguire comandi illeciti sul sistema infetto. Le minacce che colpiscono le tecnologie di base sono particolarmente preoccupanti in quanto le nuove implementazioni vanno a inserirsi su un ambiente che ha già rivelato eventuali falle.

In senso lato, i programmi che subiscono con maggiore probabilità tali exploit sono applicazioni ampiamente diffuse e molto popolari fra cui anche lettori multimediali, applicazioni office e addirittura gli stessi programmi per la sicurezza.

Tecnologie Web

Le analisi di HouseCall relative alle minacce del Web 2.0 effettuate nel 2007 dimostrano che l'exploit Windows Animated Cursor (EXPL_ANICMOO) è stato quello di maggiore rilievo su scala mondiale. Ciononostante, se si effettua l'analisi sulla base dei componenti, i codici HTML superano i codici EXPL in termini di importanza. Un fatto attribuibile al numero di rilevamenti IFRAME maligni nel 2007. I rilevamenti JavaScript seguono con il 21%.



Segmentazione minacce Web per tipologia di componenti

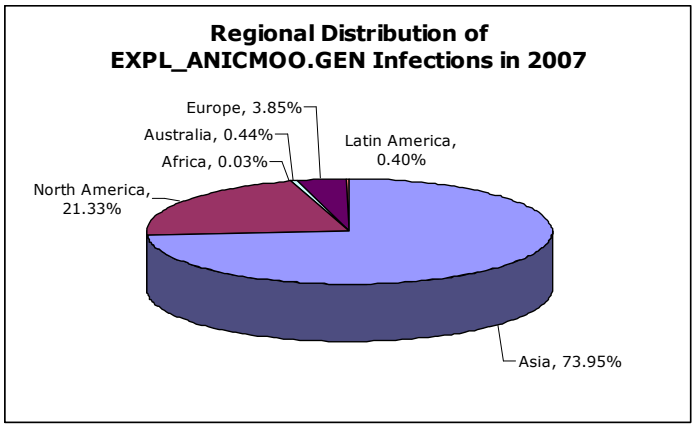
Facile, no? Gli attacchi .ANI in cima alla classifica

La prevalenza di tecniche di attacco con cursore animato e i relativi report di contagio hanno obbligato Microsoft a rilasciare una patch straordinaria lo scorso 3 aprile dopo un periodo di propagazione di un paio di settimane.

La vulnerabilità che viene sfruttata è nel modo in cui Windows gestisce i cursori animati. .ANI è un formato di file utilizzato per leggere e salvare puntatori di mouse animati; essa agisce come una pellicola di film o una striscia di cartone animato in quanto è composta da diversi fotogrammi fissi programmati per apparire in una sequenza ben definita, così che il puntatore del mouse sembri muoversi. Il formato presenta una struttura di file alquanto semplice, dove solo la seconda o ultima parte del blocco di un file .ANI maligno è responsabile delle attività illecite.

Top Ten degli exploit del 2007	% rispetto al totale degli exploit	CVE
EXPL_ANICMOO.GEN	54%	CVE-2007-0038
EXPL_WMF.GEN	18%	CVE 2005-4560
EXPL_EXECOD.A	9%	CVE-2006-4868
EXPL_DHTML.C	5%	CAN-2004-1319
EXPL_SSLICE.GEN	4%	CVE-2006-3730
EXPL_IFRAMEBO.A	2%	CVE-2006-4777, CAN-2004-1050
EXPL_MHT.AF	2%	CAN-2004-0380
EXPL_MS04-028.A	2%	CAN-2004-0200
EXPL_DHTML.G	1%	CAN-2004-1319
EXPL_TXTRANGE.A	1%	CVE-2006-1359

HouseCall è lo strumento di scansione online gratuito messo a disposizione dal sito Web di Trend Micro. I dati del presente report derivano dalle analisi relative al 2007.



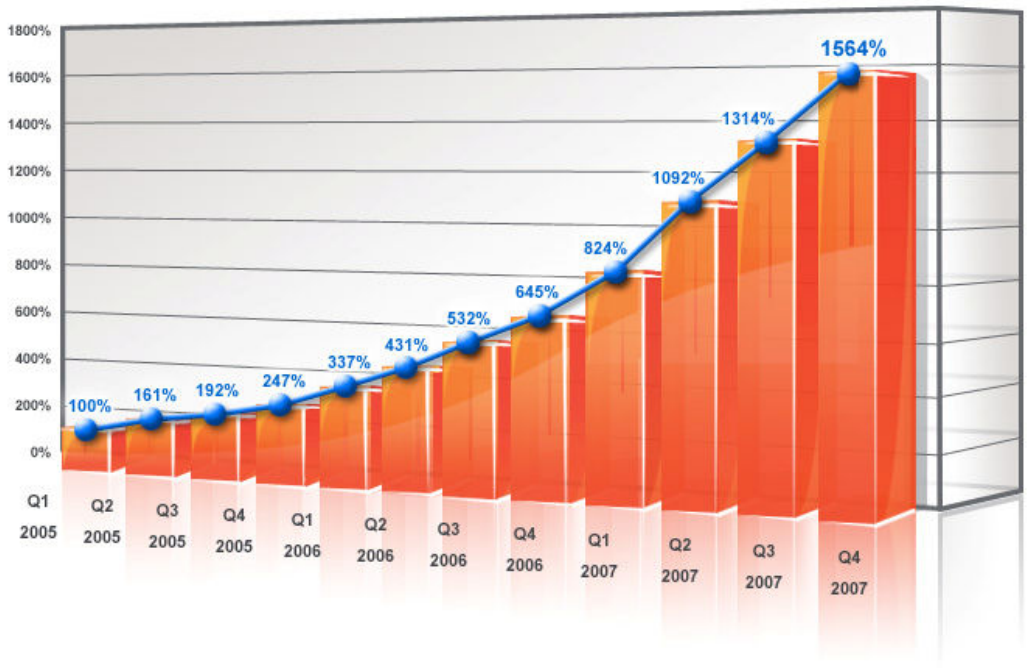
La maggioranza dei suoi contagi (74%) nel 2007 ha riguardato l'Asia. Lo stesso vale per una minaccia correlata rilevata come TROJ_ANICMOO.AX che nascondeva l'exploit al suo interno: il 64% dei computer infettati da questa minaccia si trova infatti in Cina. Il

discreto successo ottenuto colpendo gli utenti asiatici, considerando la mancanza di complessità della tecnica di attacco, riflette l'interesse verso i cursori animati in questa regione, oltre a una certa mancanza di informazione circa la sicurezza nella loro installazione e nel loro utilizzo. Il numero di contagi di EXPL_ANICMOO.GEN è diminuito solo nel mese di ottobre 2007.

Il lato oscuro del Web

Durante gli ultimi anni il social networking e altri strumenti di comunicazione hanno contribuito ad aumentare la dimestichezza degli utenti nei confronti di Internet, moltiplicando le occasioni di interazione. Nel tempo, con il concretizzarsi di tale evoluzione, anche le aziende si sono sentite sempre più sicure nell'integrare funzioni, applicazioni od oggetti remoti all'interno delle loro pagine Web. Inoltre, sempre più spesso le aziende cercano di sfruttare questi nuovi tool creando comunità di utenti o aprendo i loro siti ai più differenti livelli di input da parte degli utenti. Se da un lato questo rende il Web molto più allettante e interessante, dall'altro implica rischi nuovi e mutevoli. Quest'anno ha conosciuto una enorme crescita di attacchi basati sul Web che non fa che confermare quanto sopra.

La seguente tabella riporta la crescita della minacce Web in base alle rilevazioni di Trend Micro fra il 2005 e la fine del 2007. Si definisce minaccia Web qualsiasi minaccia si avvalga del Web per agevolare il cyber-crimine. Per dirlo con parole semplici, la maggioranza dei cyber-criminali cerca ora di gestire le funzionalità offerte dal Web al fine di ottenere profitti. Attraverso differenti meccanismi di attacco, Trend Micro ha rilevato come siano stati utilizzati metodi e tecniche ben diversificati per perpetrare attacchi di successo nei confronti degli utenti.



Scripting multi-sito e interazioni sfruttabili

Le vulnerabilità di scripting multi-sito, ad esempio, sono la suscettibilità delle applicazioni ad eseguire codice arbitrario in presenza di dati inaspettati. Due tecniche di attacco di scripting multi-sito emerse quest'anno sono EXPL_YAHOXSS.A, che sfrutta una vulnerabilità multi-scripting di *Yahoo! Mail*, e JS_QSPACE.A, che utilizza anch'essa lo scripting multi-sito per attaccare gli account di *MySpace*.

Vulnerabilità	Rilevamento	Data di segnalazione	Descrizione
Vulnerabilità scripting multi-sito di MySpace	JS_QSPACE.A	2 dicembre 2006	Reindirizza gli utenti verso un URL di phishing
Vulnerabilità scripting multi-sito di Yahoo! Mail	EXPL_YAHOXSS.A	19 giugno 2007	Codice exploit Proof-of-concept (POC)

EXPL_YAHOXSS.A, che è il rilevamento associato a un paio di componenti che operano insieme per prendere il controllo della sessione Yahoo! Mail attiva di un utente infetto, viene innescato grazie a un unico click su un link che appare proprio come quello che invia ai risultati di ricerca di Yahoo!. JS_QSPACE.A, dal canto suo, prende di mira gli utenti di *MySpace*. Quando è attivo sfrutta una vulnerabilità di scripting multi-sito di *MySpace* per reindirizzare l'utente verso un URL di phishing. Contiene inoltre un codice per editare il profilo degli account sottratti, aggiungendovi un filmato anch'esso contenente l'URL di phishing. Quando altri utenti visitano l'account *MySpace* oggetto dell'attacco, il codice JavaScript viene scaricato ed eseguito sul profilo privato dell'utente. E a quanto sembra, la grande popolarità dei siti di social networking li rende dei vettori di contagio ideali per gli autori di malware.

A luglio si è diffusa la notizia di una vulnerabilità di scripting multi-browser fra *Firefox* e *Internet Explorer*. Rilevata per la prima volta il mese precedente, giugno 2007, questa vulnerabilità riguarda la modalità con cui IE passa le informazioni a Firefox, facendo sì che Firefox esegua codice JavaScript quando viene cliccato un link. Questo avviene per via della registrazione di un certo Uniform Resource Identifier (URI) denominato “firefoxurl” nel Registry di Windows quando viene installato Firefox. Quando certi parametri rientrano nell'URI “firefoxurl”, essi vengono interpretati da Firefox come opzioni, senza bisogno di verifica. Microsoft ha rilasciato un avviso di sicurezza a questo riguardo (*La vulnerabilità di gestione URL in Windows XP e Windows Server 2003 con Windows Internet Explorer 7 potrebbe consentire l'esecuzione di codice remoto*), e una patch a novembre. Questo esempio testimonia come gli autori di malware siano davvero determinati a scoprire nuove vulnerabilità per i loro scopi illeciti.

Le vulnerabilità del Vector Markup Language

Le vulnerabilità presenti in una serie di altri elementi basati su Web hanno enfatizzato la necessità di prestare molta attenzione quando si naviga o si clicca su dei link. Le vulnerabilità del Vector Markup Language in Internet Explorer (CVE-2007-0024) sono state sfruttate anche dopo il rilascio delle relative patch da parte di Microsoft. Diverse varianti di questi attacchi VML si sono susseguite fino ad aprile 2007.

Rilevamento	Data di avviso	Descrizione
EXPL_EXECOD.C	16 gennaio 2007	Permette a utenti remoti di eseguire comandi sul sistema colpito
HTML_VMLFILL.I	14 gennaio 2007	Scarica ed esegue file
JS_DLOADER.KQZ	2 febbraio 2007	Scarica ed esegue file
HTML_IFRAMEBO.AE	12 febbraio 2007	Scarica ed esegue file
HTML_IFRAMEBO.AC	16 marzo 2007	Scarica ed esegue file
JS_IFRAMEBO.BG	29 aprile 2007	Scarica ed esegue file

Vulnerabilità nei browser e nei plug-in di terze parti

A giugno si è scoperto che *Safari 3 Beta for Windows* aveva un problema di gestione del protocollo URL. A luglio, poco dopo il lancio dell'*iPhone*, è stata rilevata una certa vulnerabilità anche in *Safari 3.* Questo sta a significare che l'uso omogeneo di componenti base da una piattaforma operativa vulnerabile risulta logicamente in una tecnica di attacco anche quando il sistema evolve verso un nuovo fattore forma come ad esempio i gadget.

Anche *Safari 3.0.03* per Windows conteneva una vulnerabilità che permetteva alle zone locali di accedere a domini esterni. Una prova delle previsioni fatte in precedenza, per le quali le applicazioni multi-piattaforma avrebbero anch'esse dato adito a vulnerabilità multi-piattaforma e relativi attacchi. Senza bisogno di grandi riprogettazioni è stato abbastanza semplice violare il porting di Safari in meno di tre (3) giorni.

La maggior parte dei lettori multimediali, come Windows Media Player, Apple QuickTime, VLC e molti altri ancora, supporta un'ampia gamma di formati media, fra cui diverse tipologie di file audio e video. Alcuni formati di file sono intrinsecamente non sicuri soprattutto se sono file .ASX o .ASF, ovvero pure incapsulazioni di video con un reindirizzatore URL. I lettori possono avere anche funzioni supplementari per negoziare connessioni di rete, funzioni anch'esse potenzialmente oggetto di abusi se erroneamente configurate.

Per fare un esempio, a settembre *Firefox* ha dovuto rilasciare una patch per risolvere una vulnerabilità multi-applicazione nella versione 2.0.0.7; nello specifico si trattava di una modalità con cui il browser può essere obbligato a eseguire un codice quando un file *Apple QuickTime* appositamente creato viene avviato usando il plug-in *Apple QuickTime*. La streaming di contenuti è un'ottima funzione, ma generalmente richiede un media server proxy raramente installato invece dalle aziende. La soluzione più rapida è costituita dal lasciare aperte le porte del firewall. Per molti utenti si tratta di un'intrusione che non aspetta altro di verificarsi - e spesso è davvero così.

Browser Helper Object
I Browser Helper Object sono degli add-on realizzati da terze parti che estendono le funzionalità del browser e generalmente integrano scorciatoie verso servizi particolarmente diffusi. A causa però della sua grande popolarità, (soprattutto in Internet Explorer attraverso ActiveX), questa funzione si è trasformata in uno dei vettori più comuni e sfruttati per le attività di contagio.

Molti esemplari di adware e spyware, e anche malware, hanno iniziato a travestirsi da BHO nel 2006. Nel 2007 l'attività BHO ha registrato un picco nel mese di aprile, scendendo quindi al minimo ad agosto. Un evento che sicuramente non ha destato sorpresa, data la fortissima migrazione dell'utenza verso browser alternativi come Firefox, Opera e persino Safari.

Altra ragione è il rilascio pubblico di Windows Vista e del suo browser IE 7 che aggiunge un numero maggiore di difficoltà all'installazione di BHO illeciti. Comunque la migrazione verso browser alternativi, in particolare Firefox, ha verosimilmente portato all'esecuzione di nuovi attacchi sotto forma di plug-in pericolosi, ancora una volta prodotti da terze parti. Gli utenti devono essere un po' più attenti in quest'ambito, in quanto BHO, plug-in e altri add-on non sono differenti da altri componenti di codice che possono essere utilizzati per scopi diversi.

Riassumendo:
1. Le vulnerabilità delle tecnologie usate a fondamento delle attuali infrastrutture digitali sono in cima alla lista dal punto di vista dell'attenzione a loro rivolta, dato il loro potenziale contributo allo scenario globale delle minacce.

2. Il codice legacy è stata la rovina di numerosi nuovi prodotti lanciati sul mercato a causa del mutevole ciclo di vita del software e alle considerazioni eseguite in passato circa il rapporto di precedenza tra sicurezza e funzionalità.

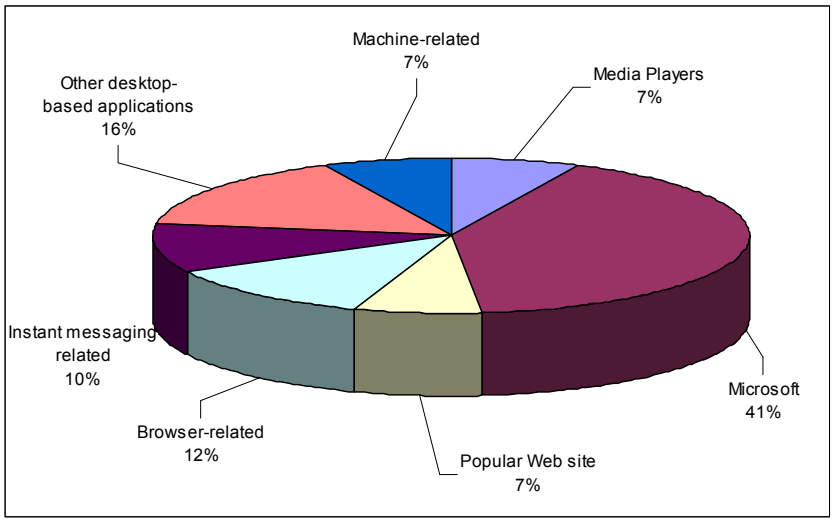
3. Gli strumenti tradizionalmente utilizzati per migliorare l'esperienza online degli utenti vengono ora rivisitati dai cybercriminali per diventare tra i principali vettori di attacchi illeciti.

4. Le tradizionali minacce malware di virus e Trojan, spesso attribuite all'improvvisa follia di un aspirante hacker, negli ultimi tre anni sono state sostituite in maniera mirata da minacce progettate in condivisione e scritte da professionisti man mano che i cybercriminali si accorgono delle numerose opportunità lasciate facilmente accessibili nonostante la diffusione e l'utilizzo del mezzo online si diffondano ormai in tutto il mondo.

5. Prende sempre più piede il codice user-generated che abbandona i tradizionali cicli di vita produttivi in favore di feedback pubblico e altre forme di auto-pubblicazione: queste pratiche lasciano però la porta aperta a opportunità pericolose e alla facile diffusione di minacce miste in ambito sia aziendale che domestico.

Applicazioni desktop: la ricerca dei bug continua

Anche il 2007 ha registrato la sua quota di bug in diverse applicazioni basate su desktop. Le vulnerabilità di Windows sono continuate a crescere a migliaia. Come visto in una sezione precedente, gli esemplari di malware che sfruttano la vulnerabilità del cursore animato (CVE-2007-0038) sono stati la causa del maggior numero di contagi mensili dal momento della scoperta della falla da aprile fino a ottobre (EXPL_ANICMOO.GEN).



Nell'arco del 2007 i ricercatori di Trend Micro hanno osservato che gli autori di malware sembrava stessero analizzando le informazioni riportate dagli ultimi Security Bulletin, sviluppando di conseguenza un codice sulla base dei dati raccolti. Ad esempio, agli inizi di febbraio 2007 Microsoft ha pubblicato il proprio Security Bulletin. TROJ_DROPPER.FC è stato rilevato solo una settimana dopo, sfruttando una vulnerabilità di *MS Excel* riportata proprio nel bollettino appena uscito. Un altro esempio è stato TROJ_DROPPER.WN, che ha sfruttato una vulnerabilità di *MS Word* pochi giorni dopo l'annuncio da parte di Microsoft. Nel corso dell'anno si sono comunque verificati anche casi in cui le vulnerabilità sono state scoperte in un momento in cui non vi erano patch disponibili: ad esempio nel caso di *Microsoft PowerPoint* (febbraio), dei file di aiuto di Windows e del Domain Name System (DNS) Server Service (aprile), e di *Microsoft Access* (settembre). In casi come questi gli autori del malware contano sulla cosiddetta “finestra di vulnerabilità”, ovvero il tempo che intercorre fra il momento in cui vulnerabilità si diffonde tra il pubblico e il momento in cui viene emessa la relativa patch.

Altre applicazioni basate su desktop sono state colpite da attacchi malware progettati come prova concettuale (proof-of-concept), e in particolare:

Vulnerabilità	Rilevamento	Data di segnalazione	Descrizione
Sun Solaris TelNet Remote Authentication Bypass, una nota vulnerabilità trovata nel demone Sun Solaris 10/11 TelNet, in.telnetd	ELF_WANUK.A	28 febbraio 2007	Si è propagata attraverso le reti
Piattaforma iPodLinux con installata la Graphical User Interface (GUI) Podzilla e Podzilla2	ELF_PODLOSO.A	6 aprile 2007	Virus ELF Proof-of concept (POC)
Vulnerabilità in un componente ThunderServer ActiveX nel codice Web Thunderbolt ThunderServer.webThunder.1	JS_AGENT.KGN	14 giugno 2007	Scarica un file
Adobe Reader 8.1 e versioni precedenti. Adobe Acrobat Standard, Professional, e Elements 8.1 e versioni precedenti. Adobe Acrobat 3D	EXPL_PIDIEF.A	16 ottobre 2007	Codice exploit Proof-of-concept (POC)

A testimonianza dell'aumento di minacce Web localizzate, le vulnerabilità sono state sfruttate nelle applicazioni giapponesi *Ichitaro* (word processing) e *Lhaz* (archiviazione), e in altre applicazioni che non sono target tipici o prevedibili. Ad esempio:

Vulnerabilità	Rilevamento	Data di segnalazione	Descrizione
Media player *XMPlay versione 3.3.0.4*, in cui un file .ASX appositamente costruito può causare un buffer overflow	TROJ_MPEXPL.A	8 dicembre 2006	Rilascia ed esegue un file
Lhaca versione 1.20, un'applicazione giapponese di archiviazione	TROJ_LHDROPPER.A	26 giugno 2007	Verifica se la macchina infetta ha installato un sistema operativo giapponese e poi rilascia il file
Vulnerabilità in *Ichitaro*, una applicazione di word processing diffusa in Giappone prodotta da *JustSystem*	TROJ_TARODROP.Q	3 agosto 2007	Rilascia ed esegue un file
LHAZ versione 1.33, un'applicazione giapponese di archiviazione	TROJ_LZDROPPER.A	20 agosto 2007	Verifica se la macchina infetta ha installato un sistema operativo giapponese e poi rilascia il file

In fase di esecuzione il payload di questi attacchi malware include il download di altri file e l'installazione di una backdoor. Le vulnerabilità presenti nelle diverse applicazioni ammontano a migliaia, una situazione resa ancor più complessa dall'esistenza di una tecnica di test software nota come “fuzzing”, che sottopone le applicazioni a una raffica di input random volti a determinare quale punto di un programma possa causare un crash o un errore. Se è vero che una pratica di questo tipo non è maligna di per sé, essa è però al servizio degli autori di malware impegnati nello sviluppo di exploit su larga scala.

Se è vero che il rilevamento delle vulnerabilità sta diventando sempre più automatizzato, è altrettanto vero che gli autori del malware si stanno a loro volta indirizzando verso obiettivi ancora più ambiziosi. Ecco dunque l'emergere di un'ampia gamma di exploit pacchettizzati in toolkit che, uniti ai tool basilari per la creazione di malware customizzato, offrono ai cybercriminali tutto ciò di cui hanno bisogno per architettare nuovi attacchi. I più diffusi di questi kit, MPack e IcePack, vengono presentati più avanti in questo report nella sezione intitolata “*L'economia digitale sommersa*”.

Widget: la prossima rivoluzione

Il concetto di widget, mini-applicazioni che forniscono agli utenti informazioni rapide e l'accesso ai tool usati più di frequente, introduce un altro aspetto notevolmente vulnerabile del Web. A prescindere dalla piattaforma operativa usata, i widget sono soggetti ad attacchi maligni a causa dell'uso da parte degli sviluppatori di codice Asynchronous JavaScript e XML (AJAX) praticamente incuranti dell'aspetto sicurezza, facendone così dei potenziali bersagli di attacchi di scripting multi-sito.

Un difetto nel controllo ActiveX che potrebbe causare un buffer overflow stack-based è il responsabile della possibile esecuzione di un codice random in *Yahoo! Widgets versione 4.0.3* (noto anche come Konfabulator), il motore che gestisce programmi o tool virtuali interattivi quali stock ticker che visualizzano le quotazioni di borsa, calendari, sveglie, calcolatrici, ecc. La Versione 4.0.5 risolve questa specifica vulnerabilità.

Microsoft Vista Gadgets è la versione dei widget sviluppata da Microsoft. All'inizio di agosto è stata rilevata una vulnerabilità che permetteva a un cybercriminale operante da remoto di attivare il codice sul computer di un utente con i privilegi dell'utente loggato. Nel caso in cui un utente si fosse abbonato a un feed RSS maligno nel Feed Headlines Gadget o avesse aggiunto un file contatti maligno nel Contacts Gadget, o avesse cliccato su un link maligno nel Weather Gadget, un cybercriminale avrebbe potuto caricare codice illecito nel sistema. Il 14 agosto scorso Microsoft ha rilasciato un aggiornamento di sicurezza per fare fronte a questa problematica.

Le minacce mobili: pronte a colpire

Il numero di smartphone che usano telefoni basati su sistema operativo è destinato ad aumentare con un tasso di crescita annuo pari al 30% per i prossimi cinque anni, mentre il volume di unità di smartphone a livello globale supera già quello dei laptop, secondo i

dati della società di analisi di mercato In-Stat (http://www.instat.com/press.asp?Sku=IN0703823WH&ID=2148). Questa popolazione di dispositivi mobili rappresenta un obiettivo sempre più invitante per qualsiasi hacker che desideri fare profitti in maniera illecita.

Le stime di In-Stat parlano inoltre di una cifra come 8 milioni di telefoni cellulari andati perduti nel 2007, 700.000 dei quali erano smartphone (http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026944). Il rischio maggiore per questo genere di dispositivi è il potenziale in termini di informazioni perse o compromesse. Oggi vediamo già notizie inerenti le quantità di laptop contenenti dati sensibili che vanno smarriti; probabilmente vedremo titoli simili nel prossimo futuro anche per quanto riguarda gli smartphone. Dato che l'ultima generazione di cellulari permette di inserire memory card grandi fino a 8 GB, questa è una probabilità alquanto realistica. Al di là poi dei dati compromessi, i rischi maggiori per i dispositivi mobili riguardano le perdite finanziarie attraverso episodi di frode oltre che la perdita di produttività dovuta agli attacchi malware.

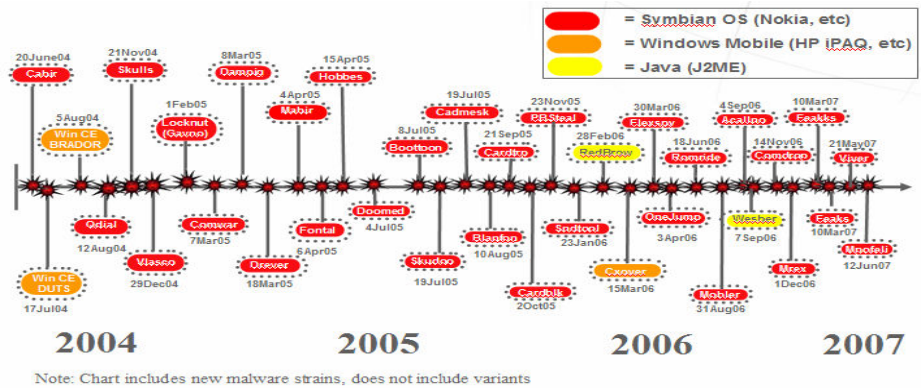
Le previsioni parlano di una prossima evoluzione delle minacce in ambito mobile che avverrà in maniera del tutto simile a quella verificatasi per i PC. I sistemi operativi Microsoft rappresentano un bersaglio allettante per gli autori di malware per una serie di motivi: innanzitutto perché il sistema operativo Windows permette di raggiungere una vasta fetta di popolazione. Anche se sono stati disponibili sistemi operativi come IBM OS/2, Mac OS e Linux, è Microsoft Windows ad aver avuto l'ingrato onore di essere l'obiettivo primario dei malintenzionati del malware. Perché focalizzarsi su piattaforme di nicchia quando puoi scrivere un codice in grado di infettare milioni di PC Windows?

In maniera simile, i sistemi operativi mobili stanno diventando motivo di attrattiva per gli autori di malware. Le principali piattaforme mobili sono diventate abbastanza estese da attrarre l'interesse di questi personaggi. Le piattaforme dispongono di una bandwidth di rete sufficiente, sotto forma di network HSDPA, EV-DO e WiFi, permettendo di scaricare applicazioni a velocità ragionevole. Esiste poi una diffusa familiarità tecnica con i sistemi operativi mobili sufficiente per mettere gli autori di malware nella condizione di poter manipolare i dispositivi mobili.

Per quanto riguarda la sicurezza di tali dispositivi, lo scenario evidenzia un bilanciamento fra sicurezza e facilità d'uso. Creare un dispositivo eccezionalmente sicuro determina in genere dei limiti nella semplicità d'uso o restrizioni nello sviluppo software. Un dispositivo mobile facile da usare soffre tipicamente di una sicurezza appena sufficiente. Ad esempio, avere una semplicità d'uso ottimale vorrebbe dire non dover digitare alcun PIN (Personal Identification Number) per accedere a un determinato dispositivo; ma la scomodità di dover inserire un PIN garantisce un dispositivo molto più sicuro.

I nuovi dispositivi puntano al mercato focalizzandosi sulla semplicità di utilizzo, perché è questo che fa vendere i prodotti. Raramente i consumatori scelgono di acquistare un nuovo prodotto perché promette più sicurezza; generalmente tendono invece a comprare un dispositivo perché permetterà loro di migliorare i livelli di disponibilità o perché ha un look alla moda. In generale è necessario che si verifichi un problema di sicurezza affinché questo aspetto prevalga sulla semplicità di utilizzo in fase di scelta.

La tabella sottostante mostra come le minacce mobili siano aumentate fra il 2004 e il 2007. Ad oggi, le minacce mobili si sono focalizzate sui maggiori sistemi operativi mobili - Symbian OS (usato da Nokia, Sony Ericsson, e altri produttori di telefonia) e Microsoft Windows Mobile.



Note: Chart includes new malware strains, does not include variants

Impatto delle vulnerabilità e del malware in ambito mobile

Tutti i sistemi operativi hanno delle vulnerabilità, ma sono in genere quelli più diffusi a diventare il principale obiettivo di attacchi. Trend Micro ha identificato nelle applicazioni un numero di vulnerabilità che possono essere usate in attacchi Denial of Service (DoS). Per queste vulnerabilità vengono create apposite patch da parte dei vendor nelle release successive, una pratica che però solitamente non avviene nel caso delle migliaia di dispositivi mobili in circolazione.

Il malware mobile esiste, ma fino ad oggi è stato utilizzato più nella modalità proof of concept che non come fonte di danni diffusi. Il malware mobile che ha generato profitti illeciti, RedBrow, ha colpito nel 2006 i dispositivi mobili che usavano Java.

Gli esemplari di malware utilizzabili per furto di dati sono emersi prima nel 2005 con PBSteal, in grado di sottrarre informazioni telefoniche dai supporti Nokia, e poi nel 2006 con Flexspy, capace di inoltrare informazioni inerenti le chiamate e i messaggi SMS.

Sin dal 2004 sono stati rilevati nell'ambito dei moderni sistemi operativi mobili esemplari di malware capaci di generare problemi ai dispositivi o addirittura comprometterne l'operatività. Se da un lato le informazioni presenti sulle memory card e sui principali supporti storage possono essere distrutte da tali esemplari di malware, il funzionamento del dispositivo infettato può essere invece ripristinato eseguendo un “hard reset” reimpostando i settaggi alla configurazione di fabbrica. Le istruzioni per eseguire questo procedimento sono generalmente riportate sul manuale o sul sito del produttore.

Apple iPhone e iPod touch

Lo scenario mobile è eccezionalmente dinamico. A partire da febbraio 2008 Apple aprirà il sistema operativo usato per l'iPhone e l'iPod touch a sviluppatori terzi. Dato il profilo elevato e la quantità di dispositivi Apple circolanti, l'apertura del sistema operativo costituirà un'opportunità per provocare danni digitali da parte di coloro che vogliono macchiare l'immagine, ormai icona, dei prodotti mobili di Apple.

Google Android
Google ha annunciato la formazione della Open Handset Alliance, un'entità tramite cui rilasciare Android, una piattaforma mobile gratuita e aperta. Secondo Google (http://code.google.com/android/what-is-android.html), Android è uno stack software per dispositivi mobili che include sistema operativo, middleware e applicazioni principali. Se Android riesce a conquistare il mercato, aggiudicandosi una fetta rilevante del segmento smartphone, esso diventerà probabilmente un bersaglio per gli autori di malware.

Widget
Come discusso in un paragrafo precedente, i widget sono delle mini-applicazioni che permettono agli utenti di prendere informazioni dai loro siti preferiti, in particolare usando feed RSS. Queste piccole applicazioni offrono la possibilità di dare un senso al flusso di informazioni. I widget costituiscono un vettore interessante per quanto concerne gli attacchi, come dimostrato dall'esemplare di malware “Secret Crush” che ha assunto le sembianze di un widget Facebook per autoinstallarsi su qualcosa come un milione di PC tra la fine del 2007 e l'inizio del 2008. Se i widget iniziassero a proliferare sui supporti mobili come è avvenuto nel caso dei PC, potrebbero diventare un vettore di attacco all'interno dello scenario mobile.

Java e AJAX
Il linguaggio di programmazione Javascript insieme ad Asynchronous JavaScript e XML (AJAX) offrono un potenziale punto d’ingresso per manomettere i dispositivi mobili; questi ultimi in genere vengono venduti con Java 2 Mobile Edition (J2ME). AJAX è un'estensione del linguaggio di programmazione JavaScript che può essere usata per aumentare la reattività dei siti Web automatizzando lo scambio di informazioni fra il software del browser e i server Web backend. I tool AJAX sono largamente utilizzati in molteplici modi da siti come Google Maps, Yahoo e MySpace.

Mentre i dispositivi mobili erano soliti operare in un loro mondo Web fatto di siti appositamente progettati, le dimensioni del Web mobile e di quello PC si stanno unendo. Gli attacchi di scripting che prendono di mira i PC potrebbero quindi estendersi anche ai dispositivi mobili.

Blackberry
Blackberry è stato un pioniere del mercato dei dispositivi aziendali portatili, proponendo l'uso dell'e-mail sui propri dispositivi e la gestione backend con Blackberry Enterprise Server (BES). BES consente di bloccare i dispositivi e cifrare i dati dell'utente, mitigando le potenziali minacce: agli utenti può infatti essere vietata l'installazione di applicazioni e i dati vengono messi in sicurezza grazie al processo crittografico.

Le vulnerabilità presenti nella soluzione Blackberry si presentano nel momento in cui un amministratore non mette in sicurezza il dispositivo o non codifica i dati. Anche se BES offre questa funzione, sono molti gli amministratori che scelgono di non avvalersene per evitare lamentele da parte degli utenti sulla diminuzione delle prestazioni del dispositivo. In questo modo però i dispositivi diventano vulnerabili nel caso in cui l'utente installi software di terze parti inaffidabile o Trojan.

Per gli utenti dei dispositivi Blackberry che non si connettono alle aziende tramite BES, i rischi assomigliano molto a quelli rilevati su altri sistemi operativi per dispositivi mobili. Ad esempio, un produttore software vende una soluzione che gira su Windows Mobile,

Symbian e Blackberry in grado di telefonare e inviare SMS all'interno e all'esterno all'insaputa dell'utente.

Riassumendo

1. Gli ultimi dieci anni sono stati segnati da exploit ai sistemi operativi dovuti a compromessi fra sicurezza e funzionalità. Nell'ultimo triennio TM ha rilevato qualche passo indietro da parte di questo tipo di attacchi, a fronte dell'impegno delle aziende nel verificare meglio il software in termini di sicurezza. Oggi gli attacchi sono decentralizzati, nel senso che invece di rivolgersi al sistema operativo sottostante si concentrano sulla varietà di applicazioni desktop e server. Il nuovo mantra è comunque "patch, patch, patch" ma ora include tutte le applicazioni esistenti a parte il sistema operativo o la piattaforma.

2. Ciascuna nuova tecnologia introdotta negli ultimi anni e da subito applicata a un uso di massa ha dovuto affrontare diverse problematiche. Questo ha di conseguenza generato delle opportunità volte a favorire un approccio corretto sin dall'inizio, e laddove questo non sia possibile, a impegnarsi successivamente per trovare il giusto equilibrio fra funzionalità e sicurezza al fine di supportare il posizionamento della tecnologia o del dispositivo sul mercato.

3. I dispositivi palmari, mobili e alla moda che permettono un uso condiviso multi-piattaforma/fattore-forma rappresentano un ben noto vettore di minacce data la loro rapidità di raggiungere il mercato di massa a costi sempre più contenuti. Sembra che le attuali policy aziendali non abbiano ancora preso atto del fatto che i dipendenti che utilizzano dispositivi non gestiti in ambiente di ufficio rappresentano dei cavalli di Troia virtuali pericolosi per l'azienda stessa.

Minacce a impatto elevato

Le minacce a impatto elevato sono minacce che hanno la capacità di causare danni ben localizzati in una specifica regione, comunità, azienda o gruppo. Esse sono costituite da attacchi mirati e attacchi su aree geografiche.

Attacchi su aree geografiche

Le minacce a impatto elevato possono essere localizzate e su scala regionale, o mirate a specifici gruppi di individui. Anziché esaminare i contagi di malware su scala globale, un'analisi nel dettaglio della specificità territoriale ha una rilevanza maggiore, seguendo la natura delle minacce Web. Di seguito un riepilogo degli esemplari di malware più diffusi nel 2007 suddivisi per aree geografiche:

Area geografica	Malware più diffuso sulla base dei rilevamenti
Asia Pacifico e Australia (tranne Cina e Giappone)	Varianti TROJ_ZLOB.CHK, HTML_WUKE.AF, WORM_SILLYFDC
Cina	Varianti PE_VIRUT.A, TSPY_FRETHOG, TSPY_ONLINEG, TSPY_QQPASS
Giappone	PE_VIRUT.K, TSPY_LINEAGE e diverse varianti WORM_NUWAR.CQ
Europa, Medio Oriente e Africa	Diverse varianti WORM_NUWAR e TROJ_SMALL
America Latina	WORM_RONTKBR.GEN, alcune varianti TSPY_BANCOS, TSPY_BANPAES, TSPY_BANKER
Nordamerica	Varianti WORM_BRONTOK.HS, EXPL_ANICMOO.GEN, WORM_NUWAR

Dati raccolti attraverso i portali Trend Micro per la segnalazione degli utenti

Trojan generici a bassa pericolosità sono in grado di diffondersi su computer di tutto il mondo, e la presenza di varianti WORM_NUWAR in quasi tutte le aree geografiche sta a significare un attacco più ampio (vedere la sezione intitolata *Minacce distribuite*); guardando però nel dettaglio dei dati raccolti si rileva la prevalenza di determinate minacce in determinate aree geografiche.

Nella tabella sopra illustrata, l'America Latina appare essere il bersaglio preferito per le famiglie spyware TSPY_BANCOS e TSPY_BANKER. Le varianti di queste famiglie sono note per visualizzare pagine Web che si spacciano per schermate di login legittime di banche brasiliane e del resto dell'America Latina. Gli utenti che cascano nella trappola finiscono col fornire informazioni relative al proprio conto - e quindi accesso al proprio patrimonio finanziario - ai responsabili di questa frode.

Per contro, gli utenti cinesi sono colpiti da una serie di varianti spyware che mirano alla comunità Massive Multiplayer Online Role-Playing (MMORPG) e all'ampia base di utenti di *QQ Messenger*, una applicazione di instant messaging molto diffusa in Cina.

Tecniche di social engineering

Le minacce a impatto elevato includono anche quelle che prendono di mira gruppi di vittime, come ad esempio gruppi di interesse, audience locali o regionali, o determinati segmenti della società. Gli autori del malware stanno diventando sempre più abili nel mettere a punto strategie la cui puntualità è tale da ingannare gli utenti rispetto all'autenticità di quanto viene offerto. Di seguito un esempio di eventi di portata mondiale utilizzati nel 2007 per sferrare attacchi:

Episodio di vita reale	Nome del malware rilevato	Data di rilevamento
Esecuzione di Saddam	TROJ_BANLOAD.BLK	7 gennaio 2007
Uragano Kyrill	TROJ_SMALL.EDW	17 gennaio 2007
Rilascio di Vista	WORM_SOHANAD.U	1 febbraio 2007
Superbowl	JS_DLOADER.KQZ	3 febbraio 2007
Giorno di San Valentino	WORM_NUWAR.AAI	14 febbraio 2007
Rilascio di IE7	PE_GRUM.B-O	31 marzo 2007
Massacro al Virginia Tech	TROJ_BANLOAD.CFU	19 aprile 2007
Film di Harry Potter	TROJ_DLOADER.NKY	22 giugno 2007
Rilascio iPhone	TROJ_AYFONE.A	2 luglio 2007
Lancio libro Harry Potter	WORM_HAIRY.A	4 luglio 2007
Festa 4 luglio negli USA	WORM_NUWAR.FU	5 luglio 2007
Schianto aereo in Brasile	TROJ_BANLOAD.CGL	18 luglio 2007
Penetrazione nel sito Monster.com	HTML_IFRAME.GN	22 agosto 2007
Festa del Lavoro negli USA	WORM_NUWAR.AQK	4 settembre 2007
Campionato football NFL	WORM_NUWAR.AQN	11 settembre 2007
Nomina Primo Ministro giapponese	BKDR_DARKMOON.BG	28 settembre 2007
Manifestazioni birmane	TROJ_MDROPPER.WI	28 settembre 2007
Halloween	WORM_NUWAR.ARI	31 ottobre 2007

Pagine compromesse: abuso della fiducia verso i siti Web legali

L'hacking di siti Web legittimi ha subito una crescita esponenziale durante il 2007, ponendo una delle sfide più pericolose in quanto scalza uno dei modi di dire più vecchi del browsing sicuro: “non visitare siti dubbi”. Uno degli attacchi più degni di nota è stato il famoso “Italian Job”, che ha coinvolto un numero ingente di pagine Web di siti italiani che contenevano IFRAME nascosti rilevati come HTML_IFRAME.CU. La quantità totale di siti colpiti è stata nell'ordine delle migliaia. Insieme, il numero di siti colpiti unito al numero di singole pagine Web per ciascun sito coinvolto formano una cifra a dir poco spaventosa.

L'attacco è stato sferrato all'inizio della stagione italiana delle vacanze, quando gli utenti si presume siano più inclini alla vita sociale che non al lavoro e allo studio. Si ritiene che l'attacco sia stato perpetrato usando il toolkit MPack, creando quindi un precedente circa l'efficacia di tali tecniche. MPack e uno dei suoi contemporanei, IcePack, vengono presentati e discussi in una sezione successiva del presente report, *L'economia digitale sommersa.*

Siti di interesse specifico

Durante la prima settimana di febbraio, il sito ufficiale del Miami Dolphins Stadium era stato violato e ospitava un Trojan silente. La stagione del Super Bowl negli Stati Uniti aveva generato un picco del traffico Web del sito, e gli hacker ne avevano approfittato scommettendo sul successo di questo download drive-by.

Le pagine Web violate rappresentano il punto di partenza delle catene di contagio che reindirizzano gli utenti verso URL che provvedono a introdurre sui sistemi colpiti spyware, keylogger e altri esemplari di malware. Questa catena di contagio forma una strategia che fornisce la flessibilità necessaria in termini di payload: un giorno l'URL maligno mostra semplicemente una pubblicità o un'immagine inerte, poi, il giorno successivo quello stesso URL contiene una backdoor o uno script per l'installazione di malware.

Dato che molte di queste pagine compromesse appartengono a nomi conosciuti, siti legittimi che erano assolutamente privi di insidie prima di ricevere un attacco, anche gli utenti più guardinghi rischiano di essere infettati a loro totale insaputa.

Violazione domini di alto livello

Un'altra tendenza particolarmente rilevante quest'anno è stata la violazione di siti appartenenti al dominio .GOV. Il sito della Nigerian Economic and Financial Crime Commission è stato colpito nel mese di giugno. Nello stesso periodo, le pagine di domini .GOV come i siti della Corte Superiore di Tulare e Madera.courts.ca.gov hanno subito una violazione da parte di spammer specializzati in Search Engine Optimization (SEO). Gli spammer SEO manipolano i risultati di un motore di ricerca distribuendo i termini di ricerca nei siti Web: questi appaiono prima di quelli legittimi nella lista nel momento in cui un utente inserisce una chiave di ricerca prevedibile.

Il sito della Arizona Government University e quello di una contea della California sono stati anch'essi infettati con codice che rimandava a siti pornografici o scaricava altro malware. Lo stesso mese una cosa analoga è accaduta ad alcuni siti governativi asiatici e a un sito cinese specializzato in sicurezza. A novembre inoltrato un sito del governo ucraino è stato colpito dagli hacker, mostrando messaggi pubblicitari inerenti a prodotti per il dimagrimento.

L'aumento del numero di siti colpiti con domini .GOV registrato durante l'anno indica un abuso della fiducia nelle pagine .GOV e la persistente indifferenza da parte dei proprietari dei siti a proteggerli da possibili infiltrazioni.

Un altro modo per abusare della fiducia di domini .GOV e .EDU è l'uso di configurazioni server con nomi violati. Aggiungendo sub-domini maligni al nome legittimo del server di un dominio .GOV o .EDU, gli autori di malware sono riusciti a ingannare gli utenti facendo credere che l'URL fosse legittimo. Nel 2007 c'è stato un aumento dei casi di configurazioni DNS compromesse su diversi siti .EDU e .GOV. I ricercatori sono stati addirittura in grado di identificare gli spammer SEO che facevano esclusivamente lo switch da nomi di domini liberi a domini .EDU e .GOV violati.

Altri attacchi mirati

- La famiglia TROJ_YABE ha colpito la Germania e altre aree di lingua tedesca, oltre ad altri Paesi scandinavi.
- La famiglia TSPY_LDPINCH ha inizialmente colpito la Russia.
- TROJ_BANLOAD.BLK effettuava lo spamming di e-mail in portoghese.
- TROJ_VB.BLV recuperava il fuso orario del sistema e la configurazione del layout della tastiera per determinare se il sistema colpito fosse situato in Estonia, Lituania o Lettonia.
- WORM_SILLY.CQ scaricava diversi file maligni e installava *Chinese Navigation 2.6.0.0*, una toolbar di ricerca diffusa in Cina.
- WORM_WALLA.B verificava innanzitutto se la lingua usata dal sistema fosse arabo o persiano prima di continuare la sua attività.
- TSPY_ONLINEG ha interessato la comunità di online gaming in Asia, in particolare la Cina.

Attacchi contro entità online

Sempre più aziende conducono le proprie attività di business online: in questo modo la sfida e l'opportunità per gli autori di malware si sono fatte alquanto interessanti. *Monster.com*, *eBay, e America Online* hanno tutti subìto in un modo o nell'altro attacchi e minacce. Uno spyware denominato TSPY_MAMAW.A si collega a pagine Web relative a *Monster.com* al fine di sottrarre informazioni come ad esempio l'indirizzo di posta elettronica. Questa non era la prima volta in cui *Monster.*com veniva attaccato: a ottobre è stata infatti scoperta una pagina di phishing che riprendeva la sua schermata di login legittima, mentre a novembre il sito è stato colpito dagli hacker per installare *Neosploit*, un kit per exploit. TSPY_EBBOT.A, invece, opera come un attacco a forza bruta distribuito su *eBay:* accede a determinati URL per ripescare combinazioni di nomi e password utente che possono essere stati prelevati da siti Web di phishing.

Sottrazione di dati: sono le persone l'anello debole

Secondo il Ponemon Institute, il 78% delle fughe di dati viene realizzata dalle stesse figure interne autorizzate che lavorano presso una determinata azienda. La perdita di informazioni riservate e di proprietà intellettuali può portare a multe, cause legali, danni al marchio e cattiva stampa.

Le soluzioni convenzionali per la sicurezza non riescono ad affrontare in maniera adeguata questa crescente minaccia proveniente dall'interno. Proprio perché hanno accesso agli asset informativi, gli insider rappresentano una delle principali vie di fuga dei dati, siano esse violazioni intenzionali delle policy o perdite accidentali (ad esempio lo smarrimento di un dispositivo mobile contenente dati personali) Per tutelare i dati sensibili, le aziende hanno bisogno di una efficace soluzioni di data leak prevention (DLP) in grado di monitorare le potenziali falle esistenti presso il punto di utilizzo.

Ciò nonostante, la grande e repentina diffusione di sistemi di messaging, networking wireless e dispositivi storage USB ha reso alquanto difficile la protezione delle informazioni aziendali critiche. Di conseguenza le aziende stanno assistendo a un aumento dei volumi di dati smarriti o sottratti da parte di dipendenti o lavoratori a contratto che causano la fuoriuscita, accidentale o intenzionale, di informazioni.

Principali fonti di minaccia alle quali le aziende devono fare fronte:

Figure interne all'azienda	Dipendenti, persone a contratto che generalmente hanno accesso legittimo a dati sensibili, che causano la fuoriuscita di informazioni in maniera accidentale o intenzionale
Hacker esterni	Persone che violano le reti o i sistemi corporate, o che creano fisicamente le condizioni atte a sottrarre dati.
Figure esterne: ladri	Individui che rubano laptop, drive USB o che acquistano beni rubati contenenti dati sensibili per attività o profitti finanziari illeciti.
Malware	Software maligno che, dopo aver infettato il sistema, invia i dati sensibili all'esterno del perimetro di sicurezza aziendale.

Mai prima d'ora si era registrato un tale livello di minaccia nei confronti dei dati aziendali — tanto elevato quanto costoso. Secondo Attrition.org, società che monitora il settore, nel corso del 2007 (fino alla data del 21 dicembre) sono stati violati oltre 162 milioni di record come dati di carte di credito e numeri di polizze assicurative. Per contro l'anno precedente erano stati compromessi, sempre secondo Attrition.org, 49 milioni di record. Inoltre, l'Identity Theft Resource Center elenca oltre 79 milioni di record compromessi negli Stati Uniti alla data del 18 dicembre 2007. Questo rappresenta un aumento di ben quattro volte rispetto ai 20 milioni di record violati durante il 2006.

I principali episodi del 2007
Di seguito alcuni esempi di falle nei sistemi di sicurezza avvenuti e resi noti nel corso del 2007.

> **Boeing Breach**
> "Fonti di polizia hanno riferito [parlando di un dipendente della Boeing che ha sottratto informazioni] di aver trovato una chiavetta collegata al suo computer via cavo USB che correva lungo il retro del terminale fino al dispositivo storage 'nascosto in un cassetto' della sua scrivania". Da Information Week, 11 luglio 2007. Risulta chiaro che con il proliferare di dispositivi storage e sistemi mobili rimovibili diventa sempre più difficile prevenire e ostacolare situazioni di perdita di dati sensibili.
>
> **Il furto alla Fidelity NIS**
> "Per evitare il rilevamento, [l'amministratore che ha commesso il furto di dati] sembra aver scaricato le informazioni su un dispositivo storage anziché trasmetterli per via elettronica". Da CSO Magazine, 3 luglio 2007. Questo furto alla Certegy Check Services, una consociata di Fidelity National Information Services, illustra come i dipendenti stiano diventando sempre più bravi nel tentativo di sottrarre dati. In questo caso l'amministratore ha pensato che l'azienda fosse dotata di soluzioni per il filtraggio della rete e della posta elettronica, optando quindi per altri metodi volti a portare le informazioni all'esterno.
>
> **L'incidente del Governo del Regno Unito**
> CD del Ministero delle Finanze contenenti informazioni dettagliate e riservate di 25 milioni di cittadini britannici e di coloro che ricevono sussidi per l'infanzia. I record contengono nomi, indirizzi, numeri di polizze assicurative dell'intero database del Ministero delle Finanze, con dettagli relativi anche a oltre 7 milioni di famiglie, tutori e assistenti. Da Computerworld UK, 20 novembre 2007.

Uno studio condotto nell'anno da Cisco e dalla National Cyber Security Alliance rivela che gli utenti business in generale non prendono ancora in seria considerazione gli aspetti legati alla sicurezza nel momento in cui utilizzano dispositivi mobili. Puntando esclusivamente alla maggiore produttività, nomi del calibro di Marks & Spencer, NHS, Nationwide Building Society, Metropolitan Police, e lo US Department of Veterans Affairs sono stati vittime di alto profilo nell'ambito del furto di dati legato a episodi di laptop rubati o smarriti.

Anche le chiavette o drive USB si sono rivelate ottimi veicoli per introdurre esemplari di malware in una rete, per sottrarre velocemente ed efficacemente i dati in ambito

corporate, o per smarrirsi facilmente, compromettendo le informazioni di business riservate residenti proprio su questi supporti. Queste tendenze non mitigano il fatto che i malintenzionati stiano rivolgendo la loro attenzione ai dati aziendali, e l'aumento di attacchi rivolti alle informazioni business sottolinea come la cifratura dei dati sia l'elemento di tutela che meglio protegge le informazioni rendendone impossibile il riutilizzo una volta sottratte.

Prognosi per il 2008: può solo andar peggio
L'incapacità dei responsabili della sicurezza nell'affrontare le minacce interne, insieme con la mancanza di sensibilizzazione e conoscenza da parte dei dipendenti delle policy aziendali per proteggere i dati riservati, significa che il problema può solamente peggiorare.

Nel complesso, le minacce a impatto elevato di quest'anno sono state caratterizzate da un abuso di fiducia e da una preferenza verso obiettivi localizzati.

Riepilogo

1. Mentre i metadati diventano la nuova ossatura dell'information age, la nuova piaga è il furto di dati grezzi e non filtrati. I criminali impiegano combinazioni di social engineering, malware, informazioni carpite dall'interno e tecnologie modernissime per gettare una testa di ponte attraverso credenziali illecitamente sottratte e, quindi, mettere a frutto il più possibile l'accesso iniziale cercando di rimanere sotto il radar fintanto che non si raggiunga un obiettivo più grande. L'uso della crittografia per impedire l'accesso ai dati in transito è destinato a diffondersi in futuro.

2. I report di IDG affermano che la principale preoccupazione delle aziende nel 2007 è stata l'esposizione non intenzionale di informazioni riservate. Intenzionali o accidentali, alcune delle principali vie d'uscita di queste informazioni sono state l'utilizzo inappropriato della posta elettronica aziendale, il malware, il ricorso a servizi webmail pubblici, lo smarrimento di supporti di memorizzazione in transito, e il furto di dispositivi. Questa preoccupazione è ben fondata considerando le varie notizie recenti e il fatto che molte policy per la protezione dei dati utilizzate oggi non hanno preso in considerazione la discesa dei prezzi dei supporti storage, né il fatto che molti dispositivi spesso usati anche in ufficio come lettori MP3 o telefoni cellulari sono ora capaci di memorizzare grandi quantità di dati.

Minacce process-based

Le minacce process-based sono quelle che si presentano sotto forma di applicazione eseguibile lanciata sui computer infetti. Questi singoli esemplari di codice possono essere o non essere parte di un attacco a più componenti ma, in generale, eseguono sui sistemi colpiti una serie di attività nocive.

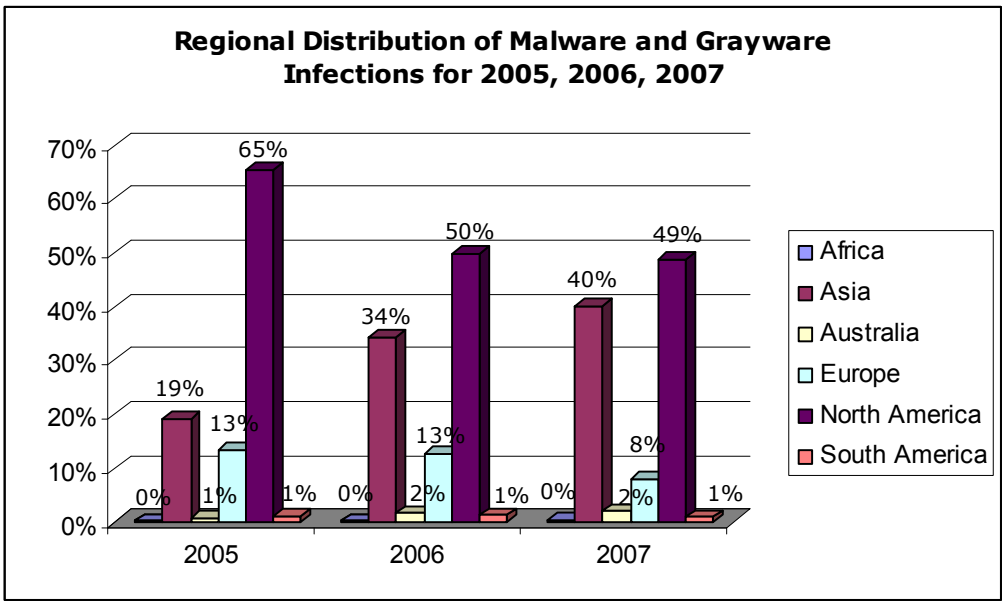
Statistiche sulle tipologie di malware

Posizione	10 malware più diffusi del 2007	
1	WORM_SPYBOT.IS	595,402
2	WORM_GAOBOT.DF	567,895
3	PE_LUDER.CH	539,788
4	TROJ_AGENT.ACSF	414,595
5	PE_PARITE.A	413,880
6	HTML_IFRAME.KQ	287,724
7	WORM_NETSKY.P	283,340
8	EXPL_ANICMOO.GEN	280,532
9	EXPL_WMF.GEN	248,826
10	WORM_NYXEM.E	245,449

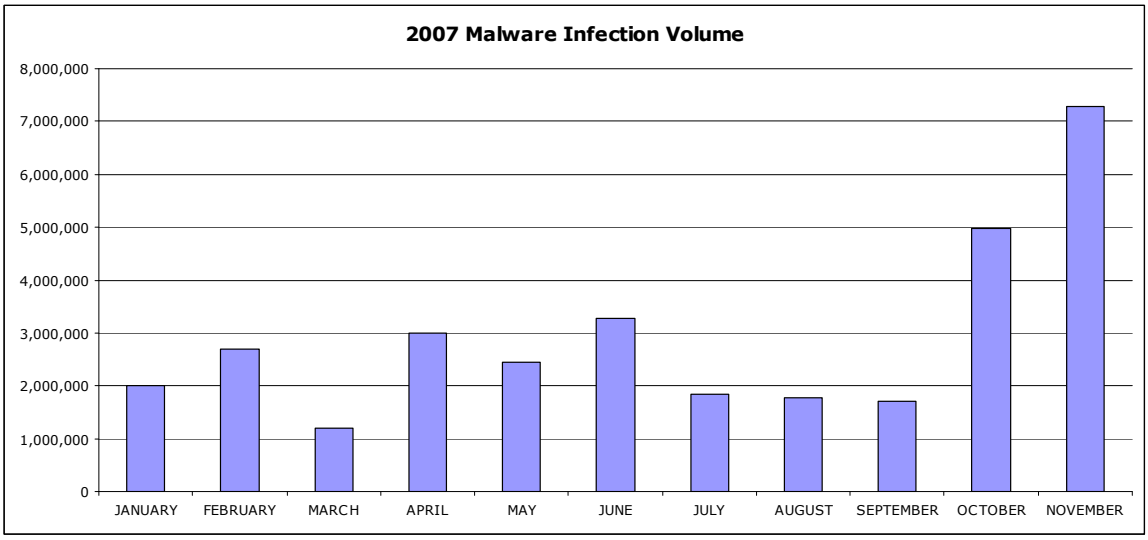
I dati che seguono si riferiscono alle tendenze del malware registrate nel 2007. Come si può vedere nella classifica dei primi 10 esemplari più diffusi del 2007, le due posizioni di vertice sono occupate da due worm nonostante siano rimasti fuori classifica per tutto l'anno. La maggior parte di queste minacce circola da tempo, in alcuni casi fin dal 2004. Poiché i bot sono tipicamente impiegati per diffondere spam, è possibile che nei prossimi mesi si possa assistere a una mobilitazione delle botnet per campagne di spamming intensive. Visto che questi rilevamenti sono relativamente datati, potrebbero approfittare di computer di nuovo acquisto che vengono collegati in rete senza che siano preventivamente applicate le patch appropriate. La stessa ragione serve probabilmente a spiegare il ritorno di EXPL_WMF.GEN, un exploit di fine anno (2005). Ciò dimostra la persistenza delle varie vulnerabilità e l'importanza di controllare regolarmente la disponibilità di aggiornamenti software.

PE_LUDER.CH si diffonde per mezzo di drive fisici e removibili ed è particolarmente diffuso nella regione APAC (Asia-Pacifico), dove le segnalazioni parlano di intere scuole infettate tramite USB. La relativa facilità con cui le chiavette USB vengono passate da una persona all'altra (e da un computer all'altro) le rende vettori di infezioni ideali per gli autori di malware che probabilmente intendono assicurarsi la vicinanza fisica ai sistemi da loro infettati.

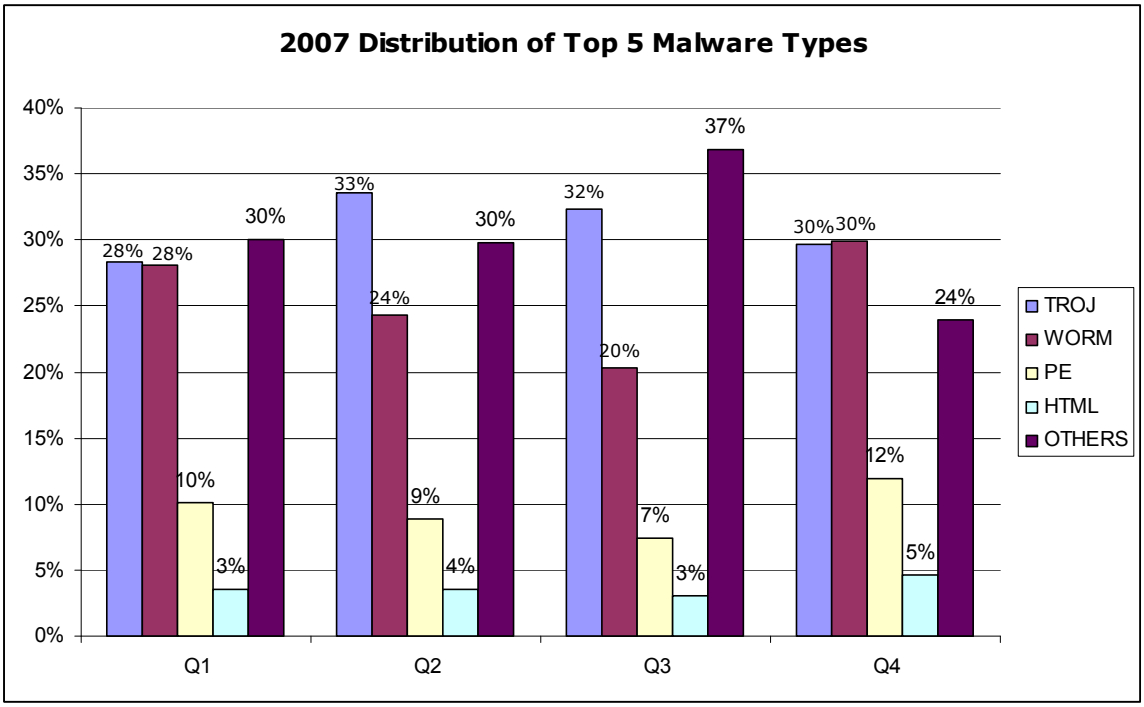
Per quanto concerne la distribuzione regionale di malware e grayware, le tendenze annuali indicano che l'Asia sta acquisendo una fetta sempre più grande della torta infettiva finora appannaggio del Nordamerica. Metà delle infezioni globali si riferisce tuttora al Nordamerica, mentre Australia e Sudamerica rimangono quasi invariate in termini di volume e l'Europa vede diminuire del 5% il numero di infezioni rispetto alle altre regioni. Ciò potrebbe essere causato dalla prevalenza di diversi esemplari di malware specifici per la regione asiatica come programmi per la sottrazione di informazioni relative a giochi online, worm e persistenza dell'exploit .ANI (EXPL_ANICMOO.GEN) per buona parte del 2007.



Una tendenza verificata nel corso dell'anno è stato il picco improvviso dei volumi di infezioni dal mese di settembre, più che triplicato in ottobre e ancora aumentato nelle prime tre settimane di novembre. A questo fenomeno hanno contribuito i già citati worm presenti nella Top 20, e ciò potrebbe significare che gli autori di malware intendessero sfruttare il periodo natalizio come opportunità per diffondere spam o spyware approfittando di coloro che fanno i loro acquisti online.



Come si può vedere oltre, le tipologie di malware più diffuse dell'anno sono state worm e Trojan, anche se il numero di utenti infettati da quest'ultimo tipo supera quello di qualunque altro malware. I singoli esemplari di malware fanno sempre più spesso parte della routine di un altro malware sotto forma di dropper o componenti oggetto di drop, downloader o componenti scaricati da downloader, redirector per inviare gli utenti a siti contenenti malware, o residenti su siti remoti accessibili da altro malware.



Distribuzione delle tipologie di malware nel 2007 con le principali percentuali di infezioni

Nonostante la natura multicomponente degli attacchi verificatisi negli ultimi due anni, esistono ancora tentativi identificabili di diffondere singoli programmi capaci di creare danni da soli. Tra i più importanti si trova PE_EXPIRO.A, che sottrae informazioni sulle carte di credito mostrando un finto messaggio di errore per convincere gli utenti a digitare i dati delle loro carte. TROJ_KILLAV.GG modifica alcune funzioni di Windows finendo col rendere inutilizzabili i sistemi colpiti. TSPY_MSTEAL.A visualizza una schermata di login fasulla con lo stesso aspetto della pagina di login di *MSN Messenger*, mentre TSPY_SPEYK.A cerca di fare lo stesso con Skype, diffusissima applicazione per instant messaging e VoIP (Voice-over-Internet Protocol). TROJ_CAPTCHAR.A, invece, si presenta sotto forma di gioco spingendo l'utente a digitare correttamente il codice CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) visualizzato spogliando progressivamente una modella a video.

L'utilizzo di codec fasulli, come rilevato lo scorso anno, ha continuato a infastidire gli utenti anche nel 2006. La famiglia TROJ_ZLOB usa costantemente questa strategia facendo credere agli utenti che sia necessario installare un determinato codec per poter visualizzare filmati online. Nel 2007 il malware ZLOB ha iniziato a rivolgersi anche agli utenti Apple, a conferma del fatto che persino i sistemi operativi alternativi non sono più un riparo sicuro per gli utenti online.

Minacce Web

Un altro modo di analizzare le minacce Web è sotto forma di software appartenente a singole entità specializzate in malware e adware. Da una parte vi sono regolari aziende

come Integrated Search Technologies e Zango; dall'altra si trovano entità più oscure vagamente confederate sotto denominazioni come CoolWebSearch e Russian Business Network (RBN).

	Famiglia di minacce Web	% PC infetti	% di tutte le infezioni	% di tutte le varianti	# varianti identificate
1	Fun Web Products	33.0%	9.7%	0.2%	35
2	A Better Internet	22.0%	6.5%	0.2%	33
3	Zango	9.2%	2.7%	2.4%	356
4	BYTEVER family of scripts	7.6%	2.2%	0.3%	47
5	Hotbar	6.8%	2.0%	0.6%	92
6	Winfixer	6.1%	1.8%	0.4%	52
7	Drivercleaner	6.0%	1.8%	0.1%	8
8	WhenU	5.4%	1.6%	0.3%	45
9	DLOAD Trojans	5.2%	1.5%	4.8%	726
10	New.net	4.9%	1.4%	0.1%	17
11	Zlob	4.8%	1.4%	0.4%	68
12	IBIS	4.6%	1.3%	0.3%	39
13	Purity Scan	4.1%	1.2%	0.7%	105
14	Softomate	3.8%	1.1%	0.4%	56
15	VIRTUMUNDO	3.5%	1.0%	0.9%	141
16	CDT	3.3%	1.0%	0.4%	65
17	Claria/Gain	2.8%	0.8%	0.4%	61
18	IST	2.7%	0.8%	0.8%	119
19	Comet Systems	2.0%	0.6%	0.3%	41
20	Starware	1.9%	0.6%	0.01%	2

Le famiglie di minacce Web sono gruppi di singole minacce e relative varianti usati dalla medesima entità. Dato che su un singolo PC possono esservi più esemplari di software, il dato più pertinente è la percentuale di PC infetti e non il conteggio dei vari elementi di software come programmi di infezione o loro varianti.

Ciò che emerge da questa tabella è un'altra visione dell'economia delle minacce Web. *Fun Web Products* è una famiglia conosciuta per i suoi banner *"Smiley Central"* che installano toolbar come *MyWay* e *MySearch*. *A Better Internet* (nota anche come *Direct Revenue*) vanta una tradizione di installazioni illecite del proprio adware mediante exploit, worm e varie forme di social engineering.

Il falso anti-spyware

Con la diffusione delle applicazioni anti-spyware emerse negli ultimi cinque anni si è affermato anche un particolare gruppo di minacce denominato “falso anti-spyware”. Il suo modo di agire inizia visualizzando sul browser dell'utente un avviso circa la verificata infezione del sistema da parte di malware; l'utente è quindi spinto ad acquistare una certa applicazione allo scopo di eliminare un'infezione che in realtà non esiste.

Le applicazioni di falso anti-spyware hanno provato di essere minacce longeve. Confrontando le prime dieci applicazioni di questo genere all'inizio e alla fine di un semestre si evince come 8 esemplari su 10 siano rimasti nella Top Ten lungo tutto il periodo (cfr. tabella sottostante).

Falso anti-spyware		
3' trim. 2006		
Pos.	Nome minaccia	%PC
1	Zlob Trojan	8.2%
2	Winfixer	3.2%
3	Adclicker	1.8%
4	Spywarestormer	1.3%
5	SpywareQuake	1.3%
6	Renos Trojan	1.2%
7	ErrorGuard	1.0%
8	ErrorSafe	0.8%
9	SpySheriff	0.5%
10	[illegible]	0.5%

Falso anti-spyware		
1' trim. 2007		
Pos.	Nome minaccia	%PC
1	Zlob Trojan	8.6%
2	Drivercleaner	5.7%
3	Winfixer	5.6%
4	Renos Trojan	1.7%
5	Spywarestormer	1.2%
6	Adclicker	0.9%
7	ErrorGuard	0.6%
8	ErrorSafe	0.5%
9	SpySheriff	0.5%
10	SystemDoctor	0.4%

I principali falsi anti-spyware misurati come percentuale dei computer infetti. Otto minacce su dieci sono rimaste in classifica per sei mesi.

Proprio di recente, i lettori del sito del *Boston Herald* si sono visti comparire un allarme JavaScript che, in realtà, era parte di un falso anti-spyware. Vi sono state anche numerose pubblicità in Shockwave che puntavano a script per il reindirizzamento a siti contenenti falso anti-spyware.

Riepilogo

1. In generale vi sono oggi più persone online che mai. Negli ultimi cinque anni molte zone dell'Asia hanno iniziato a competere con Nordamerica ed Europa in termini di presenza online. Apparentemente questo volume elevato comporta un pubblico più vasto presso il quale, considerando i diversi gradi di sensibilizzazione alla sicurezza online, il malware è in grado di proliferare.

2. Come già detto, il volume delle minacce rilevate negli ultimi due anni ha già superato la soglia del 1500%. Non molte di queste minacce sono nuove, bensì sono semplici versioni rinnovate di minacce preesistenti. I casi più diffusi si riferiscono a malware finalizzato alla creazione di botnet e combinazioni di exploit per raggiungere il medesimo scopo.

3. Una grande percentuale di minacce si occupa di tener traccia delle preferenze dell'utente per scatenare strategie marketing aggressive mediante adware. Il rovescio della medaglia è composto da pretesi prodotti per la sicurezza che si travestono da "soluzioni" quando invece sono solo tattiche per sottrarre direttamente i dati dell'utente e sfruttarli in maniera truffaldina.

Minacce basate sui contenuti

Le minacce basate sui contenuti vengono inviate alla vittima come parte di un contenuto, come ad esempio phishing o spam.

Motivati dai potenziali guadagni, gli spammer sono disposti a investire risorse considerevoli nell'ottimizzazione dello spam. Questo finisce col creare un rapporto di continuo contrasto tra spammer e produttori anti-spam. Se gli spammer creano nuove tecniche di spamming, i produttori anti-spam creano tecnologie adatte a bloccarle; entrambi gli schieramenti mettono a punto risposte sempre più sofisticate man mano che il processo evolve.

Lo spam ha continuato la propria evoluzione nel corso del 2007 modificandosi nei messaggi, nei metodi di diffusione e nei sistemi backend; inoltre ha continuato a fondersi con altre tipologie di minacce e protocolli. Tutti questi cambiamenti hanno favorito l'incremento dello spam, che ora costituisce almeno il 90% del traffico e-mail complessivo. Il report che segue fornisce una panoramica sulle tendenze dello spam verificate nel 2007 offrendo alcune previsioni per il 2008.

1. Lo spam nel 2007

Gli spammer devono riuscire a confezionare un messaggio sufficientemente persuasivo per chi lo riceve e, nel contempo, un contenuto che sia in grado di aggirare i filtri anti-spam. Si tratta di un processo senza fine: gli spammer devono continuare a sviluppare nuove tecniche perché i filtri si adattano agli attacchi del momento bloccandoli. Questa sezione mette in evidenza come lo spam sia cambiato nel corso del 2007.

1.1 Spam basato su immagini

Questo genere di spam mostra il messaggio in un'immagine inserita nel corpo dell'e-mail. Non è certo una tecnica nuova; tuttavia, verso la fine del 2006 gli spammer hanno iniziato a spedire volumi crescenti di immagini essendosi accorti della maggior difficoltà con cui i filtri riescono a bloccare questo tipo di spam. Lo spam basato su immagini è aumentato nella prima parte del 2007 toccando il 40% di tutto lo spam inviato. Nel corso di questo periodo i filtri si sono adattati diventando più efficienti nel bloccare questo genere di messaggi. Di conseguenza lo spam basato su immagini ha iniziato a diminuire a metà 2007: nel mese di giugno rappresentava ormai meno del 6% dello spam complessivo, riducendosi a meno del 2% a fine anno.

1.2 Spam basato su allegati

Mentre lo spam basato su immagini andava perdendo di efficacia, gli spammer si sono rivolti agli allegati nel tentativo di nascondere i messaggi durante l'analisi dei filtri. Nel giugno 2007 è comparso uno spam sperimentale con allegato PDF, e per la fine di quel mese lo spam PDF aveva ormai inondato Internet. Il picco si è verificato a metà agosto, totalizzando il 18% di tutto lo spam. Tuttavia anche in questo caso il fenomeno si è rapidamente diradato in seguito all'adattamento dei filtri, scendendo fino quasi allo 0% a fine agosto. Gli spammer hanno trascorso la restante parte dell'anno usando diverse tipologie di allegati – FDF, ZIP, XLS, RTF, DOC e persino file MP3 che riproducevano il messaggio spam in audio anziché mediante testo o immagini.

Figura 1: Spam PDF nella seconda metà del 2007

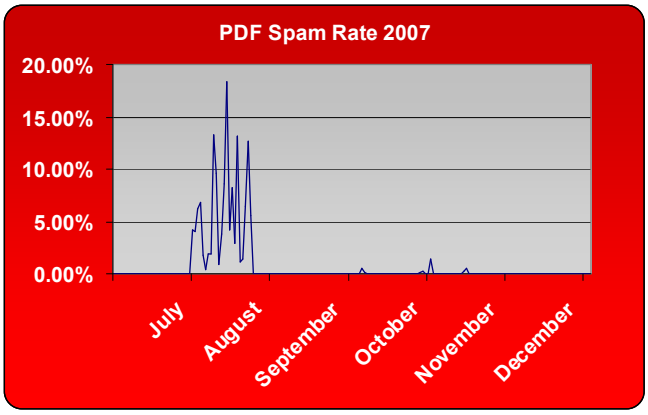
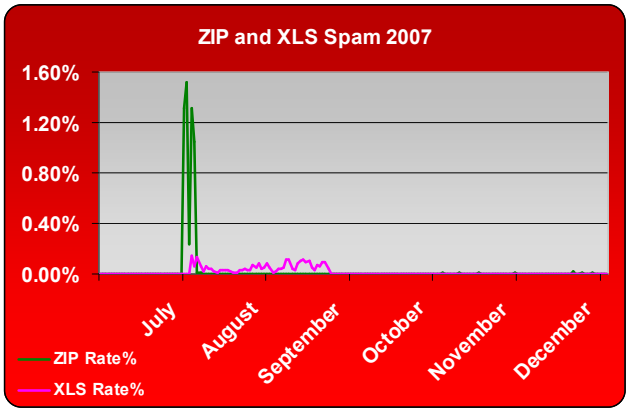


Figura 2: Altri allegati spam, seconda metà del 2007



Come si vede nella Figura 1, lo spam basato su allegati è stato diffuso soprattutto in luglio e agosto, diminuendo quindi nella parte successiva dell'anno. Sebbene spediti in volumi minori rispetto agli spam PDF, gli allegati ZIP e XLS hanno comunque totalizzato numeri significativi. Molti attacchi sembrano essere stati degli esperimenti per inviare specifiche tipologie di allegato in intervalli di tempo brevissimi. Probabilmente gli spammer cercavano di capire quali potessero essere i metodi più efficaci. Lo spam ZIP mostrato in Figura 2 potrebbe corrispondere a questo genere di tentativo.

1.3 Spam con link interni

Lo spam deve contenere qualcosa che spinga chi lo riceve a compiere una certa azione: spesso si tratta di un link interno che inoltra l'utente a un sito Web. I filtri anti-spam possono assegnare un punteggio di reputazione agli URL di questi collegamenti in modo da identificare e bloccare lo spam. Per questo gli spammer hanno cercato di nascondere o evitare l'uso di URL. Ad esempio, un attacco del gennaio 2007 usava degli asterischi nell'URL per evitare il rilevamento. Il messaggio recitava: *"http://www.printeryml*.com (Important! Remove '*' to make the link working)"*. Non certo un approccio particolarmente sofisticato, ma che può aver avuto qualche successo fino a quando i filtri non si sono adattati anche a questa tecnica.

Gli spammer inseriscono inoltre gli URL in messaggi di testo molto semplici. Limitando il contenuto dello spam diventa più difficile identificare come tale un messaggio e

assegnare una reputazione all'URL interno. Gli spammer
non usano testo per comunicare i loro messaggi, ma sperano che i destinatari seguano il link verso un sito Web. Per tutto il 2007 i messaggi contenenti link che scaricano malware sono costantemente aumentati.

Nel 2007 gli spammer hanno insistito tantissimo sulle frodi azionarie con messaggi che non contenevano alcun URL ma che si limitavano a promuovere l'acquisto di azioni di poco valore. Lo spammer acquista queste azioni quando non valgono nulla e quindi le promuove attivamente mediante spam. Molti destinatari acquistano le azioni "consigliate" facendone salire il valore, così che lo spammer possa guadagnarci. Le truffe di questo tipo sono collegate a numerose tipologie di spam come immagini, allegati e persino file MP3. Tuttavia gli spammer inviavano spesso i loro messaggi come semplice testo usando una varietà di trucchi di punteggiatura per camuffare il simbolo di borsa delle azioni e altri contenuti.

Gli spammer continuano a usare una serie di trucchi nel tentativo di sfruttare la buona reputazione di domini legittimi. Un esempio è quello di un URL che utilizzava il pulsante "Mi sento fortunato". Anziché ricevere un elenco di risultati da una ricerca, il browser apre la pagina Web del primo risultato trovato dal motore. Nell'ambito di questo processo Google crea un URL "Mi sento fortunato" che indirizza gli utenti a queste pagine. La formazione dell'URL avviene dietro le quinte in modo invisibile all'utente. Tuttavia alcuni spammer hanno scoperto come costruire gli URL "Mi sento fortunato" utilizzandoli per dirigere gli utenti a siti di spam o a pagine Web pericolose. Questi URL erano inseriti nei messaggi spam. Tecnicamente l'URL mandava l'utente alla pagina Web di destinazione passando attraverso Google: un trucco che ha permesso di scavalcare i servizi di reputazione Web, dato che Google non è un sito di spam.

Gli spammer passano inoltre da un dominio all'altro con più velocità rendendo più difficile per i filtri riuscire ad acquisire e applicare le reputazioni in maniera tempestiva. Nel biennio 2003-2004 gli spammer mantenevano un sito per qualche giorno, fino anche a una settimana. Questo intervallo ha continuato a diminuire e oggi alcuni siti sono attivi per meno di un giorno, talvolta anche per solo un paio d'ore.

1.4 Spam internazionale

In qualità di azienda internazionale con una rete globale di centri di ricerca, Trend Micro ha tracciato nel 2007 lo spam diffuso in 38 lingue. La maggioranza dei messaggi era ancora in lingua inglese (una media del 73%), ma le altre lingue sono cresciute e si sono diversificate in maniera notevole. Dopo l'inglese le altre due lingue principali sono il giapponese e il cinese, ciascuna con un 10% circa di spam e una distribuzione relativamente omogenea lungo tutto l'anno salvo una piccola flessione nell'ultima parte. Insieme, lo spam giapponese e quello cinese compongono circa un quinto dello spam mondiale. Le aziende, specialmente quelle multinazionali, devono possedere filtri capaci di bloccare lo spam scritto con caratteri a doppio byte e in grado di identificare nello specifico lo spam giapponese e cinese. La Figura 3 mostra le percentuali di spam per le prime tre lingue nel corso del 2007.

Tutte le altre lingue hanno contato ciascuna per meno dell'1% dello spam mondiale del 2007, totalizzando nel complesso quasi l'8%. Sebbene possa sembrare poca cosa, l'enorme volume di spam rende persino percentuali così piccole una quantità significativa. La Figura 4 mostra le percentuali delle quattro lingue successive: spagnolo, tedesco, portoghese e russo. Ciascuna ha contribuito in media a più dello 0,35% dello

spam. Vi è stato un forte incremento nello spam in tedesco durante maggio, e di nuovo un aumento significativo del tedesco e del portoghese verso fine anno; il russo è invece diminuito costantemente per tutto l'anno.

Figura 3: Le prime tre lingue dello spam

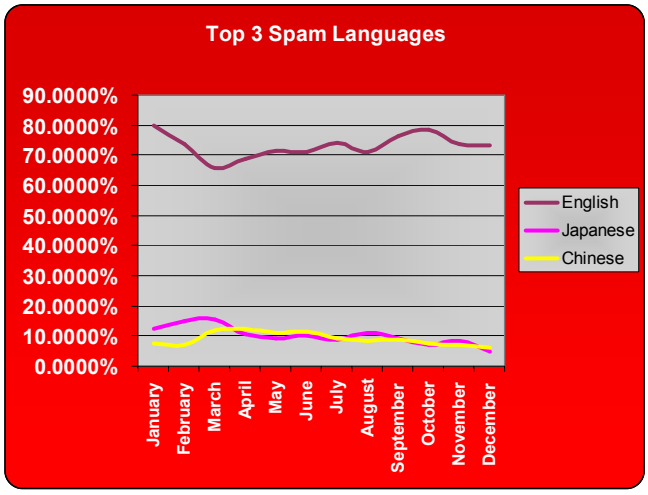
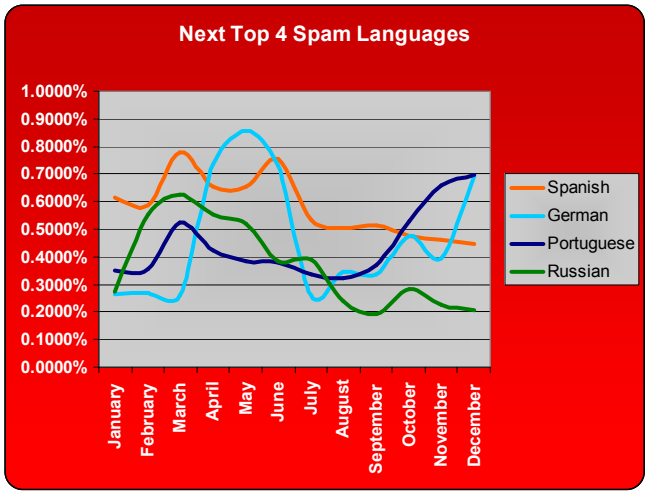
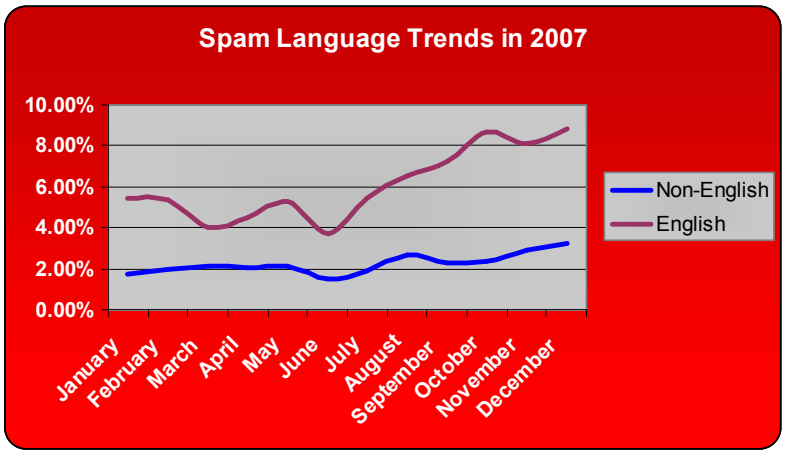


Figura 4: Le quattro lingue successive (4-7)



Con lo spam che andava aumentando nel corso del 2007, la maggior parte dei messaggi era in inglese. Vi è stato tuttavia un costante incremento di spam in altre lingue (cfr. Figura 5). In alcuni casi, come catalano, ceco, indonesiano, lettone, lituano, norvegese, slovacco e sloveno, vi sono stati forti picchi in una o due occasioni. Questo potrebbe segnalare un esperimento da parte degli spammer per capire quali lingue possano dare migliori risultati.

Figura 5: Le tendenze dello spam in inglese e altre lingue durante il 2007



Tablella1: Attacchi spam del 2007 notevoli per volume o approccio

Month	Description of Attack
Jan	Star in URLs to avoid identification
Feb	Pump and Dump Spam - plain text (moving away from image spam)
Mar	Pump and Dump Spam - plain text attacks continuing
Apr	Nuwar Worm - image spam with malware DHA Spam - only small text string in body
Jun	German Pump and Dump German PDF Spam – experiments
Jul	Flood of PDF Spam on Internet Pump and Dump – plain text Excel (XLS) Spam
Aug	Pump and Dump - text crossed out to confound filters FDF Spam - a variant of PDF spam Greeting Card Spam - links to a Web site with malware RTF Spam Invisible Ink Spam Skype Spam
Sep	Word Doc Spam Pump and Dump - punctuation tricks to obscure content You Tube Spam I Feel Lucky Spam - abuses Google “I feel lucky” search
Oct	MP3 Spam PDF Spam with Malware US Election Spam
Nov	Money Mule Spam
Dec	HTML Insert Spam - salad words hidden in style and other tags Chinese Excel Spam DHA Spam - content consists of word salad

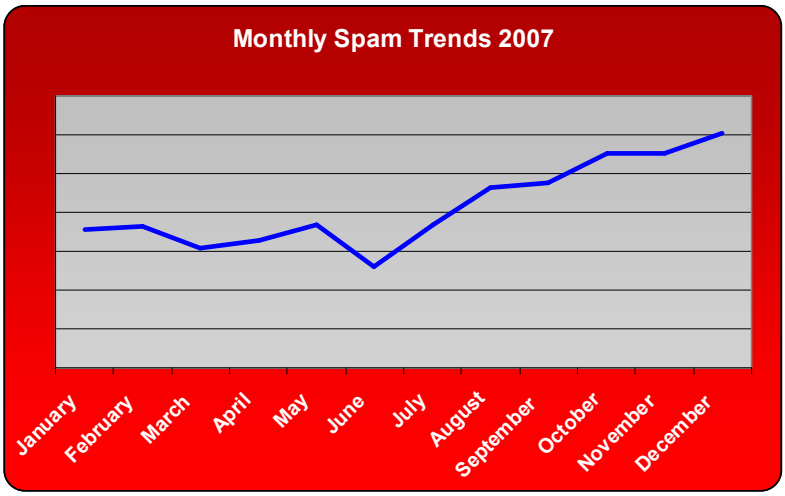
1.5 Crescita dello spam

Lo spam non è cresciuto solamente in volume ma anche in dimensioni. La prevalenza di nuove tecniche, come lo spam basato su immagini e su allegati, ha ampliato la dimensione media dei messaggi. E con lo spam responsabile di oltre il 90% del traffico e-mail globale, i volumi complessivi e le loro dimensioni intasano le infrastrutture di messaging con un significativo impatto negativo sulle reti.

L'aumento delle dimensioni e delle quantità di spam ha fatto crescere i requisiti di amministrazione, bandwidth e storage incrementando il lavoro di gestione e i costi. Per le aziende non è più sufficiente bloccare lo spam fuori dalle inbox; occorre bloccarne la maggior parte prima ancora che entri nella rete in modo da salvaguardare risorse costose. Ciò rende i servizi di reputazione un componente critico delle soluzioni anti-

spam, poiché in base alla reputazione del mittente possono bloccare i messaggi prima che giungano al gateway.

Figura 6: Le tendenze mensili dello spam nel 2007



2. La diffusione dello spam nel 2007

La maggior parte dei principali filtri anti-spam è stata in grado di mantenere l'efficacia nei valori più alti sopra il 90%. Per ottenere i risultati desiderati, gli spammer hanno dovuto spedire volumi considerevoli di messaggi così da scavalcare questi filtri: per questo sono stati necessari forti investimenti nella creazione e nel mantenimento di meccanismi di diffusione capaci di massimizzare la quantità di spam inviata.

Gli spammer hanno anche bisogno di metodi che nascondano l'identità del mittente. Per quanto lo spam non sia necessariamente un'attività illegale, esso è tuttavia spesso abbinato a frodi e altre attività illecite. Nascondere l'identità del mittente aiuta anche a confondere i servizi di reputazione che bloccano lo spam in base alla reputazione di chi spedisce mail.

Nel 2007 gli spammer si sono avvalsi di un approccio che aumenta sia le risorse dedicate alla diffusione dello spam, sia la capacità di nascondersi: le reti botnet. Un codice bot è un malware che, una volta scaricato, permette a un hacker di assumere il controllo di un computer per i propri scopi all'insaputa del proprietario della macchina. Questi computer sono chiamati zombie o bot e, quando usati insieme, formano una rete detta botnet. Il codice bot viene scaricato mediante gli stessi metodi di altro malware, soprattutto tramite il Web e gli allegati e-mail. Nel 2007 sono apparse molte varianti di codice bot, compreso Nuwar (noto anche come Storm) e Stration.

Le reti botnet possono essere usate per numerosi scopi, ma uno dei principali è l'invio di spam e di altre minacce e-mail. Le reti botnet sono diventate diffusissime in tutto il 2007 e sono ora responsabili dell'invio di oltre il 90% dello spam. Le botnet sono usate anche per ospitare i siti Web a cui sono collegati i messaggi spam.

La più grande botnet del 2007 è stata la Storm Worm
Botnet, avviata a inizio anno per continuare quindi a crescere collegando milioni di computer. Questa rete gigante è stata suddivisa in segmenti, o reti più piccole. Alcune varianti di Storm Worm usavano una chiave da 40 byte per cifrare il traffico sul protocollo peer-to-peer (P2P). La tecnica crittografica permetteva dunque la comunicazione solo tra nodi botnet dotati della medesima chiave. Questi nodi separati con chiavi di accesso differenti hanno permesso agli autori di Storm di rivendere i nodi botnet ad altri utenti (come spammer o attaccanti DDoS). Un'ulteriore analisi di Storm e di altre botnet è presente in un capitolo successivo del presente report, dal titolo “Botnet”.

Gli spammer ricorrono alle botnet per mascherare la fonte dello spam. Le botnet spediscono normalmente lo spam in brevi raffiche avvalendosi di server DNS dinamici gratuiti per cambiare rapidamente macchine. Gli spammer hanno iniziato inoltre a sparpagliare l'invio di spam dai singoli bot. Volumi di e-mail insolitamente elevati aiutano a identificare le fonti di spam; quindi, cambiare i server e minimizzare la quantità di spam spedita dai singoli bot aiuta a nasconderne l'origine. Questi approcci tentano di confondere i servizi di reputazione che bloccano i mittenti noti di spam e di altre minacce e-mail.

Le reti botnet offrono agli spammer numerosi vantaggi: aiutano a nascondere la fonte dello spam, permettono di spedire volumi più alti e utilizzano le risorse delle macchine infette minimizzando i rischi e i costi e massimizzando gli utili.

3. Modifiche al sistemi backend dello spam nel 2007

In origine gli spammer puntavano a semplificare le operazioni di invio usando un unico centro di comando e controllo per gestire le spedizioni di massa; non si preoccupavano di eventuali invii non andati a buon fine dato che l'enorme volume di spam rilasciato bastava a garantire una percentuale sufficiente di successi. Questi metodi di invio semplificati sono tuttavia usati dai filtri come indicatori di spam, costringendo gli spammer a potenziare i loro sistemi per evitare di essere rilevati e per aumentare i tassi dei messaggi giunti a destinazione. Queste modifiche ai sistemi backend risultano pressoché invisibili agli occhi di chi riceve i messaggi, ma aiutano gli spammer a contrastare particolari tecnologie di filtraggio.

3.1 Decentralizzazione delle reti botnet

In origine le reti botnet usavano un unico centro di comando e controllo che, una volta scoperto, poteva portare alla neutralizzazione di una botnet. Tuttavia le botnet come Storm Worm Botnet si sono evolute per usare protocolli peer-to-peer eliminando la centralizzazione del controllo e rendendo più difficile lo smantellamento delle botnet.

3.2 Uso di funzioni MTA

In passato i sistemi spam non rispedivano i messaggi che ritornavano una notifica di errore nella consegna. Alcune soluzioni anti-spam sfruttano questa caratteristica applicando una tecnica di graylisting: ogni volta che viene aperta una connessione con il mail server, il sistema registra indirizzo IP, indirizzo e-mail del mittente e indirizzo e-mail del destinatario. La prima volta che il sistema riceve una combinazione di questi tre identificatori genera un errore temporaneo richiedendo al server di riprovare. La posta spedita da mail server legittimi viene molto probabilmente inviata una seconda volta; quella diffusa da sistemi spam invece no. Se un messaggio con la stessa combinazione di identificatori viene ricevuto una seconda volta, esso viene smistato regolarmente.

Per aggirare il graylisting e le tecniche ad esso associate, i sistemi spam stanno iniziando a comportarsi come Mail Transfer Agent (MTA) legittimi; alcuni rispediscono i messaggi spam temporaneamente rifiutati, riducendo l'efficacia del graylisting. I filtri anti-spam devono quindi applicare altre tecniche per identificare i messaggi sospetti.

4. Minacce multiprotocollo e a tecnica mista

4.1 Minacce a tecnica mista

In origine lo spam veniva usato per promuovere prodotti e servizi legittimi. Oggi però i cybercriminali sfruttano lo spamming per ottenere guadagni illeciti: lo spam è usato per inviare messaggi fraudolenti come phishing, truffe azionarie ecc. Inoltre lo spam contiene spesso malware come codice bot, programmi che sottraggono informazioni e altro software che aiuta ad alimentare il ciclo dello spam.

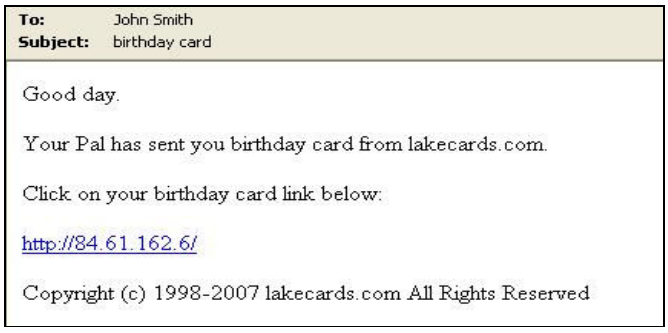
4.2 Da un protocollo all'altro

Oltre a usare minacce a tecnica mista, lo spam sta anche allargando i protocolli utilizzati. Si registra un incremento dello spam su dispositivi mobili e su instant messaging; nel 2007 si sono viste anche nuove forme di comunicazione su Skype e YouTube. Lo spam è spesso il primo passo di una minaccia Web: i link interni possono condurre il destinatario su siti illegali dediti al phishing o contenenti download pericolosi.

4.3 Un esempio di attacco a tecnica mista

Gli attacchi di spam condotti nel 2007 mediante biglietti di auguri elettronici rappresentano un eccellente esempio di attacco a tecnica mista che sfrutta molti degli elementi presentati in questo report. Le e-mail erano molto semplici, contenendo pochissimo testo e un URL (come indirizzo IP numerico e non sotto forma di dominio). Il testo poteva variare, ma il senso era quello di comunicare al destinatario che un amico gli aveva spedito un biglietto di auguri elettronico visibile selezionando il link in calce al messaggio. La Figura 7 mostra un esempio:

Figura 7: Esempio di spam con biglietto d'auguri elettronico



Questo tipo di spam utilizzava reti botnet per inviare i messaggi e infettava con malware i computer del destinatario che avesse seguito il link proposto, perpetuando così il ciclo della botnet. Le botnet non solo spedivano spam, ma venivano anche usate per ospitare

i siti Web cui erano collegate le e-mail: in questo modo veniva sferrato un attacco su più protocolli.

Molte macchine infette erano usate per l'hosting dei siti Web, ciascuno con il proprio indirizzo IP. Un template serviva a far ruotare tutti gli indirizzi IP disponibili inserendo link differenti nel messaggio spam e variando altri elementi del testo. Usare l'indirizzo IP anziché il nome di dominio aiutava a mascherare la destinazione del link, che era un server infetto altrimenti impiegato per motivi legittimi.

Lo spam dei biglietti di auguri elettronici fondeva gli attacchi utilizzando tecniche di spamming per far scaricare il malware, e passava da un protocollo all'altro portando gli utenti su siti Web pericolosi. Questi attacchi facevano inoltre uso di botnet sia per spedire messaggi che per ospitare i siti Web, e usavano trucchi sugli URL e template sul sistema backend per variare i contenuti dei messaggi stessi.

Proteggere dalle minacce a tecnica mista e multiprotocollo richiede una definizione più completa della sicurezza del messaging e una difesa integrata.

5. Previsioni per il 2008

La posta elettronica continuerà anche nel 2008 a essere il principale mezzo di comunicazione e continuerà a essere oggetto di abusi da parte di spammer e cybercriminali. Tuttavia crescerà anche la dipendenza da altre tipologie di comunicazione elettronica, rendendo questi vettori più allettanti per lo spam e altre minacce. Lo spam aumenterà su telefoni cellulari, IM, Skype, YouTube e altri siti di social networking.

L'inglese continuerà a essere la principale lingua dello spam, ma le altre lingue continueranno ad aumentare e a diversificarsi richiedendo un approccio globale al filtraggio dello spam.

Gli spammer continueranno a ottimizzare i loro sistemi di diffusione. Le reti botnet diventeranno sempre più capillari e la vendita di nodi botnet sarà più razionalizzata, forse diventando un componente di kit automatizzati per lo spam. Questo scenario potrebbe portare a un forte incremento delle infezioni botnet. Gli spammer continueranno a potenziare i loro sistemi backend rendendoli di difficile differenziazione rispetto ai mail server legittimi.

Le minacce diffuse via Web cresceranno e diverranno ancora più diffuse. Le minacce diffuse via Web sono quelle che sfruttano il Web per agevolare il cybercrimine. La posta elettronica è spesso una componente di queste minacce, poiché diffonde messaggi contenenti link a siti Web pericolosi o allegati con malware che a sua volta accede al Web. Nel 2008 lo spam sarà usato soprattutto per dirigere gli utenti verso siti Web che contengono i messaggi, che compiono frodi o che attivano download pericolosi. Di conseguenza gli spammer dovranno inventare nuovi trucchi per nascondere gli URL. Inoltre, Web server legittimi saranno presi in ostaggio e i domini fatti ruotare ancor più rapidamente per evitare di abbassarne la reputazione. Sarà dunque sempre più importante implementare la sicurezza a livello sia di posta elettronica che di Web in modo da proteggersi in maniera completa.

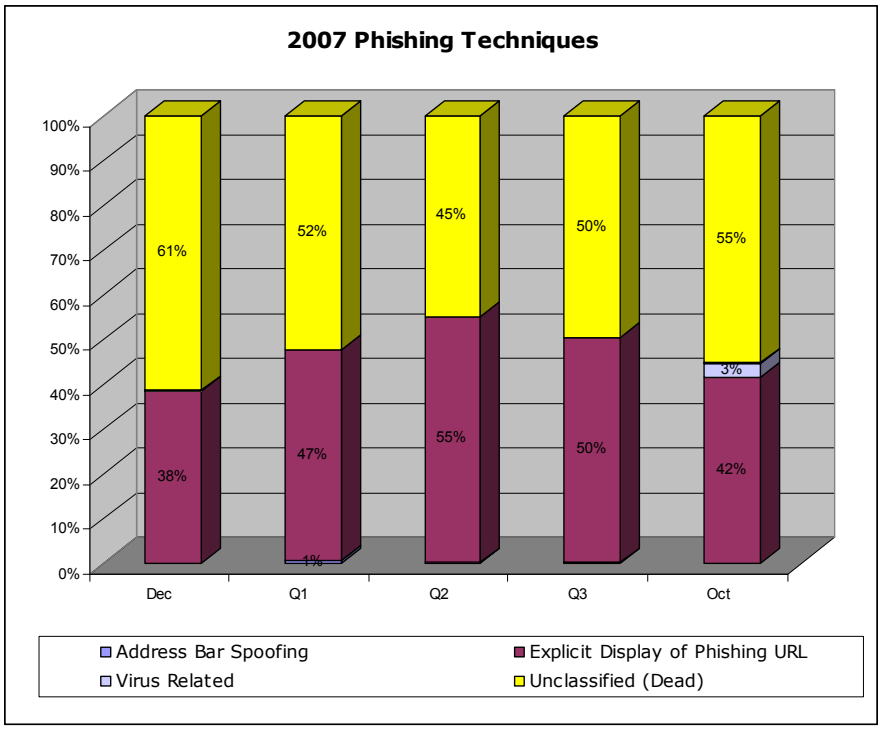
I phisher ancora all'attacco di PayPal ed eBay

Secondo il Content Security Team di Trend Micro, le prime 10 aziende attaccate dai phisher sono state le seguenti:

PRIME 10 AZIENDE ATTACCATE NEL 2007		% di attacchi sul totale	% di attacchi sulle prime 10
1	PayPal	7%	24%
2	eBay	6%	23%
3	Bank of America	5%	19%
4	Wachovia	3%	12%
5	BB&T	1%	5%
6	Citizens Bank	1%	4%
7	Fifth Third Bank	1%	4%
8	Poste Italiane	1%	3%
9	Regions Bank	1%	3%
10	Natwest	1%	3%

** Paypal appartiene ora a eBay.*

PayPal ed *eBay* sono i principali siti e-commerce attaccati dai phisher, e rispetto all'anno precedente si sono solamente scambiati le posizioni in classifica. I phisher si attendono guadagni anche dagli attacchi a istituti finanziari, ed ecco perché le posizioni successive sono quasi tutte occupate da banche. I siti di phishing per *MySpace* e *Facebook* non sono stati altrettanto comuni, ma vi è stato comunque un aumento dei casi di phishing relativi ai siti di social networking.
Le tendenze dei volumi del phishing sono influenzate soprattutto dai tool disponibili per creare siti di phishing.



Dietro all'incremento del phishing vi è la crescente popolarità tra i truffatori della tecnica rock phish. Il Content Security Web Blocking Team di Trend Micro calcola che gli URL rock phish siano mediamente tra 20.000 e 60.000 al giorno; la maggior parte di essi è associata ai medesimi indirizzi IP. Il numero di URL rock phish è cresciuto regolarmente nel corso dell'anno, sebbene i volumi complessivi abbiano seguito la tendenza del 2006 con una flessione significativa a settembre rispetto ad agosto.

Il gruppo responsabile della tecnica rock phish usa probabilmente la tecnica fast-flux per mantenere attivi i siti di phishing per periodi più lunghi. L'Anti-Phishing Work Group (APWG) ha affermato nell'*eCrime Researchers Summit* che il rock phishing contribuisce a quasi metà dei tentativi registrati. L'APWG suggerisce che se questo gruppo utilizza davvero fast-flux, allora è probabile che i siti di phishing possano essere attivi per intervalli più lunghi e attirare così un maggior numero di vittime.

Come se i kit rock phish non fossero sufficienti per aiutare i truffatori online, i phisher vendono ora un nuovo kit chiamato *Universal Man-in-the-Middle Phishing Kit.* Si tratta di un nuovo strumento che aiuta i phisher a raccogliere ancor più informazioni personali permettendo alle potenziali vittime di comunicare con un sito Web legittimo attraverso un falso URL creato dai phisher stessi. Simili ai kit rock phish, anche questi nuovi kit propongono un'interfaccia grafica basata su Web con la quale poter creare siti somiglianti a quelli legittimi presi di mira dai phisher. Il sito fasullo comunica con quello effettivo caricandone le pagine Web originali. La potenziale vittima e il sito legittimo comunicano lo stesso, ma il phisher può prelevare tutte le informazioni digitate dall'utente attraverso il falso sito.

Una pericolosa strategia che ha avuto diffusione nel 2007 è l'impiego di tecniche per il cambiamento del DNS. I server DNS sono quelli che traducono i nomi di dominio usati dagli umani negli indirizzi IP numerici che permettono ai computer di connettersi via Internet. Sebbene la maggior parte degli utenti utilizzi automaticamente i server DNS dei propri ISP, è possibile modificare la configurazione del computer perché si avvalga di server DNS differenti e magari installati in altri Paesi. Questi ultimi server traducono determinati domini in indirizzi IP diversi dagli originali, quasi certamente associati a siti pericolosi. Per esempio, gli utenti di famosi siti per cuori solitari hanno scoperto che le loro informazioni personali uscivano dai loro computer non appena infettati da un malware capace di modificare il DNS. Questa tecnica è usata anche nelle frodi perpetrate ai danni delle società pubblicitarie che pagano in base ai click effettuati. Nel 2007 Trend Micro ha registrato una crescita sostanziale delle botnet che cambiano il DNS.

Riepilogo:
1. Nei quattro anni dall'entrata in vigore della legge CAN-SPAM Act il problema dello spam non si è alleggerito. Gli spammer trasformatisi in truffatori hanno semplicemente modificato il campo d'azione avvalendosi di botnet e Trojan facenti la funzione di proxy per l'invio di spam, utilizzando i computer zombie di utenti inconsapevoli per spedire i loro messaggi: e questa è un'attività che non trova menzione nella CAN-SPAM.

2. Con i produttori di sicurezza che da anni raccomandano di filtrare gli allegati a livello del gateway, e con tecnologie che cercano di filtrare lo spam ricercando determinate parole chiave, gli spammer ricorrono oggi alle immagini e agli URL per aggirare i blocchi.

Le esigenze attuali comprendono quindi la capacità di verificare questi link in tempo reale.

3. Non vi sono state modifiche ai consueti obiettivi delle azioni di phishing, e questo è tipico poiché l'attenzione viene rivolta alle aziende commerciali e alle istituzioni bancarie e finanziarie più grandi e di maggior successo. L'ultima novità al riguardo è stata la localizzazione dei contenuti e il ricorso ai brand più noti a livello locale.

Le minacce distribuite

Le reti botnet

Nel gergo in uso nel settore della sicurezza, con il termine bot vengono identificati quei programmi pericolosi che riferiscono a una console di gestione centrale per ricevere ordini. Dal punto di vista del criminale informatico si tratta di programmi molto efficienti in quanto, mano a mano che i bot si diffondono, la popolazione che fa capo alla console aumenta e con essa la sua capacità. Le moderne botnet possono controllare centinaia di migliaia di PC infetti. Questa capacità pone nelle mani dei criminali informatici una grande potenza di calcolo e una notevole bandwidth di rete. Più cresce il numero dei computer infetti, maggiore diventa la pericolosità della botnet.

Durante il 2007 il protocollo di comunicazione più diffuso tra i creatori di botnet è stato ancora IRC (Internet Relay Chat). Ciò accade perché il software per creare programmi IRCbot è diffusamente disponibile e facile da implementare. Tuttavia il traffico IRC pericoloso può essere identificato con relativa facilità, ed ecco perché gli attaccanti hanno iniziato a utilizzare altri protocolli Internet per controllare le loro botnet. L'attenzione dei creatori di reti bot si è appuntata dunque sul protocollo HTTP (in uso nel Web) e sui protocolli P2P (Peer-To-Peer). La ragione risiede nel fatto che l'impiego di questi protocolli da parte delle botnet è molto più difficile da rilevare, in particolare quando viene fatto uso di cifratura nello scambio dei dati.

I protocolli P2P permettono di prolungare significativamente la durata e la ridondanza dei sistemi bot collegati a una botnet. In passato le reti bot erano spesso controllate da un unico server C&C (Command and Control) centrale. Quando questo server smetteva di funzionare l'intera botnet collassava, diventando inutilizzabile. L'uso dei canali di comunicazione P2P elimina questo singolo punto debole. I protocolli P2P permettono ai creatori di botnet di inserire i loro comandi in innumerevoli nodi attivi della rete P2P. I programmi bot provvedono poi a diffondere automaticamente i dati inseriti mentre si collegano l'uno all'altro. Questo approccio accresce incomparabilmente la robustezza dell'intera rete bot. Le nuove botnet P2P sono in grado di funzionare senza una console centrale, e per disabilitarle è necessario eliminare ogni singolo componente. Questo approccio è stato utilizzato per le botnet Storm e Spamthru.

DNS (Domain Name System) è uno dei protocolli Internet più vulnerabili, nonostante si tratti di un elemento essenziale per il funzionamento di Internet. Durante il 2007 i ricercatori hanno scoperto una backdoor dimostrativa che utilizzava le richieste DNS per le comunicazioni tra botnet e sistemi bot. Nonostante questo metodo di comunicazione dati appaia piuttosto nebuloso e non sia efficiente come la comunicazione HTTP, esso è comunque passibile di applicazioni pericolose, potendo essere utilizzato per facilitare il furto di informazioni.

Nel 2008 ci attendiamo un aumento della sofisticazione delle botnet. I programmi IRCbot verranno ancora utilizzati diffusamente in virtù della loro ampia accessibilità, ma le gang di criminali informatici di professione con grandi mezzi finanziari a disposizione continueranno ad ampliare l'uso di altri protocolli quali HTTP e P2P. Queste gang faranno anche un uso crescente di robusti codici per la cifratura dei dati pericolosi trasmessi, nell'intento di evitarne l'identificazione.

Nuwar: la “tempesta” continua

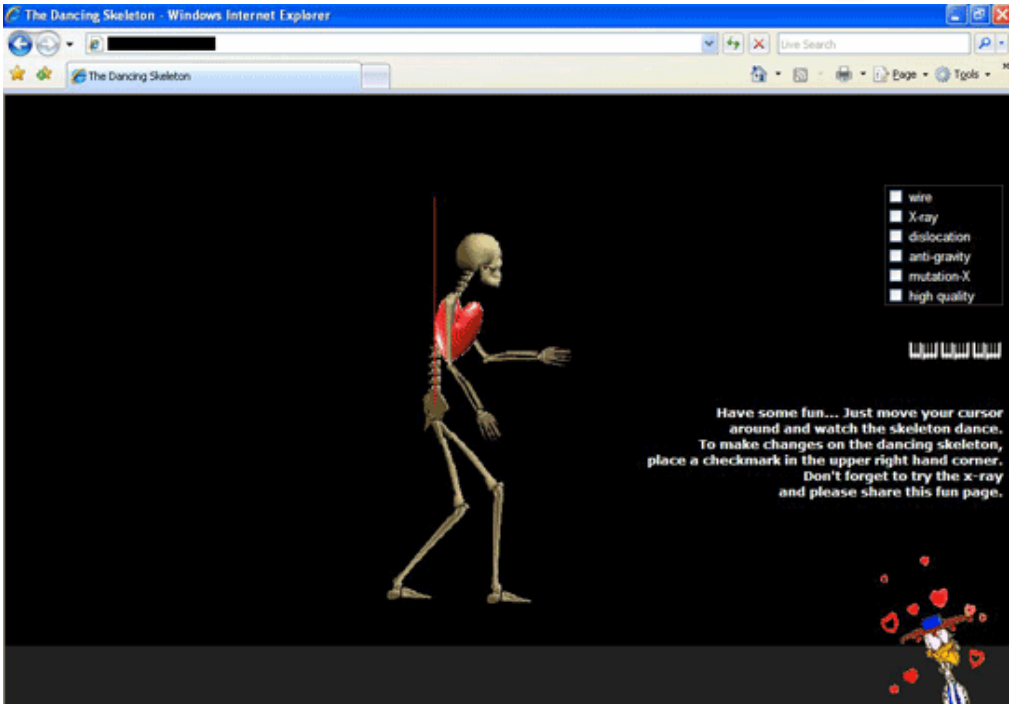
L'evento più significativo del 2007 in tema di reti bot ha riguardato NUWAR, una botnet conosciuta anche come STORM (Tempesta). Le caratteristiche salienti della rete Nuwar sono la tecnologia avanzata utilizzata, le grandi dimensioni, le drastiche misure aggressive contro qualunque ostacolo incontrato e, in particolare, le tecniche di social engineering senza precedenti.

I suoi creatori hanno utilizzato la botnet Nuwar per inviare messaggi spam, spedire spam sui guestbook, gestire siti Web pericolosi su computer infetti ed effettuare attacchi DDoS (Distributed Denial of Service). Tra le vittime degli attacchi DDoS ci sono stati anche gli esperti della sicurezza Internet che hanno probabilmente attivato un possibile attacco automatizzato quando hanno iniziato a investigare Nuwar. Tra le altre vittime degli attacchi condotti durante il 2007 spicca anche una gang rivale, spesso indicata come Stration (Warezov).

I sistemi bot appartenenti alla botnet Nuwar comunicano tra loro mediante un protocollo P2P chiamato Overnet. Ciò significa che non esiste un server Command and Control centrale che invia istruzioni ai sistemi bot. I comandi invece vengono trasmessi attraverso le comunicazioni P2P mentre i sistemi bot si collegano l'uno all'altro. Questa tecnica aumenta la ridondanza e prolunga l'esistenza dei computer infetti.

La botnet Nuwar utilizza tecniche fast-flux per i DNS e l'hosting dei domini. Fast-flux è una tecnica Domain Name System utilizzata dalle botnet per celare i siti che distribuiscono spam, phishing e codice malware dietro una rete mutevole di host compromessi che fungono da reverse proxy. Con questo approccio è possibile utilizzare una tecnica DNS round-robin per far puntare un nome di dominio a più host compromessi, i quali cambiano velocemente nel corso del tempo. Nuwar ha accresciuto notevolmente la ridondanza e la stabilità rispetto alle botnet fast-flux precedenti, le quali generalmente prelevavano contenuti Web e dati DNS da un unico server centrale. Nuwar ha eliminato questo singolo punto debole e ora i sistemi bot ricavano i contenuti Web dal traffico P2P.

La botnet Nuwar ha iniziato a operare verso la fine del 2006 con il lancio di messaggi e-mail apocalittici relativi alla morte del presidente degli Stati Uniti. I suoi creatori hanno dimostrato l'uso di tecniche avanzate di social engineering prendendo regolarmente spunto da eventi reali, quali la tempesta Kyrill che si è abbattuta sull'Europa Centrale nel mese di gennaio, il giorno di S.Valentino in febbraio, l'inizio del campionato della National Football League in settembre, Halloween in ottobre (si veda l'immagine seguente) e le festività natalizie in dicembre.



Altre tecniche efficaci hanno riguardato argomenti di interesse per i giovani: un finto programma per la condivisione di file musicali, cartoline di auguri, simpatici cuccioli di animali e i timori relativi all'opera della RIAA.

La botnet Nuwar ha visto l'uso di varie tecniche volte ad aggirare le tecnologie di rilevamento, quali l'impiego di file contenuti in archivi ZIP o RAR protetti tramite password oppure l'uso di immagini GIF nel corpo dei messaggi e-mail. A partire dal mese di maggio, i messaggi infettati da Nuwar non contenevano più una copia del worm ma un link a una pagina Web dove risiedeva il codice malware.

Uno studio delle infezioni create da Nuwar ha rivelato che il 28% degli indirizzi IP oggetto di messaggi e-mail infettati dal worm NUWAR si trova negli Stati Uniti. La distribuzione geografica completa è illustrata in Figura 1.

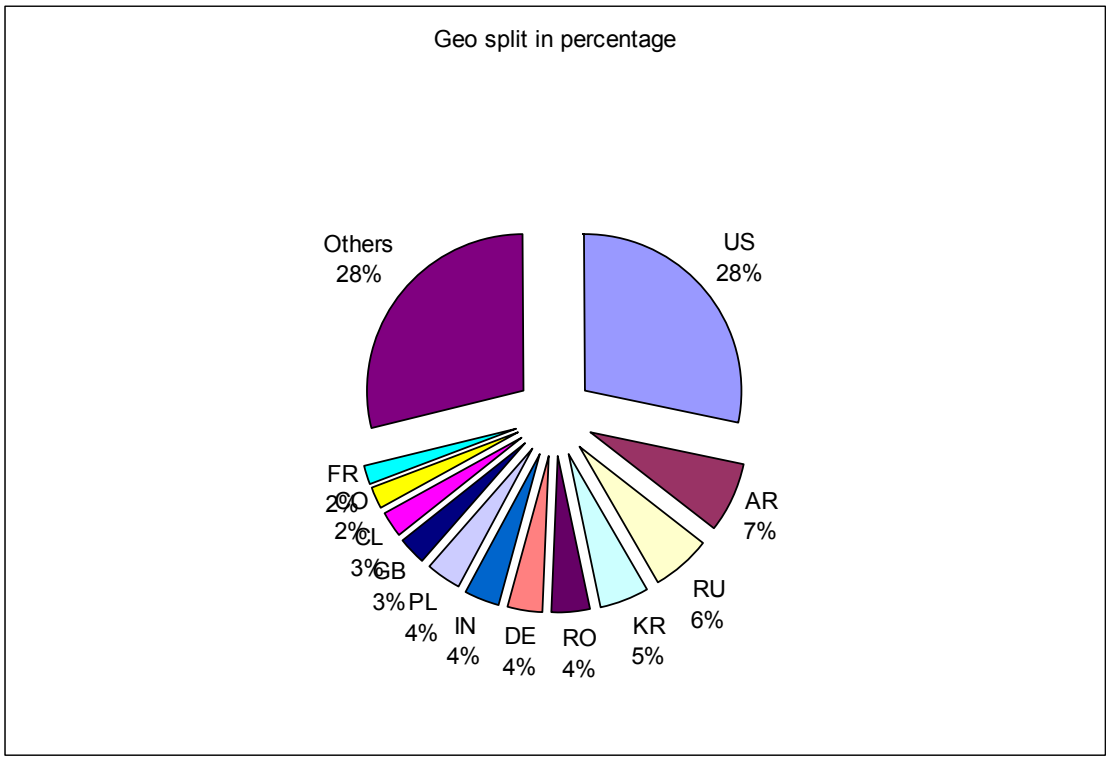


Figura 1: Suddivisione geografica degli host infettati da Nuwar.

Uno sviluppo significativo verificatosi nel mese di ottobre è stata la scoperta che questa gigantesca botnet si era suddivisa in diversi segmenti, ognuno dei quali utilizzava una differente chiave da 40 byte per cifrare il traffico trasmesso attraverso il protocollo P2P Overnet. La cifratura fa sì che le comunicazioni siano possibili soltanto tra i nodi della botnet che utilizzano l'identica chiave. Esistono diverse possibili ragioni per questa segmentazione. Una spiegazione può essere che i creatori del worm Nuwar stiano affittando separatamente i vari segmenti della botnet. Un altro motivo può essere la volontà di venderli ad altri criminali (spammer o ideatori di attacchi DoS) attraverso i forum clandestini.

Le tecnologie da combattere

L'impatto della botnet Nuwar durante il 2007 ha evidenziato la necessità di combattere l'abuso dei protocolli Internet utilizzati per le comunicazioni tra i sistemi bot e i loro creatori. Il traffico IRC pericoloso può oggi essere rilevato facilmente, ma il traffico P2P e HTTP rappresenta una sfida. Negli ambienti aziendali il traffico P2P dovrebbe essere completamente bloccato, in quanto aumenta comunque il rischio di fuoriuscite di dati. Nel caso degli utenti Internet privati, il traffico P2P pericoloso può essere rilevato attraverso il confronto con altre tipologie di traffico, come i messaggi spam in uscita. L'uso di scanner anti-virus aggiornati è in grado di proteggere gli utenti Internet da questo tipo di minaccia, mentre le comunicazioni bot via HTTP possono essere evitate bloccando il traffico indirizzato verso siti Web C&C noti.

L'economia digitale sommersa

Il settore della sicurezza è oggi pienamente conscio dell'economia sommersa che alimenta quelle attività che per gli utenti di computer si configurano come infezioni virali e altre forme di attacchi online. Il profilo degli autori di malware è davvero cambiato, passando dall'hacker teenager al criminale informatico di professione.

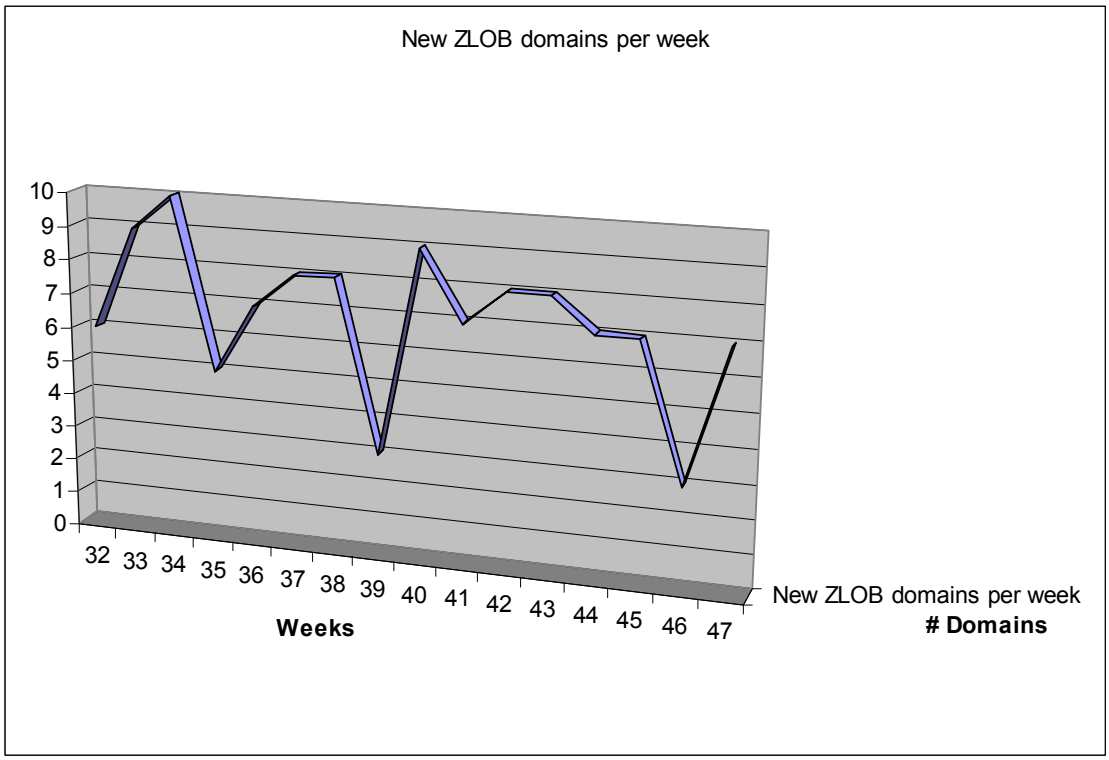
Durante il 2007 sono state rilasciate nei forum digitali clandestini nuove versioni dei toolkit malware MPack e IcePack. Questi toolkit sono programmi software di tipo "commerciale" che permettono anche a utenti non esperti di condurre attacchi informatici concentrandosi soltanto sul payload o sull'attività cui il programma malware è destinato. Oltre alle prove che confermano l'avvenuta compravendita di vulnerabilità nei forum clandestini e la loro integrazione all'interno di kit per l'aggiornamento dei sistemi bot, esistono testimonianze che indicano chiaramente come il settore del malware si stia trasformando sempre più in un'attività commerciale in grado di sfruttare l'affidabilità e la potenza economica dei mercati aperti.

La tabella che segue illustra chiaramente il crescente dinamismo commerciale dei criminali informatici. Da un lato si assiste al commercio di exploit kit impiegati congiuntamente con specifici payload, dall'altro ai frutti di queste attività: una messe di informazioni rubate relative ad account o indirizzi e-mail per lo spamming.

Tipologia	**Prezzo**
Prezzo per l'installazione di un singolo adware	Stati Uniti: 30 centesimi; Canada: 20 centesimi; Regno Unito: 10 centesimi; altri Paesi: 2 centesimi
Pacchetto malware, versione base	1.000-2.000 dollari
Pacchetto malware con servizi add-on	Da 20 dollari in su
Noleggio exploit kit - 1 ora	0,99-1,00 dollari
Noleggio exploit kit - 2,5 ore	1,60-2,00 dollari
Noleggio exploit kit - 5 ore	4,00 dollari variabile
Copia ancora ignota di Trojan horse per il furto di determinate informazioni	80,00 dollari variabile
Attacco Distributed Denial of Service	100,00 dollari al giorno
10.000 PC compromessi	1.000 dollari
Informazioni bancarie sottratte	da 50,00 dollari
1 milione di indirizzi e-mail nuovi (non verificati)	da 8,00 dollari in su, in base alla qualità

Dati campione tratti da uno studio sull'economia digitale sommersa nel 2007

Il grafico seguente mostra il numero di domini che ospitavano codice pericoloso (esclusi quelli che contenenti falsi add-on Windows Media Player) durante le ultime settimane del 2007. Si può notare che gli autori di malware creano una media di sette domini alla settimana, ognuno con una vita media di sei giorni. Ciò significa che è relativamente facile per gli autori di malware trovare nuovi servizi di hosting per le loro attività criminali.



Nel 2006 e nel 2007 sono stati identificati casi di infezione da parte di codice malware proveniente da siti Web nei quali ogni vittima ha ricevuto una versione esclusiva di un Trojan horse. Ad esempio, alcuni siti Web ospitano falsi codec ZLOB che installano un Trojan horse caratterizzato da un identificatore differente (noto anche come hash MD5) per ciascuna vittima. L'aspetto interessante è che i criminali informatici hanno la possibilità di mantenere l'algoritmo per la mutazione dei Trojan horse interamente sul server che ospita i file pericolosi. A differenza dei virus polimorfici, gli algoritmi di mutazione non devono essere distribuiti insieme al codice malware. In questo modo l'algoritmo di mutazione rimane segreto e diventa molto difficile, per non dire impossibile, creare pattern in grado di coprire tutto il codice malware diffuso dal sito Web pericoloso. Gli esperti Trend Micro prevedono che il polimorfismo del malware sul lato server conoscerà un ulteriore sviluppo durante il 2008.

Riepilogo: minacce distribuite ed economia digitale sommersa

1. L'impatto complessivo della minaccia Nuwar (Storm) in un anno del suo ciclo di vita deriva dall'attuazione di determinati elementi:

- Le tecnologie decentralizzate (P2P e IM) amplificano l'anonimato degli attaccanti.
- La legislazione e le forze dell'ordine dei vari continenti hanno un disperato bisogno di standardizzazione in relazione alle minacce e alle attività online/informatiche.
- Economia e certezza del lavoro sono fattori importanti per le attività criminali non soltanto nel mondo reale, ma anche in quello online.

- La formazione di base degli utenti è ancora carente, minando l'efficacia di qualunque tecnologia attualmente a disposizione dei consumatori. Le aziende che dispongono di policy di utilizzo più rigorose sono maggiormente in grado di apprezzare i vantaggi derivanti dal filtraggio dei contenuti.

Conclusioni e previsioni

Le tendenze identificate nel 2007 sono strettamente allineate alle previsioni stilate lo scorso anno. Il 2007 è stato realmente dominato dalle minacce Web. I numerosi attacchi contro organizzazioni online condotti attraverso siti Web violati, abuso di domini noti e innumerevoli attività di phishing testimoniano che le minacce stanno diventando sempre più mirate. L'espansione e le attività recenti della botnet NUWAR indicano chiaramente l'intensificarsi della minaccia rappresentata dalle reti bot, con il conseguente accentuarsi dei pericoli per i potenziali bersagli.

Negli anni recenti le prolifiche gang di autori di malware sono riuscite a implementare connessioni Internet di alta qualità in Asia, Europa e Stati Uniti per periodi di tempo prolungati. Un chiaro esempio di ciò è offerto da Russian Business Network (RBN), una società di hosting salita alla ribalta nel 2007 per aver ospitato attività di criminali informatici che utilizzavano falsi nomi di registrazione per creare un'infrastruttura atta a celare le loro attività. Altri esempi di questa tendenza sono costituiti dalle gang ZLOB e Gromozon. Per il 2008 prevediamo che questo tipo di minaccia non sarà più confinato in determinate aree "malfamate" di Internet, ma conoscerà una crescente diffusione.

Previsioni sulle minacce

1. Il codice legacy utilizzato nei sistemi operativi e le vulnerabilità delle applicazioni più diffuse continueranno a costituire un bersaglio ideale per l'inserimento di codice pericoloso che consenta ai criminali informatici di violare la sicurezza di reti e computer nell'intento di sottrarre informazioni proprietarie riservate.
2. I più noti siti Web operanti in aree quali social networking, banche/finanza, giochi online, motori di ricerca, viaggi, biglietti per eventi, pubblica amministrazione, news, lavoro, blog, e-commerce e aste online continueranno a rappresentare il vettore di attacco privilegiato dai criminali informatici per inserirvi link a programmi per il phishing e il furto dell'identità.
3. I dispositivi non gestiti, quali smartphone, lettori MP3, cornici digitali, chiavette USB e console per videogiochi, continueranno a offrire a criminali informatici e autori di malware l'opportunità per penetrare il perimetro di sicurezza delle aziende grazie alle loro capacità di archiviazione, elaborazione e supporto Wi-Fi. Gli access-point pubblici, come quelli presenti all'interno di locali di ritrovo, biblioteche, alberghi ed aeroporti continueranno a fungere da vettore di attacco o canale di distribuzione per il malware.
4. I servizi di comunicazione, quali la posta elettronica e l'instant messaging, oltre che la condivisione dei file, continueranno a essere esposti a minacce basate sui contenuti quali spam delle immagini, URL e allegati pericolosi che utilizzano tecniche di social engineering mirate e localizzate, in considerazione dell'efficacia dimostrata nei confronti delle potenziali vittime da parte dei criminali interessati ad estendere le dimensioni delle botnet e a sottrarre informazioni riservate.
5. Le strategie per la protezione dei dati e la sicurezza del software diventeranno uno standard nel ciclo di vita delle applicazioni commerciali a causa del numero crescente di

gravi incidenti verificatisi. Ciò comporterà una crescente attenzione per le tecnologie di cifratura dei dati durante le fasi di archiviazione e trasmissione, in particolare per ciò che riguarda il controllo dell'accesso ai dati nelle catene di informazione e distribuzione.

Previsioni tecnologiche:

I drammatici mutamenti che interessano il panorama delle minacce continueranno ad alimentare l'evoluzione delle tecnologie necessarie per proteggere efficacemente i clienti. L'epoca in cui la protezione antivirus basata sulle segnature era sufficiente sono ormai tramontati. Oggi gli autori di malware collaborano attivamente per evitare il rilevamento attraverso la creazione di minacce in costante mutazione che interagiscono fra loro per aggirare le metodologie di rilevamento tradizionali basate sulle segnature. Le attività criminose sono globali, collaborative e insidiose, mirando a sovraccaricare e saturare i sistemi di tipo legacy che analizzano la "firma" del malware sviluppati e utilizzati proficuamente dai vendor di programmi antivirus nel corso degli ultimi 20 anni. La crescita esplosiva dei file pattern testimonia la difficoltà di mantenere aggiornata la protezione, e i benchmark tradizionali che confrontano il tasso di identificazioni positive non costituiscono più un indicatore valido della capacità di una soluzione di proteggere efficacemente gli utenti.

Gli aggiornamenti dei tradizionali pattern anti-virus/anti-spam rivolti a identificare ed eliminare i programmi malware attraverso l'identificazione delle relative segnature devono essere utilizzati congiuntamente ad altre tecniche e tecnologie in grado di implementare una protezione onnidirezionale e stratificata contro le minacce Web che tentano di sfruttare a proprio vantaggio la natura interattiva di Internet. L'implementazione generalizzata delle soluzioni di sicurezza a livello di gateway, rete ed endpoint non basta più. È necessaria una rivoluzione per far sì che i criminali informatici non riescano nei loro intenti. Oltre a fornire la protezione di base, le tecnologie di sicurezza "in-the-cloud" saranno gli strumenti ideali per rispondere proattivamente alle minacce Web nuove ed emergenti.

Le tecnologie di sicurezza "In-the-cloud" devono combattere la minaccia alla fonte, prima dunque che il traffico raggiunga il gateway Internet. I database "cloud-based" vengono aggiornati dinamicamente in tempo reale, riducendo la dipendenza da database locali e aggiornamenti frequenti attraverso la minore necessità di correlazioni dei pattern e altri approcci desktop onerosi in termini di gestione e memoria.

Le tecnologie di sicurezza "in-the-cloud" d'importanza critica comprendono dunque:

Tecnologie per la reputazione Web:

- Monitorano i siti Web attraverso tecniche di filtraggio degli URL, verificano la corrispondenza tra siti IP e URL, e controllano il punteggio di reputazione dei siti Web fornito da appositi database.
- Aggiornano continuamente e dinamicamente i database, permettendo ai vendor di prodotti per la sicurezza di rispondere tempestivamente e controbattere ogni nuova minaccia proveniente dal Web e dalla posta elettronica.
- Bloccano l'accesso ai siti Web pericolosi sulla base del punteggio di reputazione del dominio relativo.

Tecnologie per la reputazione e-mail:

- Confrontano gli indirizzi IP con un database reputazionale e un servizio dinamico che monitora in tempo reale i pattern del traffico Internet e il comportamento degli IP che spediscono e-mail , bloccando le minacce Web rappresentate da computer zombie, botnet e altre sorgenti di spam.

Tecnologie per il monitoraggio di botnet e comportamenti bot:

- Analizzano il traffico sulla rete e i comportamenti bot per identificare i server botnet di comando e controllo.
- Monitorano costantemente i server per identificare e bloccare soltanto quelli effettivamente attivi.
- Forniscono un feed aggiornato di indirizzi IP corredato da informazioni dettagliate riguardanti il grado di confidenza e il tipo di minaccia.
- Bloccano le comunicazione da e per i server di comando e controllo sulla base dell'indirizzo IP.

Best-practice

Gestione di patch e vulnerabilità

- Installare sulla rete programmi software per la scansione delle vulnerabilità e programmarne l'esecuzione almeno a cadenza settimanale.
- Verificare che tutti i sistemi operativi e tutte le applicazioni software installate siano aggiornate con gli update e le patch di sicurezza più recenti rilasciate dai vendor.
- Quando possibile, abilitare le funzioni di aggiornamento e installazione automatici.
- Applicare i nuovi aggiornamenti non appena vengono rilasciati. Utilizzare programmi software per la gestione groupware per implementare gli aggiornamenti in tutta l'organizzazione.
- I consumatori dovrebbero utilizzare i pacchetti per la sicurezza Internet più recenti, che incorporano funzionalità integrate per firewall, filtraggio dei contenuti e prevenzione di vulnerabilità ed exploit.

Gestione delle risorse software

- Formulare rigorose policy per l'utilizzo di Internet e del software e standardizzare il software nei vari segmenti della rete.
- Condurre iniziative di auditing della sicurezza e rimuovere qualunque software non correlato alle attività operative dell'azienda.
- Limitare l'accesso alle porte e ai protocolli non necessari sulla rete aziendale e valutare opzioni adeguate nel caso in cui l'uso dei protocolli P2P, IM o IRC rappresentino una necessità operativa.
- Limitare i privilegi degli utenti sulla rete e impedire la modifica non autorizzata dei vari componenti del sistema operativo allo scopo di limitare le attività di programmi rootkit e Trojan horse.
- Implementare sull'intera rete la scansione groupware di tutto il traffico relativo al Web, ai trasferimenti di file e alla posta elettronica, accertandosi che gli utenti non possano aggirarla.

- I consumatori dovrebbero utilizzare le funzioni parental control. Si consiglia di utilizzare le funzioni di controllo sugli accessi e di limitare i privilegi d'uso definiti di default. La maggior parte dei sistemi per videogiochi esistenti, infatti, dispongono di accesso online, pertanto è opportuno regolarne l'uso da parte dei minori.

Sensibilizzazione e policy per gli utenti finali

- Utilizzare strategie di sicurezza fisiche e online. Limitare l'introduzione di dispositivi di elaborazione personale tramite apposite policy aziendali.
- Accertarsi che le soluzioni per il filtraggio dei contenuti forniscano informazioni chiare, spiegando i motivi in base ai quali un determinato sito è stato bloccato anziché limitarsi a visualizzare un messaggio di errore.
- Implementare strategie comprendenti misure difensive stratificate che supportano la gestione il reporting integrati delle minacce
- Preparare report giornalieri che stabiliscono la priorità delle minacce in base alla pericolosità e definiscono le azioni opportune. Condividere i risultati tra tutti gli utenti attraverso analisi causa/effetto delle minacce.
- Varare campagne per la sensibilizzazione degli utenti relativamente ai vari ambienti di elaborazione. Formulare guideline di base riguardanti i tipici scenari di attacco.
- I consumatori dovrebbero prestare attenzione alle rubriche tecnologiche all'interno dei programmi di news quotidiani, in quanto le aziende di prodotti anti-malware generalmente si preoccupano di informare il grande pubblico riguardo le minacce relative a phishing, online banking, social network e così via.

Autori

Hanno collaborato:
Jaime Lyndon Yaneza
Todd Thiemann
Christine Drake
Jon Oliver
David Sancho
Feike Hacquebord
Anthony Arrott
George Moore
Joey Costoya
Macky Cruz
Wiebke Lips
Elizabeth Bookman