“MINACCE INFORMATICHE NEL I SEMESTRE 2008”

In questa relazione sarà analizzata la dinamica di sviluppo del malware nel primo semestre del 2008 e sarà effettuato il confronto con i dati del secondo semestre del 2007.

La relazione contiene una grande quantità di fatti e di informazioni statistiche.

In primis essa è indirizzata ai professionisti che operano nell'ambito della sicurezza informatica, e che si interessano al malware, ma può essere utile anche a tutti gli utenti che sono interessati ai problemi della virologia informatica.

Risultati del semestre

I primi sei mesi del 2008 hanno confermato le previsioni da noi fatte alla fine dell'anno scorso circa l'evoluzione dei programmi maligni, e nello specifico:

Continua evoluzione delle cosiddette tecnologie Malware 2.0
Evoluzione dei rootkit
Ritorno dei virus di file
Attacchi sui siti di social network
Minacce per la piattaforma mobile

Uno dei programmi maligni più significativi del primo semestre 2008 è stato, senza dubbio, Storm worm (classificato da Kaspersky Lab come Zhelatin), il quale rimane al comando di Malware 2.0. Ci sono state circa dieci insorgenze degne di nota che hanno fatto utilizzo di metodi conosciuti e testati: mailing di massa contententi link a server compromessi o configurati in modo da contenere un worm, diffusione degli stessi link sui siti di social messaging o diffusi tramite IM.

Per quanto riguarda i rootkit, il problema dei "bootkit" (comparso a fine 2007) è diventato più di una minaccia, con l'aggiunta di nuove modifiche di Sinowal. Anche se questo programma non si è evoluto, non si può dire che i bootkit abbiano smesso di rappresentare un problema. Le tecnologie bootkit rappresentano una sfida piuttosto seria per le attuali tecnologie anti-virus, e l'attuale assenza di bootkit sembra essere più che altro una pausa che non il frutto di una decisione da parte dei virus writer di rinunciare allo sviluppo di tali programmi maligni.

Parlando di rootkit "classici", il “mitico” Rustock.c è stato finalmente identificato (si veda http://www.viruslist.com/en/analysis?pubid=204792011 per i dettagli). Questo evento ha provocato alcuni problemi all'industria anti-virus, non solo in termini di identificazione e disinfezione, ma anche per quanto riguarda i metodi impiegati per raccogliere ed esaminare nuovi campioni e la velocità di reazione alle minacce da parte del produttore di soluzioni AV.

È possibile, partendo dalle tecnologie usate in Rustock.c, costruire due catene: una catena logica e una tecnologica, entrambe che conducono ad altre due questioni importanti, cioè l'offuscamento e il polimorfismo. I metodi utilizzati in Rustock per camuffare il codice e complicare la sua analisi, e la messa a punto di metodi di resistenza, sono da tempo stati impiegati attivamente nei virus di file. Questi approcci sono stati sviluppati soprattutto da scrittori di virus cinesi. Comunque, questi sviluppi hanno portato all'aggiunta delle funzioni-virus a una varietà di backdoor e worm, piuttosto che condurre alla creazione di nuovi virus di file.

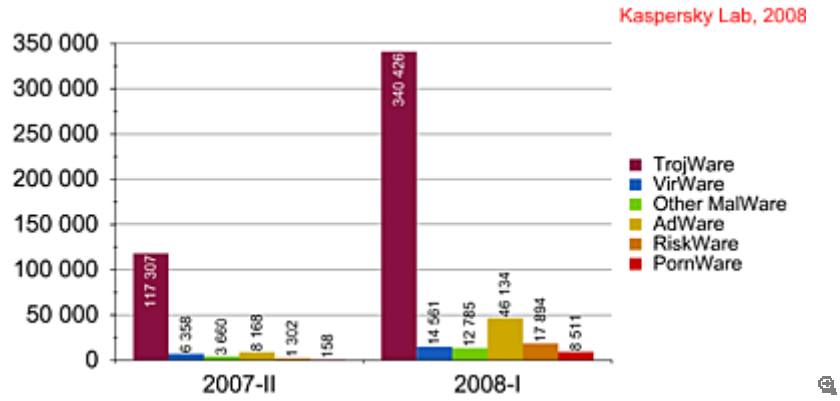
I virus di oggi non si limitano più esclusivamente alla funzione di infezione dei file: essi sono diventati dei potenti componenti delle botnet creati per rubare dati dell'utente e condurre attacchi DDoS. Gli esempi più ovvi sono Virut, Alman, Allaple, e i worm Fujack e Autorun. Nel primo semestre del 2008, questi codici maligni hanno provocato una miriade di infezioni nel mondo, portandoci a capire che, nel futuro prossimo, la funzionalità dei virus continuerà ad essere aggiunta ai backdoor e ai worm.

I social network sono stati oggetto dei più grandi attacchi della loro storia. Queste popolarissime reti sono diventate terreno di gioco per le tecnologie virus e spam, e vengono attaccate non più solo dai worm XSS: i virus writer si sono spostati dalla ricerca di vulnerabilità nei motori dei siti di social network verso approcci provati di ingegneria sociale, come

il semplice invio di messaggi da parte di "amici" che contengono link a siti infetti. MySpace e Orkut sono tra I siti più attaccati, mentre Facebook è diventato un bersaglio un po' più tardi (gli utenti russi sono stati attaccati da worms e Trojan che si diffondevano tramite i popolarissimi portali Odnoklassniki.ru e Vkontakte).

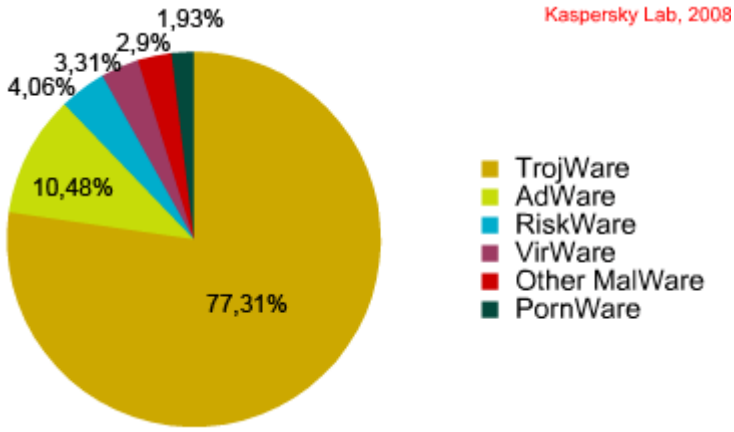
Le “minacce mobili” hanno improvvisamente cambiato direzione: invece di attaccare gli smartphone, i virus writer hanno deciso di cambiare tattica e specializzarsi in Trojan per le piattaforme J2ME, capaci di funzionare quasi su qualsiasi telefono cellulare. Questi programmi maligni (ne sono stati identificati circa 50) hanno lo stesso payload: inviano SMS a numeri a pagamento, azzerando o riducendo il conto telefonico dell'utente e convogliando i profitti direttamente nelle tasche dell'autore del Trojan.

Nei primi 6 mesi del 2008, ben 440.311 programmi sono stati aggiunti al nostro database anti-virus, contro i 136.953 dei sei mesi precedenti.



Numero dei nuovi programmi maligni identificati (secondo semestre 2007 – primo semestre 2008)

Programmi identificati	2007-II	2008-I	2007-II%	2008-I%	Differenza	Crescita
TrojWare	117307	340426	85,65%	77,31%	8,34%	190,20%
AdWare	8168	46134	5,96%	10,48%	-4,51%	464,81%
RiskWare	1302	17894	0,95%	4,06%	-3,11%	1274,35%
VirWare	6358	14561	4,64%	3,31%	1,34%	129,02%
Other MalWare	3660	12785	2,67%	2,90%	-0,23%	249,32%
PornWare	158	8511	0,12%	1,93%	-1,82%	5286,71%
Totale progr. identificati	136953	440311	100,00%	100,00%		



Ripartizione dei programmi maligni identificati, per classi. I semestre 2008

Malware

Nel primo semestre del 2008 gli analisti di «Kaspersky Lab» hanno rilevato 367.772 nuovi programmi malware, 2,9 volte di

più rispetto al secondo semestre del 2007. Il numero dei nuovi programmi maligni rilevabili in media in un mese è stato pari a 61.295,33.

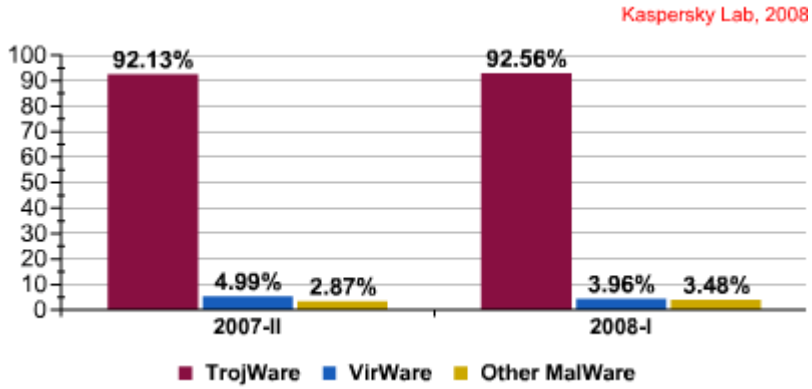
In totale il numero dei nuovi programmi malware è aumentato del 188,85%. I dati relativi ai ritmi di crescita superano notevolmente i risultati del 2007, quando era stato rilevato il 114% in più di malware rispetto al 2006.

Ricordiamo che secondo la classificazione di «Kaspersky Lab» esistono tre classi di malware:

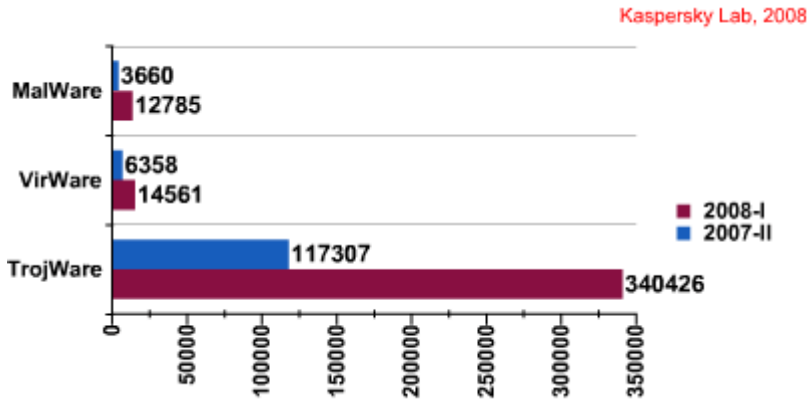
1. TrojWare: vari programmi Trojan senza possibilità di autoreplicazione (backdoor, rootkit e Trojan di vario tipo);
2. VirWare: programmi malware autoreplicanti (i virus ed i worm);
3. Other MalWare: vari software, usati intensamente dai malfattori per creare malware e per organizzare attacchi.

L'anno 2008 non ha riportato modifiche significative riguardo alle classi di malware. Leader assoluti, come prima, rimangono i Trojan, i quali rappresentano oltre il 92% di tutto il malware esistente. Il numero di nuovi Trojan, rilevati nel primo semestre del 2008, è aumentato del 190,2% rispetto al semestre precedente. Ma la percentuale di Trojan fra tutti i programmi di malware è cresciuta solo dello 0,43%: questo è un risultato notevolmente inferiore rispetto alla crescita di oltre il 2,5 % del 2007.

Si è intravisto un mutamento di tendenza negli ultimi due anni, quando la quota dei vari Trojan aumentava e gli indici di VirWare e di Other MalWare diminuivano. Nel primo semestre del 2008 la quota dei programmi del gruppo Other MalWare è cresciuta. Tra l'altro questa crescita, superiore allo 0,5 %, è maggiore rispetto ai risultati della categoriasse dominante, il TrojWare.



delle classi di malware (secondo semestre del 2007 e primo semestre del 2008)



Numero dei nuovi malware, rilevati nel primo semestre del 2008 (per classi)

Total	2008	2007	Quota 2008	Quota 07	Differenza	Crescita
TrojWare	340426	117307	92,56%	92,13%	0,43%	190,20%
VirWare	14561	6358	3,96%	4,99%	-1,03%	129,02%
Other MalWare	12785	3660	3,48%	2,87%	0,60%	249,32%
MalWare	367772	127325	100	100		188,85%

Un anno fa – nell'estate del 2007 – alla quota di Other MalWare si attribuiva l'1,95% di tutti i malware. Tale indice ha cominciato a crescere nel secondo semestre del 2007 (2,87%), e nella prima metà del 2008 la tendenza è rimasta invariata. Secondo i risultati del semestre, la quota della classe Other Malware ha raggiunto il 3,48%. Tenendo conto che il numero dei nuovi programmi di questa classe è cresciuto di 3,5 volte rispetto alla seconda metà del 2007, si può constatare una crescita vertiginosa del numero delle «minacce non tradizionali».

Il numero dei nuovi programmi del gruppo Other Malware è aumentato quasi del 250%, il che ha permesso loro di avvicinarsi quasi del tutto al VirWare. In sei mesi sono stati rilevati solo 1776 rappresentanti della famiglia Other Malware in meno, rispetto ai nuovi programmi di WirWare. A fine anno, a condizione di mantenere i medesimi ritmi crescita presso ambedue le classi, sarà molto probabile che si verifichi il raggiungimento, da un punto di vista quantitativo, della seconda posizione da parte di Other Malware.

Ulteriori fattori di crescita della quota dei programmi della classe Other MalWare sono stati sia la comparsa di molteplici nuovi exploit, sia un notevole ampliamento dello spettro dei comportamenti maligni, che prima erano fuori dal campo di osservazione delle ditte produttrici di programmi anti-virus (fraud tools) e che sono stati aggiunti ai database anti-virus nel primo semestre del 2008.

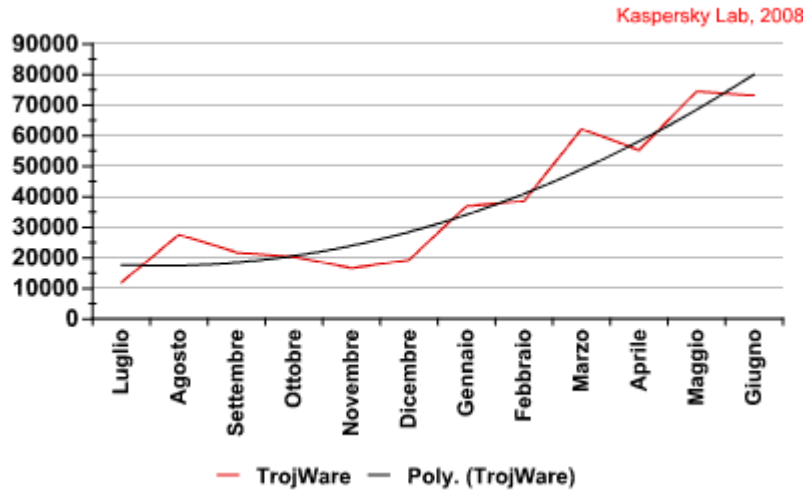
Un analogo processo di crescita della classe dei programmi VirWare, cominciato cinque anni fa, ha determinato il fatto che i virus ed i worm, leader di presenze fino a quel momento, abbiano praticamente interrotto il proprio sviluppo. La diminuzione della quota del VirWare è continuata anche nel 2008: questa categoria ora rappresenta meno del 4% di tutto il malware, con un 1,03% in meno rispetto al secondo semestre del 2007. Nonostante ciò, i ritmi di riduzione delle quote di VirWare superano quelli dello scorso anno. La crescita del numero di nuovi virus e worm rimane notevolmente indietro rispetto agli analoghi indici delle altre classi: di essi, infatti, è stato rilevato il 129,0% in più rispetto al semestre precedente.

Nel complesso, si può constatare che nella distribuzione delle classi di malware siamo giunti a un periodo di stabilizzazione. Le cause oggettive di ciò sono sia il predominio raggiunto dai TrojWare sia un lento mutamento del principale oggetto delle minacce.

Esaminiamo più nel dettaglio quali sono i mutamenti avvenuti in ognuna delle 3 classi.

Trojan

Riportiamo il numero di nuovi Trojan rilevati dagli analisti di Kaspersky Lab ogni mese in un diagramma (luglio 2007 - giugno 2008):



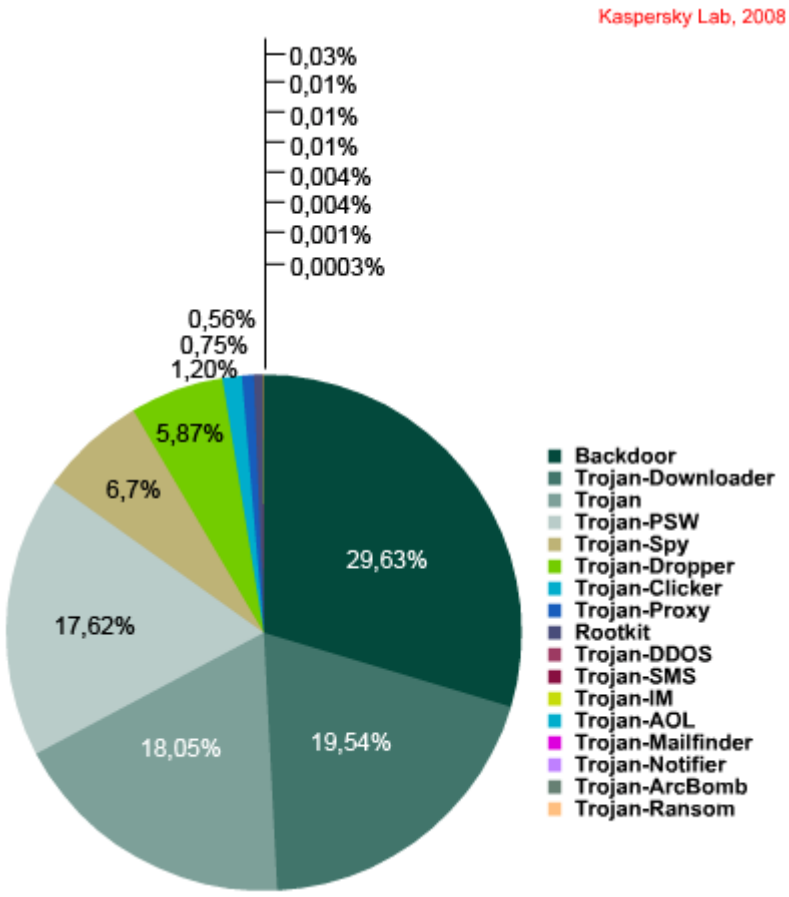
Il numero di nuovi Trojan rilevati dagli analisti di Kaspersky Lab (luglio 2007 – giugno 2008)

Nella seconda metà del 2007 il numero dei nuovi Trojan rilevati per mese ha cominciato a diminuire. Ma dall'inizio del 2008 questi hanno cominciato a crescere nuovamente raggiungendo, secondo i risultati semestrali, il 190,2%. Durante i primi sei mesi del 2008 sono stati registrati tre picchi: a gennaio, a marzo e a maggio. Dopo ognuno di questi picchi, seguiva un leggero calo oppure un periodo di stabilità, successivamente alternato ad un periodo di crescita ancora più rapida del numero di nuovi Trojan. Questo quadro ripete in parte la dinamica del 2007. Allora, sono stati notati due picchi (a maggio e ad agosto) con successive riduzioni, il che si differenzia radicalmente dalla dinamica del 2006, quando la crescita del numero dei nuovi Trojan era di tipo continuo.

È più probabile che in un futuro scrutabile continueremo ad assistere ad una rapida crescita del numero di nuovi Trojan. Questa, tuttavia, non viene accompagnata dal perfezionamento tecnologico: i Trojan rimangono, per la maggior parte, creature abbastanza primitive di script-kiddies poco istruiti, e l'aumento della loro quantità dipende esclusivamente dalla

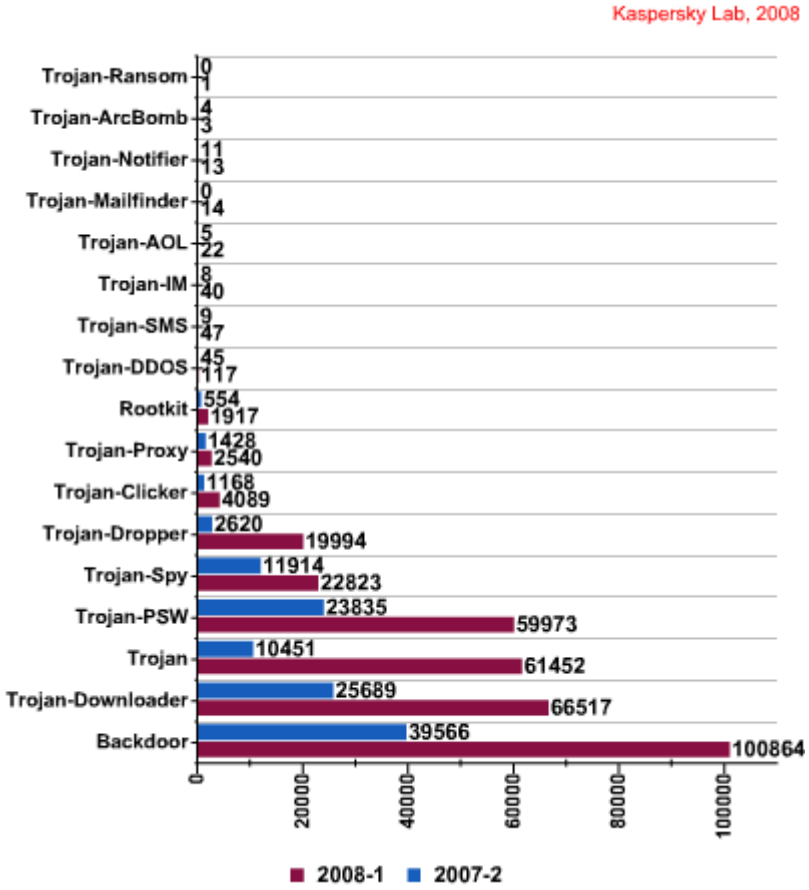
facile reperibilità nel «mercato nero», e dalla relativa facilità della loro diffusione.

I mutamenti più significativi rispetto alla distribuzione dei comportamenti all'interno di questa classe riguardano il comportamento dei Trojan (quei programmi classificati come “Trojan” invece di “Trojan-Dropper”, ad esempio), che sono risaliti dalla quinta posizione alla terza, diventando uno dei primi comportamenti.

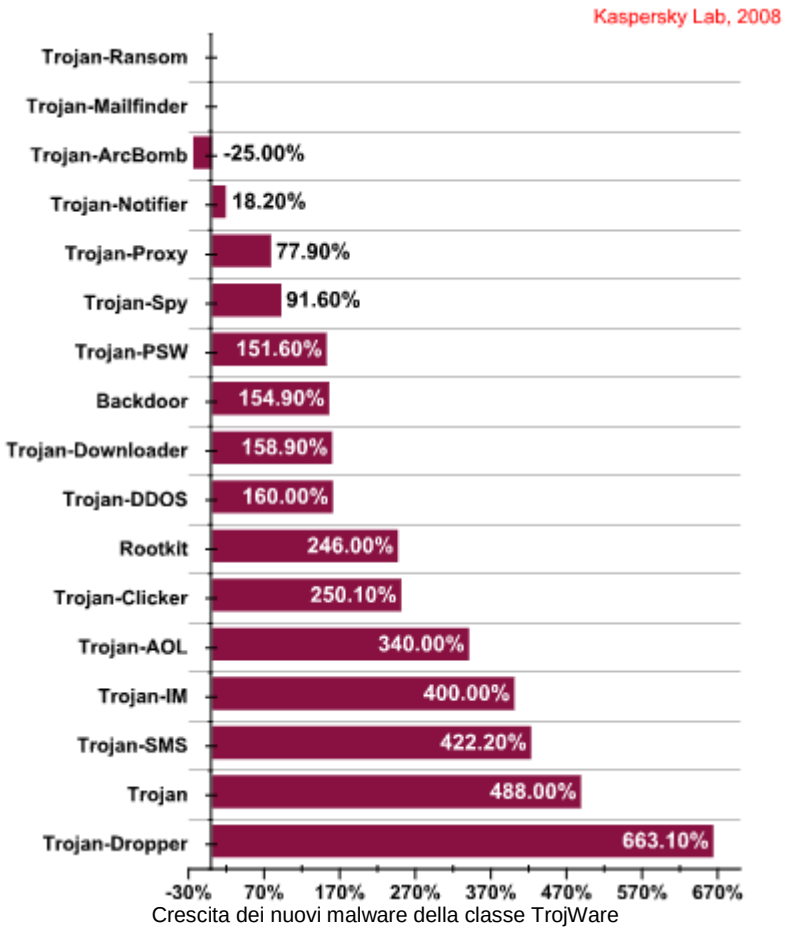


TrojWare: rapporto dei comportamenti

Per capire meglio i mutamenti verificatisi tra i Trojan, esaminiamo ora l'incremento avvenuto tra i vari comportamenti così come sono stati manifestati dai programmi maligni .



Numero di nuovi malware della classe TrojWare (per comportamento)



Crescita dei nuovi malware della classe TrojWare

TrojWare	Primo semestre del 2008	Secondo semestre 2007	Crescita	Quota 2008	Quota 2007	Differenza
Backdoor	100864	39566	154,90%	29,63%	33,73%	-4,100%
Trojan-Downloader	66517	25689	158,90%	19,54%	21,90%	-2,360%
Trojan	61452	10451	488,00%	18,05%	8,91%	9,142%
Trojan-PSW	59973	23835	151,60%	17,62%	20,32%	-2,701%
Trojan-Spy	22823	11914	91,60%	6,70%	10,16%	-3,452%
Trojan-Dropper	19994	2620	663,10%	5,87%	2,23%	3,640%
Trojan-Clicker	4089	1168	250,10%	1,20%	1,00%	0,205%
Trojan-Proxy	2540	1428	77,90%	0,75%	1,22%	-0,471%
Rootkit	1917	554	246,00%	0,56%	0,47%	0,091%
Trojan-DDOS	117	45	160,00%	0,03%	0,04%	-0,004%
Trojan-SMS	47	9	422,20%	0,01%	0,01%	0,006%
Trojan-IM	40	8	400,00%	0,01%	0,01%	0,005%
Trojan-AOL	22	5	340,00%	0,01%	0,004%	0,002%
Trojan-Mailfinder	14	0		0,0040%	0,000%	0,004%

Trojan-Notifier	13	11	18,20%	0,0040%	0,009%	-0,006%
Trojan-ArcBomb	3	4	-25,00%	0,0010%	0,003%	-0,003%
Trojan-Ransom	1	0		0,0003%	0,000%	0,000%
Totale TrojWare	340426	117307	190,20%			

Nel primo semestre del 2008 una crescita davvero impressionante (oltre 200%) fra i Trojan l'hanno dimostrata i Trojan-Dropper, i Trojan, i Trojan-Clicker e i Rootkit. (Non prendiamo in considerazione gli indicatori dei ritmi di crescita dei comportamenti di Trojan-AOL, Trojan-IM, Trojan-SMS, perché il numero di tali programmi è davvero esiguo).

Più di tutto colpiscono i risultati relativi ai Trojan-Dropper. La crescita di oltre il 660% è un record degli ultimi anni per i tutti i tipi di Trojan. La crescente popolarità di questi programmi di malware è stata causata dal fatto che un numero sempre maggiore di virus writer ha cominciato ad usare la tattica di nascondere il Trojan all'interno delle distribuzioni di altri programmi per collocare nel medesimo tempo, sul computer ormai infetto, la massima quantità possibile di vari Trojan. Questa situazione è la conseguenza del fatto che nel mondo della criminalità informatica della distribuzione dei programmi si occupano gruppi specializzati e non i loro diretti autori o gli acquirenti.

Queste stesse cause, probabilmente, hanno un legame con la dinamica degli indici dei Trojan-Downloader. Questo comportamento, che nel 2006 era numericamente all'apice, nello scorso anno ha ceduto il primo posto al comportamento Backdoor. Nel primo semestre del 2008 i Trojan-Downloader sono riusciti a conservare il secondo posto (superando i Trojan solo per l'1%), ma ciò è stato accompagnato da una successiva diminuzione della quota dei Downloader fra i tutti i TrojWare (-2,4%).

Suscita interesse anche la crescita del 488% nel numero di Trojan «comuni». Precedentemente i Trojan facevano parte della «seconda categoria» di comportamento e non c'era nessun presupposto che alludesse alla loro crescita impetuosa. Quello che è successo con i Trojan nel primo semestre del 2008 è causato, per svariati motivi, dal tentativo degli scrittori di virus di migliorare la versatilità del codice Trojan. Sempre più spesso rifiutano la pratica della creazione di un certo numero di moduli funzionali che interagiscano l'uno con l'altro, ma provano piuttosto a realizzare tutto nell'ambito di una sola applicazione. Tale approccio è una reazione dei malintenzionati al potenziamento delle esistenti tecnologie antivirali: è più facile per un singolo Trojan prolungare il periodo fra la nascita del malware e la sua cattura nei database anti-virus.

La crescente popolarità dei Trojan-Clicker è dovuta all'attenzione dei criminali informatici verso uno dei vari metodi di guadagno illegale di Internet, ovvero quello che si ottiene cliccando sui link pubblicitari e con la gonfiatura del rating di certi siti. Questo tipo di frode è noto da tanto tempo, ma fino al 2008 non suscitava grande interesse tra i virus writer. La situazione è cambiata nel 2008: in 6 mesi si è riscontrato un aumento del 250% di nuovi Trojan-Clicker rispetto al semestre precedente.

Relativamente ai rootkit, nonostante i significativi ritmi di crescita (246%) la loro quota rispetto a tutti i Trojan ha subito un cambiamento piuttosto irrilevante (+0,9%).

Nel mese di giugno Kaspersky Lab ha individuato alcune nuove categorie di comportamento: Trojan-Mailfinder e Trojan-Ransom.

Le funzioni di base dei programmi, entrati a far parte del Trojan-Mailfinder, consistono nella raccolta degli indirizzi di posta elettronica dai computer infetti per completare i database degli spammer. Questo comportamento è composto da vari Trojan e da segmenti di programmi che precedentemente appartenevano al comportamento SpamTool della categoria OtherMalware.

Anchi se pochi nel numero, i pericolosissimi Trojan-Ransom sono da noi identificati in un comportamento a parte. Di essi fanno parte tutti quei programmi maligni che in un modo o nell'altro rendono inutilizzabile il sistema operativo, criptano i file dell'utente per permettere ai malintenzionati di ottenere, dalle vittime, del denaro per il loro ripristino.

Nel luglio del 2008 nella nostra classifica apparivano ancora due comportamenti: Trojan-Banker e Trojan-GameThief.

Del Trojan-Banker entreranno a far parte tutti i Trojan che si occupano del furto dell'accesso agli account dei sistemi bancari e dei dati delle carte di credito. Precedentemente tali programmi facevano prinicpalmente parte del comportamento Trojan-Spy e Trojan-PSW.

Il Trojan-GameThief dovrebbe unificare una moltitudine di Trojan orientati al furto dei dati degli utenti dai giochi online di maggior popolarità. Ricordiamo che lo scorso anno proprio i Trojan di gioco sono diventati il tipo di malware più diffuso. Del comportamento Trojan-GameThief andranno a far parte alcune famiglie, che prima venivano classificata come Trojan-Spy e Trojan-PSW.

La creazione di una serie di nuovi comportamenti dei Trojan deve esercitare una notevole influenza sull'esistente distribuzione di questi programmi in base al comportamento. Probabilmente potremo essere in grado di raccontare

qualcosa di ciò già nel nostro successivo rapporto sui risultati dell'intero anno 2008.

Ora, all'interno della specie dei Trojan si possono identificare tre principali gruppi di comportamento:

1. Backdoor, Trojan-Downloader, Trojan, Trojan-PSW. Sono i TrojWare più diffusi, che nel complesso costituiscono circa l'85% dell'intera specie (la quota di ogni comportamento nella massa generale dei TrojWare supera il 17%). In 6 mesi i Trojan sono diventati il gruppo più numeroso, con un incremento percentuale del 9%. Bisogna notare che tra tutti e quattro i comportamenti del primo gruppo, solo la quota dei Trojan è aumentata, mentre gli indici dei restanti comportamenti sono diminuiti (ad esempio il calo dei Backdoor è stato di oltre il 4%).
   Nella seconda metà del 2008 questo gruppo registrerà un alto ritmo di crescita, stimato di oltre 150%. Continuerà l'aumento della quota di Trojan e la diminuzione dei Trojan-Downloader e Trojan-PSW. I Backdoor, come prima, resteranno comunque il malware di maggiore popolarità, soprattutto grazie agli sforzi dei virus writer cinesi.
2. Trojan-Spy e Trojan-Dropper. Durante i primi sei mesi del 2008 dal secondo gruppo i Trojan sono passati al primo, e la loro vecchia posizione è stata occupata dai Trojan-Dropper, provenienti dal terzo gruppo. I parametri dei comportamenti del secondo gruppo costituiscono il 5-7% del totale. I ritmi di crescita dei Trojan-Spy e Trojan-Dropper sono molto diversi tra di loro (dobbiamo ricordare che i Trojan-Dropper hanno stabilito un record con un ritmo di crescita pari al 663,1%).
   Nel secondo semestre del 2008 la quota dei Dropper probabilmente continuerà a crescere, la qual cosa permetterà a questo comportamento di avvicinarsi al primo gruppo. Nel secondo gruppo probabilmente rientreranno anche quei Trojan creati di recente: i Trojan-Banker e i Trojan-GameThief.
3. Trojan-Proxy, Trojan-Clicker, Other. La percentuale di crescita di ogni comportamento è inferiore all'1,2%, eccetto che per i Trojan-Clicker, i cui ritmi di crescita non sono significativi.
   Non è esclusa la crescita di programmi di uno di questi comportamenti fino al raggiungimento del livello dei Trojan-Clicker, ma è molto più probabile che il numero di programmi maligni di questo gruppo continui a diminuire, vista la spinta incalzante dei rappresentanti del primo gruppo.

Del terzo gruppo, sono di particolare interesse i Trojan-SMS, il numero dei quali nella prima metà del 2008 è cresciuto del 422%, raggiungendo quota 50. Si tratta di un indice molto modesto se confrontato con gli oltre 100.000 nuovi Backdoor. Comunque, i Trojan-SMS si differenziano da tutti i restanti programmi maligni, perché agiscono e funzionano sui cellulari e rappresentano la più pericolosa minaccia agli apparecchi mobili.

Minacce per la telefonia mobile: inizio della commercializzazione

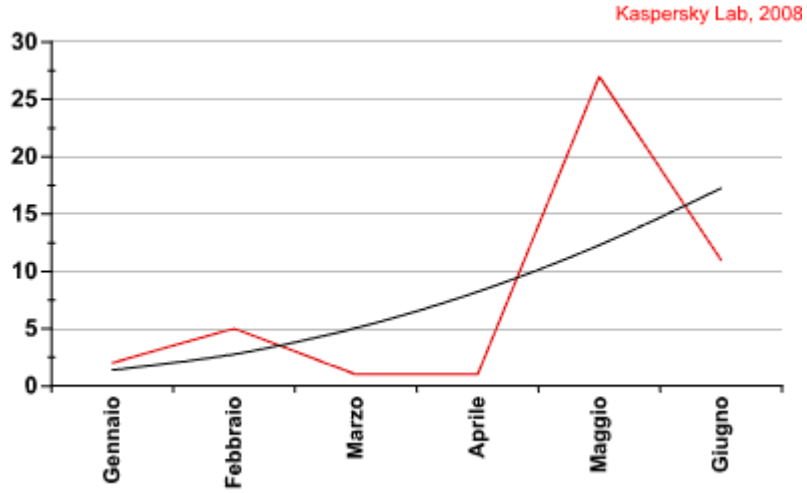
Il primo semestre del 2008 è stato interessante dal punto di vista delle minacce per la telefonia mobile, più precisamente per uno dei settori delle minacce: i Trojan che di nascosto inviano SMS a pagamento ai numeri brevi del servizio SMS Premium.

In questo contesto va notato quanto segue:

1. Crescita del numero dei programmi Trojan-SMS.
2. Capacità di adattamento dei Trojan ad altre piattaforme di telefonia mobile: viene minacciato qualsiasi tipo di cellulare che supporti le applicazioni Java o che abbia l'interprete del linguaggio Python.
3. Crescita del numero di siti WAP sui quali sono localizzati tali Trojan.
4. Comparsa in ICQ di messaggi spam che pubblicizzano i siti WAP e il malware in essi localizzato.
5. Vari metodi di ingegneria sociale usati durante la diffusione ed il mascheramento dei malware.
6. Quantità fissa dei numeri brevi ai quali di nascosto vengono inviati gli SMS.

Di queste e altre tendenze parleremo più dettagliatamente in seguito.

Cominciamo con la crescita del numero dei malware di comportamento Trojan-SMS. Durante il primo semestre del 2008 è stata rilevata una quantità di tali programmi che supera il numero di tutti Trojan-SMS che esistevano prima. Dobbiamo ricordare che il primo malware di questo comportamento è stato rilevato da noi il 27 febbraio 2006 (Trojan-SMS.J2ME.RedBrowser.a).



Quantità dei nuovi Trojan-SMS, riscontrati dagli analisti di Kaspersky Lab (secondo i mesi del 2008)

Nel complesso, durante i primi sei mesi del 2008, è stato riscontrato il 422% in più di nuovi Trojan-SMS, rispetto al secondo semestre del 2007.

Attualmente vi sono 9 famiglie per la piattaforma J2ME, 3 per Symbian e 1 per Python.

Quindi, cosa rappresentano tali Trojan? Di fatto, essi sono delle creazioni piuttosto primitive.

Parlando di Trojan J2ME, va detto che la maggior parte di essi ha la seguente struttura: archivio JAR, che contiene alcuni file class. E proprio uno di questi file esegue l'invio del messaggio SMS a pagamento al numero breve (logicamente, senza chiedere il permesso dell'utente relativamente all'invio e senza avvisarlo sul costo di tale messaggio). I restanti file class esistono al solo scopo di mascheramento. All'interno dell'archivio possono esserci varie immagini (molto spesso di contenuto erotico), come pure il file Manifest, il quale in alcuni casi viene impiegato per l'invio dei messaggi.

Per quanto riguarda la famiglia Trojan-SMS.Python.Flocker, in questo caso si differenzia solo la piattaforma del malware, ma l'essenza (il programma primitivo e l'obiettivo del programma) rimane la stessa. Nell'archivio SIS c'è uno script, scritto in linguaggio Python, che effettua l'invio dei messaggi al numero breve del servizio SMS Premium, come pure i script aggiuntivi che servono per mascherare l'attività principale del malware.

Uno dei principali pericoli del Trojan-SMS è la sua capacità di adattamento a piattaforme diverse. Se in un cellulare (proprio un cellulare, non necessariamente uno smartphone) è stata installata una Java Machine, allora su tale dispositivo il Trojan-SMS.J2ME può funzionare senza alcun problema. Per quanto riguarda il Trojan-SMS.Python, in questo caso si parla di capacità di adattamento a piattaforme diverse nel segmento degli smartphone con sistema operativo Symbian. Se sul cellulare (qualsiasi sia il suo sistema operativo) c'è un interpreter Python, allora il Trojan-SMS.Python sarà in grado di funzionare.

I luoghi di diffusione di tali programmi maligni sono i vari portali WAP, nei quali viene proposto al visitatore di scaricare melodie, immagini, giochi ed applicazioni per il cellulare. La maggioranza assoluta dei Trojan si nasconde sotto l'aspetto di altre applicazioni, dalle quali si possono inviare SMS gratuiti o che danno la possibilità di usare l'Internet mobile gratuitamente, oppure sono mascherate da applicazioni di carattere erotico o pornografico.

A volte i virus writer inventano dei metodi di mascheramento delle azioni maligne del programma che sono piuttosto originali. Cosicché, dopo l'avvio da parte dell'utente di Trojan-SMS.J2ME.Swapi.g, sul display del cellulare appare una formula di saluto con la proposta di vedere un'immagine dal contenuto pornografico. Affinché questo accada è necessario riuscire a premere il tasto «SI», fintanto che non inizia a suonare un breve segnale musicale. (Nell'archivio JAR del programma si può trovare sia il file PNG con l'immagine, sia la melodia MIDI). Nel tentativo di riuscire a premere il tasto in tempo, l'utente non si accorge che ogni volta che preme il tasto (non ha importanza se viene premuto in tempo oppure no) si verifica l'invio del messaggio al numero breve ed il prelevamento di una certa somma di denaro dal suo conto.

Praticamente tutti i siti contenenti malware danno agli utenti la possibilità di collocare i loro file. La semplicità di registrazione (letteralmente avviene con un paio di click) e l'accesso gratuito a tali servizi permettono ai virus writer di diffondere le loro creazioni senza alcun problema. Al malintenzionato non resta che dare al file un nome più attraente per le sue vittime potenziali (free_gprs_internet, invio_sms_gratuito, ragazze_svestite ecc.), scrivere un commento altrettanto attraente ed attendere il momento in cui uno degli utenti decide di «inviare un SMS gratuito» o di «guardare l'immagine erotica».

Dopo la collocazione del software maligno il malintenzionato deve pubblicizzarlo. A questo punto viene in suo aiuto l'invio di massa tramite ICQ o di spam nei vari forum. Perché proprio ICQ? Dobbiamo ricordare che questo servizio di scambio di messaggi istantanei è molto popolare in Russia e nei paesi dell'ex Unione Sovietica. Tanti utenti che vogliono avere una possibilità costante di comunicare, usano gli ICQ-client mobili. Per il malintenzionato, queste persone sono le ideali vittime

potenziali.

sua◊Viene cosi creata un'interessante catena: creazione del malware invio dello◊dislocazione presso il sito WAP con un nome e commenti attraenti e spam, che può raggiungere gli utenti degli ICQ-client mobili.

Ora ci è rimasta da esaminare solo una questione che riguarda i numeri brevi usati dai Trojan per la telefonia mobile. Fra tutti i programmi malware che sono stati riscontrati da Kaspersky Lab, i numeri di maggiore popolarità erano 3 numeri brevi: 1171, 1161, 3649. Va detto che questi numeri vengono usati non solo dai malintenzionati ma anche da varie ditte legali, che forniscono servizi di vario tipo. La destinazione del pagamento dipende dal prefisso con il quale esso è stato inviato. Nei vari Trojan-SMS questi prefissi cambiano, ma a volte si riscontrano delle ripetizioni.

La popolarità di questo tipo di criminalità informatica, specialmente in Russia, è dovuta alla estrema semplicità dei metodi di pagamento via SMS.

È noto che gli operatori di telefonia mobile affittano i numeri brevi. Ad un utente privato affittare un numero di questo tipo costa troppo caro. Esistono però i Content Provider, i quali possiedono questi numeri brevi e li subaffittano, aggiungendo un determinato prefisso.

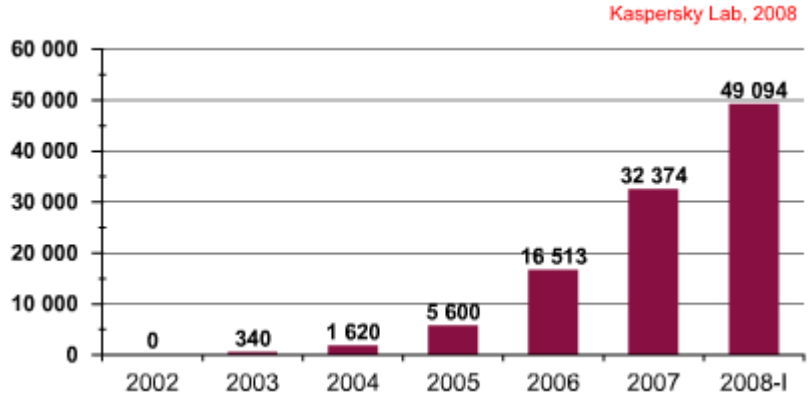
Così, un numero breve come 1171 appartiene ad uno di questi provider, però se al numero 1171 sarà inviato un messaggio che inizia con «S1», allora il sistema del provider trasferirà una parte del costo di tale SMS sul conto del subaffittuario «S1».

L'operatore di telefonia mobile trattene per sé dal 45% al 49% dal costo del messaggio inviato al numero breve, e circa il 10% lo riceve il provider che affitta questo numero. Il resto del denaro viene inviato al subaffittuario, nel nostro caso al «truffatore di telefonia mobile».

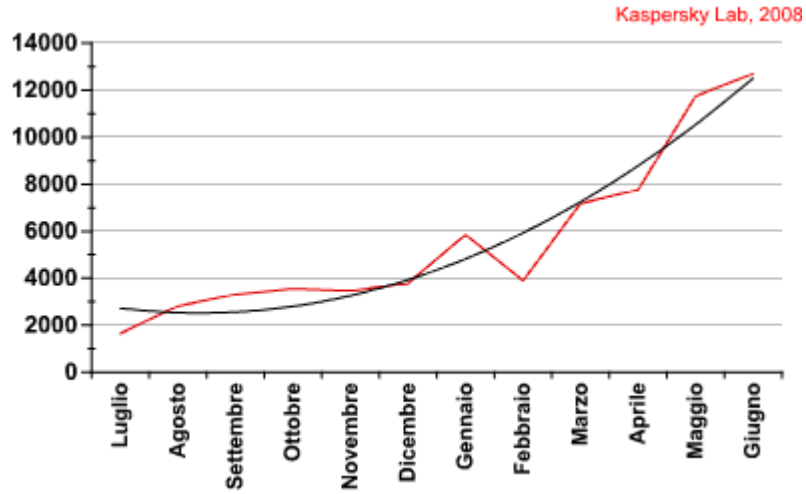
Tirando le somme, possiamo dire che il primo semestre del 2008 è stato caratterizzato dalla prima significativa crescita nella storia del malware per la telefonia mobile che invia SMS ai numeri brevi a pagamento all'insaputa dei proprietari dei cellulari. È evidente che tutti questi programmi, sono stati creati con un solo scopo: guadagnare denaro tramite i numeri brevi e, più precisamente, tramite i messaggi SMS che sono stati occultamente inviati a questi numeri. La semplicità di creazione e diffusione di tali applicazioni potrebbe portare verso una successiva crescita del malware di comportamento Trojan-SMS nel secondo semestre del 2008. Seguiremo lo sviluppo della situazione.

Trojan «ludici»: il gioco continua

Una delle tendenze più emblematiche dell'anno scorso, la crescita rapidissima del numero di nuovi programmi malware indirizzati al furto di password per i giochi online, è rimasta confermata anche nel primo semestre del 2008. In sei mesi sono stati rilevati 49094 nuovi Trojan «di gioco». Questa cifra è superiore una volta e mezza a quella rilevata durante tutto il 2007, e supera del 264,6% gli indici del precedente semestre.



Quantità dei nuovi TrojWare che rubano le password dei giochi online, riscontrati dagli analisti di Kaspersky Lab

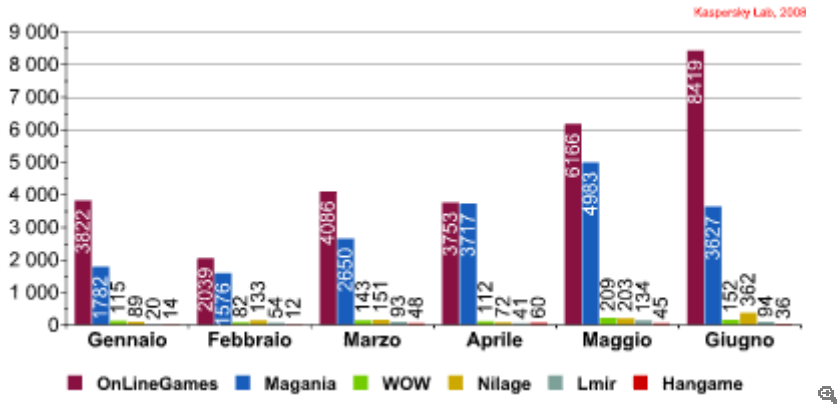


Quantità dei nuovi TrojWare «ludici»,riscontrati dagli analisti di Kaspersky Lab (luglio 2007- giugno 2008)

Il 95% di tutti i nuovi Trojan «di gioco», riscontrati nel primo semestre del 2008, ruba le password non di un solo gioco, ma a più giochi insieme. Fanno parte di tali programmi i rappresentanti delle famiglie Trojan-PSW.Win32.OnLineGames e Trojan-PSW.Win32.Magania.

OnLineGames è un gruppo numeroso, la sua quota secondo i risultati dell'anno è pari al 57,6% di tutti i Trojan di gioco. La quantità di malware di questa famiglia durante i primi sei mesi del 2008 è cresciuta vertiginosamente, superando considerevolmente la crescita dei Trojan che rubano le password di un solo gioco.

È curioso notare che i Trojan del gruppo Magania sono orientati ad utenti di un solo popolare portale di giochi (per saperne di più, si veda http://en.wikipedia.org/wiki/Gamania). Anche se dal mese di maggio questa famiglia ha cominciato bruscamente a perdere popolarità in seguito alla chiusura, sullo stesso portale, di alcuni mondi (tra cui «MapleStory»): stando ai risultati del semestre, di Magania fa parte il 37,4% di tutti nuovi Trojan «ludici».

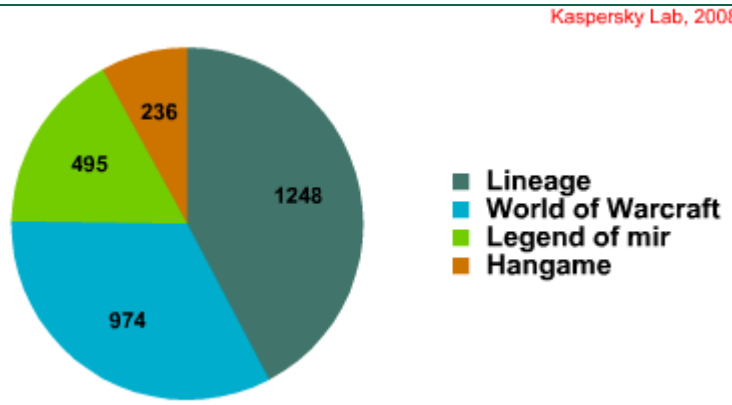


Numero dei nuovi Trojan di gioco di maggiore popolarità (per mesi del 2008)

Trojan-PSW.Win32.OnLineGames - ruba le password di più di un gioco online
Trojan-PSW.Win32.Magania – attacca il portale Gamania
Trojan-PSW.Win32.Ganhame – attacca il gioco Hangame Online
Trojan-PSW.Win32.Lmir – Legend of Mir
Trojan-PSW.Win32.Nilage – Lineage
Trojan-PSW.Win32.WOW – World of Warcraft

La popolarità dei giochi online tra i virus writer dipende direttamente dalla diffusione di questi giochi tra i giocatori e dal livello di sviluppo del mercato dei valori virtuali di un determinato gioco.

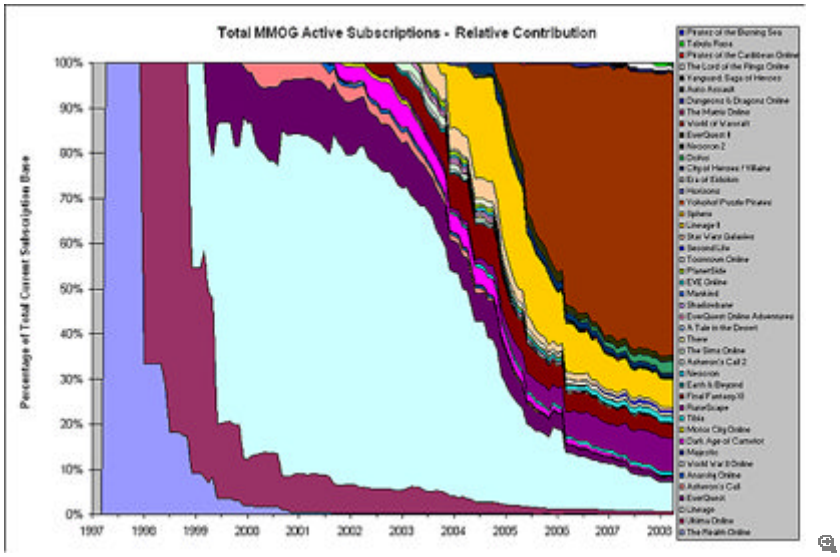
La parte del leone tra i Trojan di gioco indirizzati al furto di password di un solo gioco online spetta al malware che attacca i giocatori di quattro popolarissimi giochi in Cina: Legend of Mir, Hangame, Lineage e World of Warcraft (con essi si gioca in tutto il mondo).



Ripartizione dei Trojan maggiormente popolari orientati verso un solo gioco

Come si vede dal grafico, qui i Trojan sono indirizzati al furto delle password del gioco online Lineage. Secondo la statistica del sito mmogchart.com (vedi qui sotto), Lineage, che è stato uno tra i primi a comparire nella rete, ancora nel 1999, occupò per quattro anni una posizione leader per numero di associati. Attualmente Lineage, il più sviluppato fra tutti i giochi online, ha un mercato di proprietà virtuali completamente formato, e che vende ormai proprietà per del denaro che non è per nulla virtuale.

Il gioco World of Warcraft, leader assoluto nel mercato online, occupa il secondo posto in fatto di popolarità fra i virus writer. Ma nonostante ciò, proprio ad esso appartiene il record mensile del numero di nuovi TrojWare: a maggio sono stati riscontrati 209 Trojan indirizzati ad utenti che giocano con World of Warcraft, il ché corrisponde a 6 -7 nuovi Trojan al giorno.



Ripartizione degli iscritti ai giochi online
Fonte – mmogchart.com

Nel primo semestre del 2008 si è modificato il metodo principale di diffusione di malware che si occupano del furto di password per i giochi online. Nel 2007 i malintenzionati preferivano usare come veicolo i programmi auto-propaganti (worm e virus). Attualmente, il metodo più popolare per diffondere i Trojan di gioco ai computer degli utenti è la forzatura massiccia di siti (per esempio tramite iniezione SQL) e l'uso di exploit per caricare Trojan sui computer dei visitatori di questi siti.

Lo schema usato per la diffusione è abbastanza riuscito. Ma nella maggioranza dei casi l'attacco non era indirizzato ad un obbiettivo preciso: qualsiasi visitatore del sito forzato poteva essere infettato dal Trojan «ludico», e non solo il giocatore. I malintenzionati hanno deciso di sfruttare i vantaggi dell'infezione effettiva ed hanno allargato le funzioni base dei TrojWare «ludici»: nel primo semestre del 2008 gli scrittori di virus hanno cominciato ad aggiungere nei programmi di furto di password dei giochi online i moduli backdoor, i quali permettono di riunire i computer infetti in reti-zombie.

Così, nel primo semestre del 2008 il business criminale legato al furto dei personaggi dei giochi online e della proprietà virtuale continuava a svilupparsi. Ogni giorno Kaspersky Lab rivelava in media 273 nuovi Trojan di gioco, dei quali 259 erano capaci di rubare password non solo per uno, ma contemporaneamente per più di un gioco online. Per quanto riguarda il numero di nuovi malware, la famiglia Trojan-PSW.Win32.OnLineGames occupa il secondo posto, preceduta

solo da Backdoor.Win32.Hupigon.

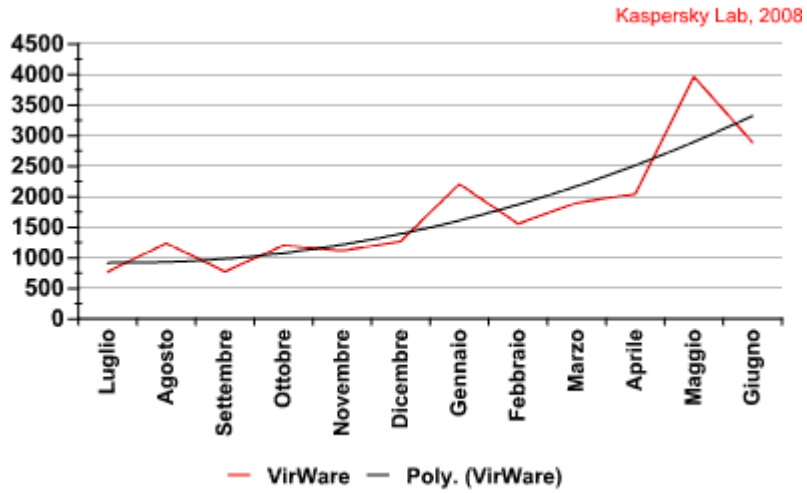
I virus writer hanno ottimizzato lo schema di attacco da loro elaborato precedentemente, cominciando ad utilizzare i siti forzati. Se precedentemente i Trojan che rubavano le password dei giochi online rappresentavano una minaccia solo per i giocatori, ora essi sono pericolosi per tutti: la schiacciante maggioranza di Trojan «ludici» rilevati nel corso degli ultimi mesi è fornita delle funzioni base di backdoor.

Nel prossimo futuro lo sviluppo del malware indirizzato ai giocatori online continuerà senza dubbio alcuno.

Worm e virus

Delle tre classi di malware il VirWare ha mostrato il ritmo di crescita più basso: “solo” il 129%, tuttavia risultati così modesti si osservano in oltre duemila nuovi virus e worm al mese.

Rappresentiamo, con questo diagramma, la quantità di nuovi programmi VirWare riscontrati ogni mese dagli analisti di Kaspersky Lab:

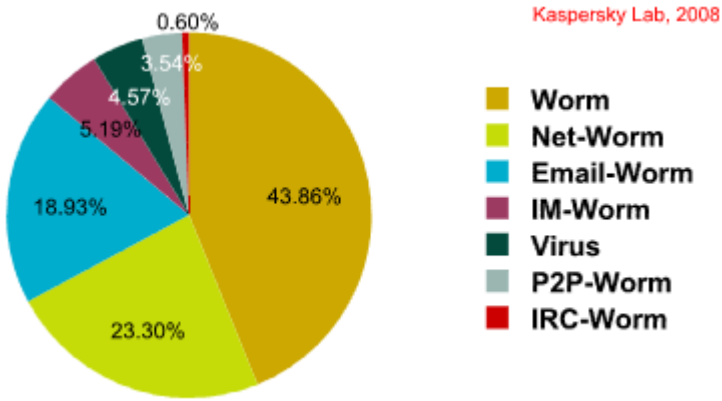


Numero di nuovi programmi VirWare, riscontrato dagli analisti di Kaspersky Lab (luglio 2007 – giugno 2008)

A prima vista, la situazione riguardante la dinamica della crescita del numero di nuovi malware di questa classe è abbastanza simile a quella del TrojWare: anche qui si osservano periodi di salita e di successivo calo. Però, il VirWare di simili picchi nel 2008 ne ebbe solo due e non tre come è per la categoria TrojWare. Questo significa che questa classe di malware vive e si sviluppa secondo leggi proprie. La diversità dei virus e dei worm rispetto alle restanti classi di malware viene evidenziata da ritmi di crescita molto più lenti, per i VirWare solo del 129%. Nel primo semestre del 2008 questo ha portato ad un'altra diminuzione della loro quota di più dell'1%.

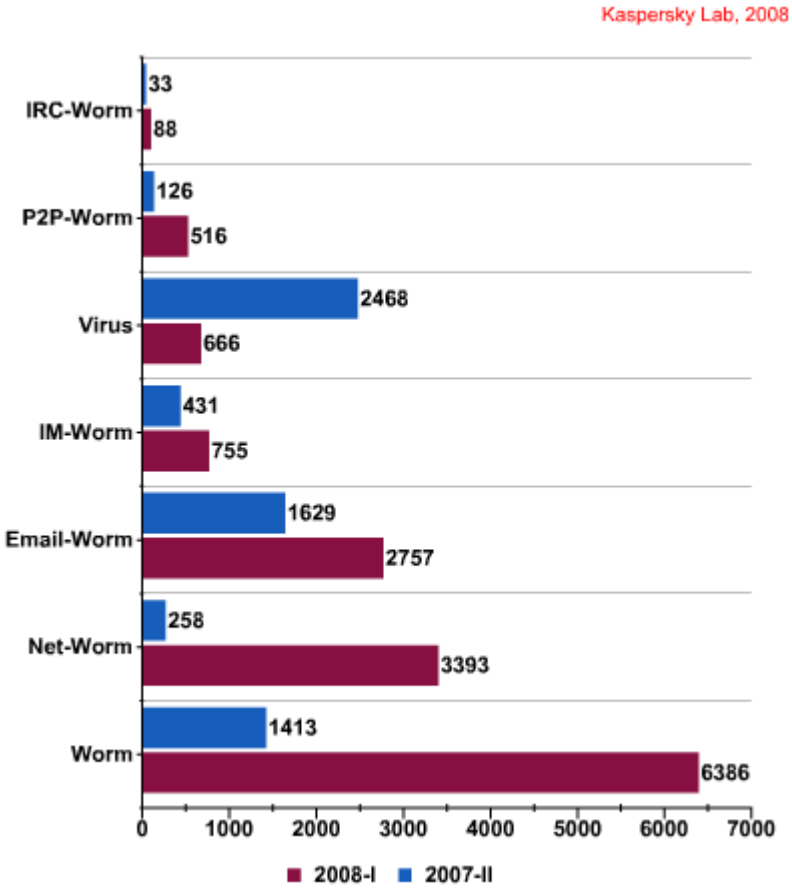
Se una dinamica simile sarà confermata anche nel secondo semestre del 2008, allora non è escluso lo slittamento di questa classe al terzo posto ed il piazzamento, al secondo, del gruppo Other Malware.

Proprio all'interno della classe VirWare in metà anno sono avvenuti cambiamenti abbastanza significativi. Ecco la ripartizione delle quote dei comportamenti del VirWare:

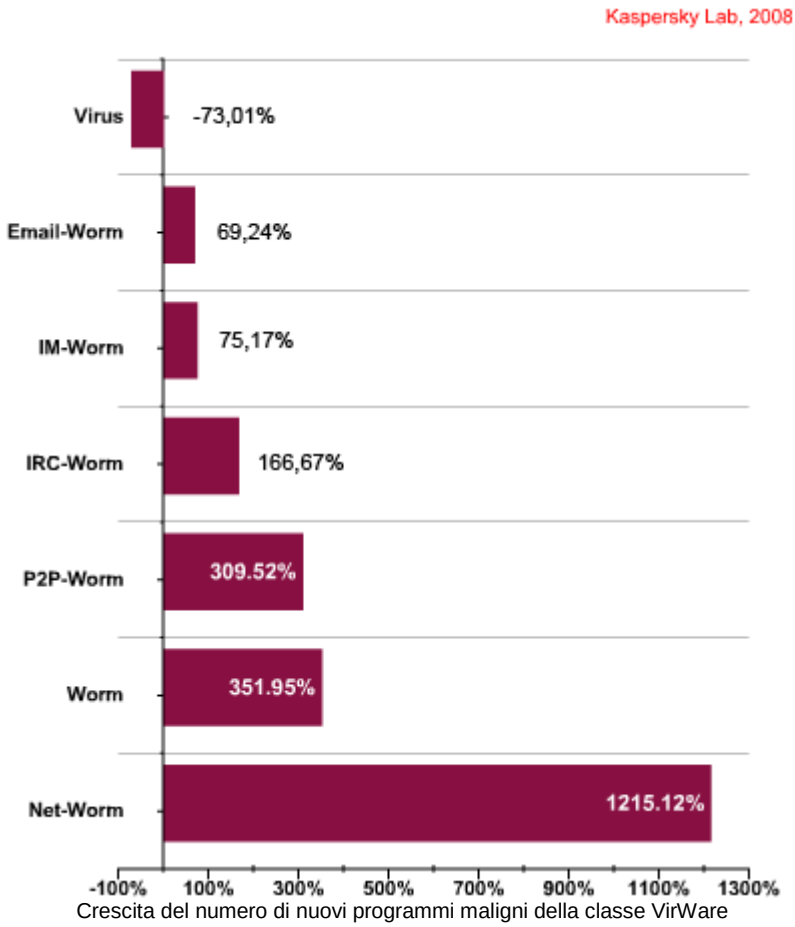


VirWare: rapporto percentuale dei comportamenti all'interno della classe

Per capire meglio i cambiamenti avvenuti nella classe dei malware ad auto-diffusione, esaminiamo come è aumentato il numero dei malware di diversa natura (per comportamento).



Quantità di nuovi codici maligni della classe VirWare (per comportamento)



Crescita del numero di nuovi programmi maligni della classe VirWare

VirWare	Totale 2008	2007-2	Crescita	2008%	"+/-"
Worm	6386	1413	351,95%	43,857	21,63%
Net-Worm	3393	258	1215,12%	23,302	19,24%
Email-Worm	2757	1629	69,24%	18,934	-6,69%
IM-Worm	755	431	75,17%	5,185	-1,59%
Virus	666	2468	-73,01%	4,574	-34,24%
P2P-Worm	516	126	309,52%	3,544	1,56%
IRC-Worm	88	33	166,67%	0,604	0,09%
Totale	14561	6358	129,02%	100	

Le principali metamorfosi nella classe VirWare si sono verificate con i classici virus di file. È difficile da spiegare ciò che è successo loro nel primo semestre del 2008. I virus nel 2007 erano primi assoluti per ritmo di crescita (390%) fra tutti i programmi maligni, ed hanno completato il semestre precedente raggiungendo il primo posto fra i VirWare con un indice del tutto ragguardevole, pari al 38,8%. Nel primo semestre del 2008 i virus hanno invece mostrato dei ritmi di crescita negativi

(-73%) e nei risultati semestrali la loro quota è stata solo di poco superiore al 4,5%.

Ci eravamo aspettati un aumento graduale del numero dei virus più complessi ed uno sviluppo ulteriore delle tecnologie polimorfe. Ma, a quanto pare, i criminali informatici si sono appassionati al «processo di creazione di nuovi Trojan» e non possiedono sufficienti conoscenze tecniche per implementare le tecnologie di virus. Per l'industria anti-virus, questo è senz'altro un buon segno.

Sono stati i worm di rete ad aver registrato la crescita più rapida durante i primi 6 mesi dell'anno, un ritmo di crescita pari

al 352% ha portato al raddoppiamento della loro quota all'interno del VirWare, ed ha loro permesso di raggiungere il primo posto con un risultato vicino al 44%. Proprio da Worm simili, che si diffondono tramite i dischi rimovibili e le reti locali, è più difficile ripulire i computer degli utenti.

Nel primo semestre del 2008 i worm di rete sono quelli che hanno manifestato la crescita più rapida, una crescita senza precedenti, pari al 1200% (!), e maggiore rispetto al semestre precedente. Il comportamento, che era praticamente sparito del tutto nel 2007, improvvisamente si è posizionato al secondo posto. La ragione di una crescita così rapida evidentemente si trova nel successivo sviluppo dei worm di tipo ordinario, i quali si stanno collocando sulla spirale evolutiva successiva. I loro autori cercano di prendere dimestichezza con i nuovi metodi di diffusione e cominciano ad usare i vecchi metodi ma già ad un livello più elevato. Ad esempio, in condizione di assenza di vulnerabilità critiche, che erano la base funzionale di tali worm in passato, i moderni worm di rete Lovesan e Sasser sempre più spesso usano, per la loro diffusione, i siti web forzati e i social networks.

Nel corso degli ultimi anni la crescita stabile del numero di Worm di posta elettronica è continuata anche nel 2008, però non è stata sufficiente per assicurare a loro il secondo posto. Nel primo semestre del 2008 la quota dei worm di posta elettronica si è ridotta del 6,7% ed essi sono andati ad occupare il terzo posto con un indice del 19%. Nonostante ciò, questo significa che dei nuovi rappresentanti della classe VirWare uno su cinque è un Worm che si diffonde tramite posta elettronica. La crescita del numero di tali Worm continua principalmente grazie a tre famiglie: Warezov, Zhelatin e Bagle. Così è stato anche nel 2007.

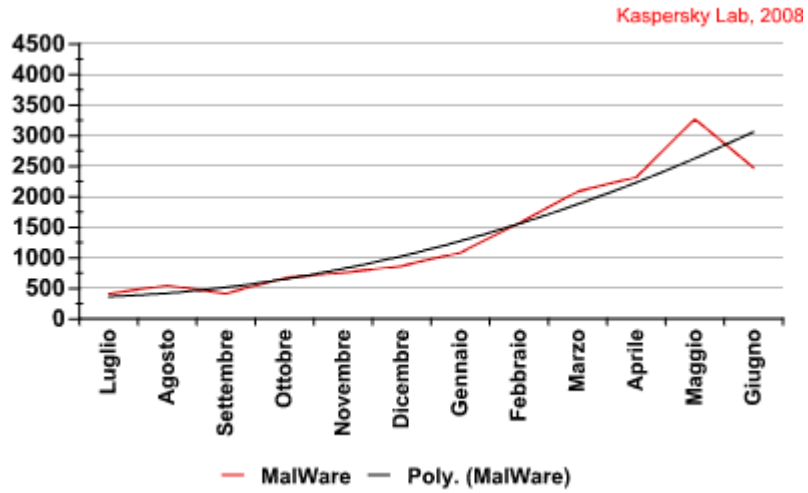
Nella categoria VirWare si possono evidenziare due principali gruppi di comportamento:

1. Email-Worm, Worm, Net-Worm. Ognuno di questi comportamenti supera del 18% il numero complessivo di VirWare. Si osservano una stagnazione dello sviluppo dell'ex-leader (E-mail-Worm) e indici esplosivi di crescita delle categorie Worm e Net-Worm.
2. IM-Worm, Virus, P2P-Worm, IRC-Worm. La quota di ognuno dei comportamenti nel numero complessivo di VirWare è inferiore al 6%. I ritmi di crescita si differenziano fortemente: da tassi negativi fino a tassi paragonabili con quelli dei leader (oltre il 300%). Tuttavia, la probabilità di un significativo aumento di quota esiste solo per la categoria Virus: i restanti comportamenti dipendono dai servizi Internet secondari (IM, IRC, P2P).

Other Malware

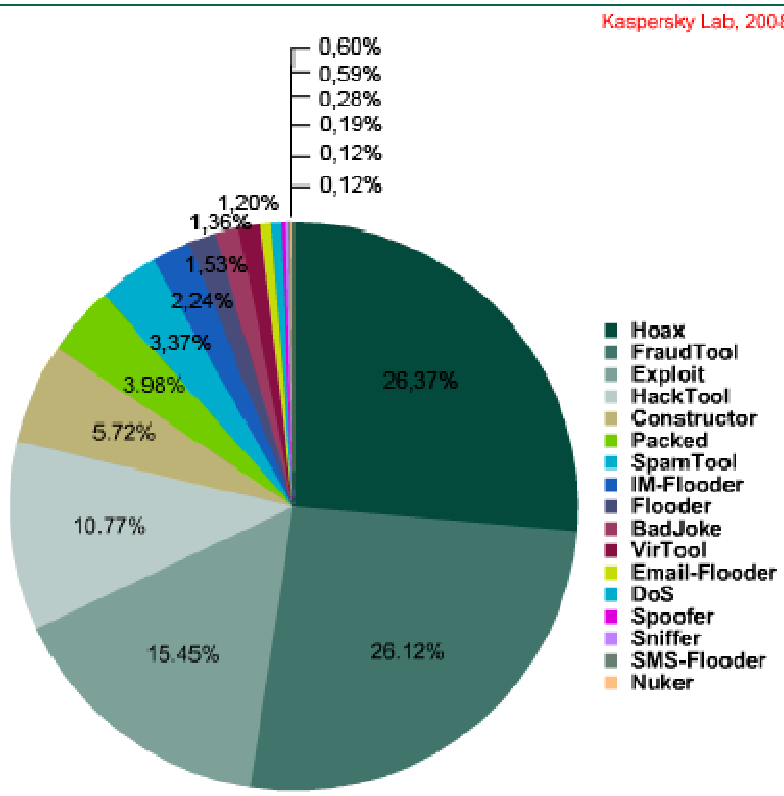
Questa classe appare sempre più spesso come la meno diffusa per quantità di malware rilevati, ma la più numerosa per numero di comportamenti.

È molto difficile fare pronostici riguardo il numero di malware della classe Other MalWare: la loro dinamica numerica è caratterizzata da un periodo di crescita debole negli anni 2004-2005, un leggero calo nel 2006 e da una crescita del 27% secondo i risultati del 2007. Ma il primo semestre del 2008 è risultato più che proficuo per Other MalWare: sono stati riscontrati nuovi programmi maligni di questa categoria per il 249,3% in più rispetto al semestre precedente.



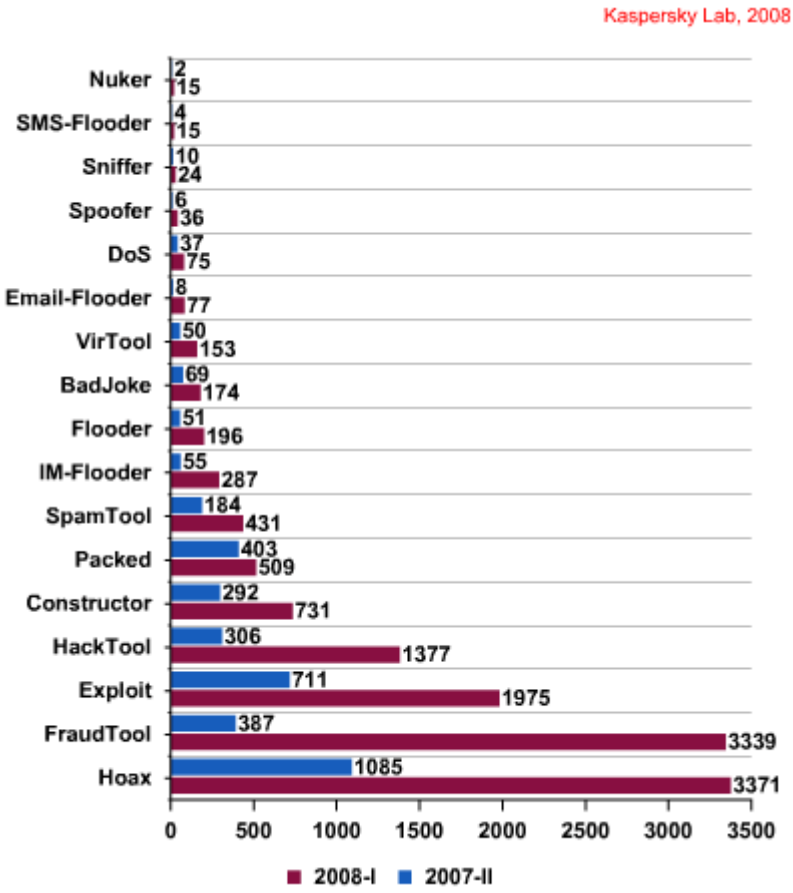
Numero dei programmi della categoria Other Malware, riscontrati dagli analisti di Kaspersky Lab (luglio 2007 – giugno 2008)

La distribuzione del comportamento di Other MalWare può essere rappresentata dal seguente diagramma circolare:

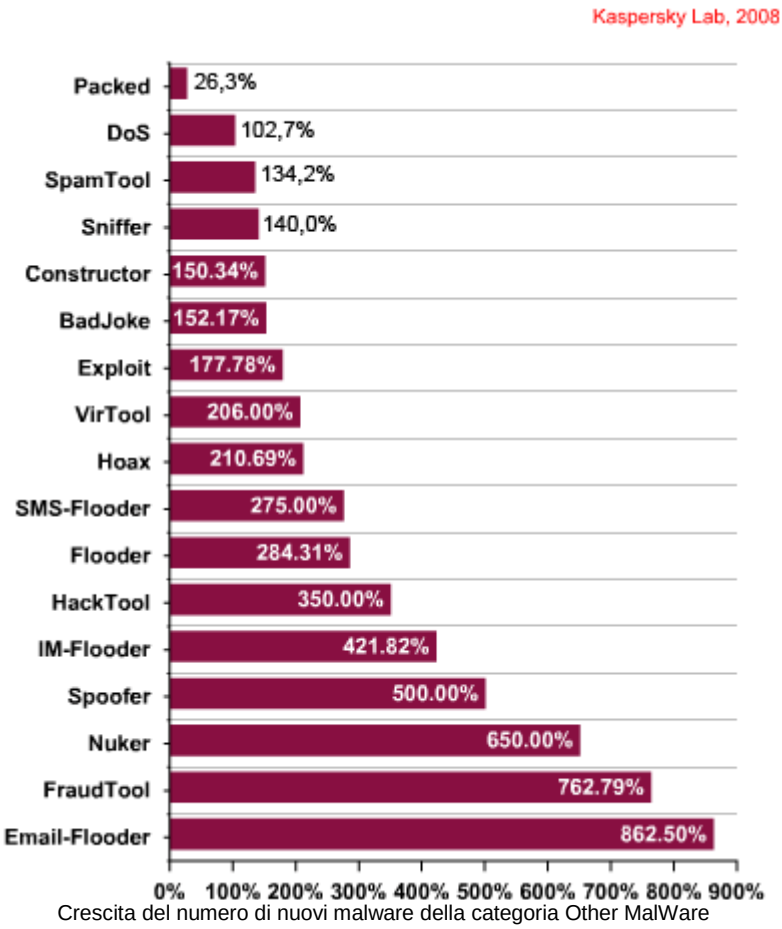


Other MalWare: rapporto in percentuale dei comportamenti all'interno della categoria

Per capire meglio le modifiche verificatesi in questa classe di malware, esaminiamo in quale modo in questa categoria aumentava il numero di malware di diverso comportamento:



Numero dei nuovi programmi della classe Other MalWare (per comportamento)



Crescita del numero di nuovi malware della categoria Other MalWare

MalWare	Totale 2008	2007-2	Crescita	2008%	"+/-"
Hoax	3371	1085	210,69%	26,367	-3,28%
FraudTool	3339	387	762,79%	26,117	15,54%
Exploit	1975	711	177,78%	15,448	-3,98%
HackTool	1377	306	350,00%	10,77	2,41%
Constructor	731	292	150,34%	5,718	-2,26%
Packed	509	403	26,30%	3,981	-7,03%
SpamTool	431	184	134,24%	3,371	-1,66%
IM-Flooder	287	55	421,82%	2,245	0,74%
Flooder	196	51	284,31%	1,533	0,14%
BadJoke	174	69	152,17%	1,361	-0,52%
VirTool	153	50	206,00%	1,197	-0,17%
Email-Flooder	77	8	862,50%	0,602	0,38%
DoS	75	37	102,70%	0,587	-0,42%
Spoofer	36	6	500,00%	0,282	0,12%
Sniffer	24	10	140,00%	0,188	-0,09%
SMS-Flooder	15	4	275,00%	0,117	0,01%
Nuker	15	2	650,00%	0,117	0,06%

Totale	12785	3660	249,32%	100%	

Il gruppo degli Hoax continua a rimanere il comportamento più diffuso in questa classe. Per il terzo anno successivo essi dimostrano una crescita veramente esplosiva: dal 150% fino al 286%. Tuttavia, osservando i risultati dei primi sei mesi del 2008, notiamo come la loro quota fra i tutti programmi di OtherMalware sia diminuita più del 3%.

Gli Exploit, precedenti leader per numero, continuano a perdere posizioni. Malgrado la crescita del 178%, essi non sono riusciti a mantenere il secondo posto. Attualmente occupano il terzo posto per popolarità, e costituiscono solo il 15,5% del numero complessivo di OtherMalware.

Due nuovi comportamenti sono comparsi nella nostra classifica solo nel 2007: Packed e FraudTool, i quali si comportano in modo diverso.

La significativa crescita che i Packed hanno mostrato lo scorso anno, nel primo semestre del 2008 si è praticamente fermata (26%). Questo ha portato ad una diminuzione della quota dei Packed fra tutti i programmi della classe Other Malware di oltre il 7%.

D'altro canto, i gruppi leader sono diventati FraudTool e Hoax, che sono cresciuti ben del 760%. La popolarità di questo comportamento di programmi maligni continua a crescere fra i virus writer. La versione principale del programma FraudTool è costituita dai cosiddetti programmi “rogue-antivirus”, che si spacciano per soluzioni anti-virus. Dopo che sono stati installati sul computer, essi «trovano» necessariamente un virus qualsiasi anche su di un sistema assolutamente pulito e propongono di comperare la loro versione di programma a pagamento, se si vuole disinfettare il proprio computer. Oltre alla frode diretta degli utenti, questi programmi hanno anche, al loro interno, funzionalità di adware.

Programmi potenzialmente indesiderati (PUPs)

L'anno scorso abbiamo iniziato ad includere nelle nostre relazioni i programmi potenzialmente indesiderati (Potentially Unwanted Programs, o PUPs). Questi, che si sviluppano e diffondono tramite ditte legali, hanno però un assortimento di funzioni che permettono ai malintenzionati di impiegarli a danno degli utenti. È impossibile attribuire tali programmi in modo univoco alle macrocategorie dei programmi pericolosi o innocui: tutto dipende dalle mani in cui essi si trovano.

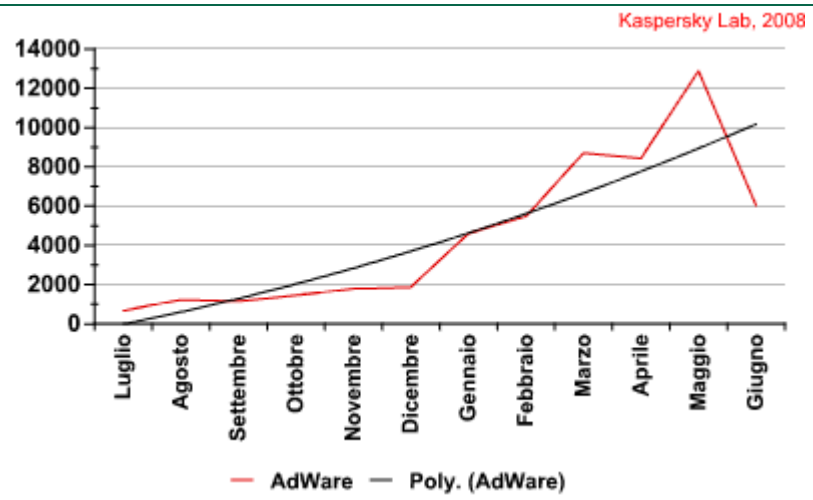
Secondo la classifica di Kaspersky Lab, dei programmi potenzialmente indesiderati entrano a far parte tre classi di programmi.

1. AdWare: è un software destinato a mostrare comunicazioni pubblicitarie, oppure destinato a inviare richieste fatte durante la navigazione verso pagine web pubblicitarie. L'adware è destinato anche alla raccolta di dati riguardanti l'utente, necessari a scopi di marketing (ad ex., siti visitati e quali le tematiche predilette).
2. RiskWare: programmi legali che i malintenzionati possono usare a danno dell'utente e dei suoi dati, eliminandone, bloccandone, modificandone oppure copiandone l'informazione, alterando il funzionamento del computer o delle reti di computer.
3. PornWare: utility collegate, in un modo o nell'altro, con la pornografia (a questa classe vengono attribuiti solo tre comportamenti: -Porn-Tool, Porn-Dialer e Porn-Downloader).

Adware

È la classe di PUPs più stabile per il secondo anno di fila: l'AdWare possiede indici di crescita di oltre il 450%. Il numero mensile medio dei nuovi campioni già si avvicina alle 8000 unità, il che ha posizionato i programmi pubblicitari al secondo posto tra quelli rilevabili dal nostro programma anti-virus.

Osserviamo il diagramma del numero di nuovi programmi AdWare rilevati ogni mese da parte degli analisti di Kaspersky Lab:



Numero di nuovi programmi della classe AdWare (luglio 2007 – giugno 2008)

AdWare	Totale 2008	2007-2	Crescita
AdWare	46134	8168	464,81%

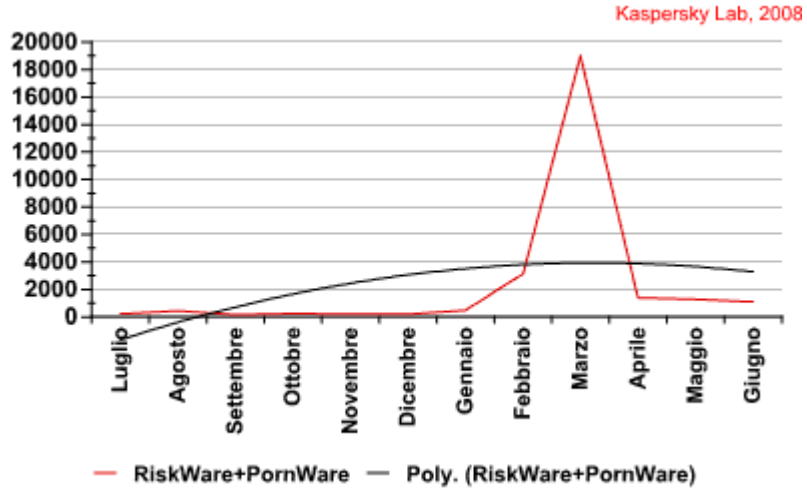
Il diagramma mostra come nei primi mesi del 2008 si sia registrato un picco di simili programmi. Ancora una volta dobbiamo a malincuore riconoscere il totale insuccesso degli sforzi profusi dalle autorità legislative di molti paesi del mondo, che dovrebbero proibire simili programmi e semmai ricondurli su di una via più «legale». Certamente, molti creatori di AdWare hanno modificato alcune delle funzioni ed il comportamento dei loro elaborati: ne deriva, in particolare, una crescita nel numero di programmi AdTool, della quale parleremo in seguito. Questo, purtroppo, evidentemente non è sufficiente ad aiutare gli utenti a liberarsi dalla pubblicità invadente.

La cosa ancora più scocciante, è che tanti programmi pubblicitari acquisiscono vere funzioni tipiche dei Trojan, ed arrivano ad usare le tecnologie rootkit per nascondersi all'interno del sistema. Un esempio emblematico è Virtumonde. Qualche anno fa questo programma era un «comunissimo» AdWare, ma attualmente viene da noi classificato come Trojan, poiché per diffonderlo i suoi gli autori usano i metodi più «sporchi ».

RiskWare e PornWare

Poiché esistono solo tre programmi di comportamento PornWare e la percentuale dei nuovi programmi di questa classe, rilevati dagli analisti di Kaspersky Lab nel primo semestre del 2008 rappresenta l'11,7% di tutti programmi potenzialmente indesiderati, nel corso delle analisi abbiamo riunito i programmi di questa classe con i programmi del gruppo RiskWare.

Rappresentiamo in un diagramma la quantità di nuovi programmi RiskWare e PornWare rilevati, mese dopo mese, dagli analisti di Kaspersky Lab:



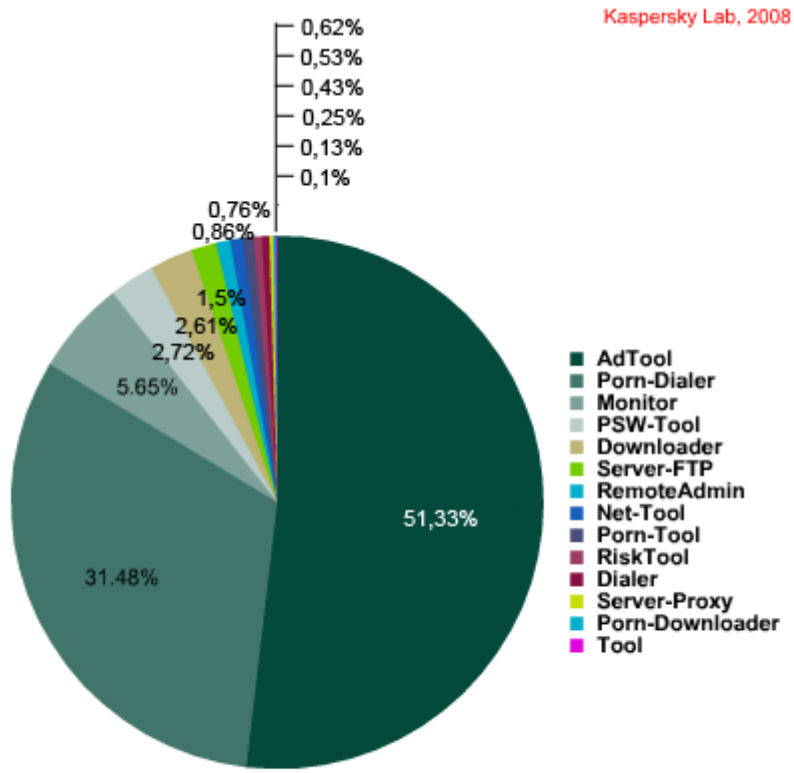
Numero dei nuovi programmi delle classi RiskWare e PornWare (luglio 2007 – giugno 2008)

Nel 2008 il numero dei programmi di tipo Riskware e PornWare rilevati da Kaspersky Lab ha superato la cifra di 26000 unità, e la crescita complessiva del numero dei programmi delle due classi ha superato il 1700%.

Questo è successo per il fatto che alla banca dati anti-virus sono state aggiunte alcune migliaia di programmi classificabili come AdTool. Nel diagramma si vede chiaramente questo picco nel mese di marzo. Successivamente, la statistica delle classi RiskWare e PornWare si è stabilizzata e ha cominciato ad essere conforme alle aspettative.

La ripartizione dei programmi delle classi RiskWare e PornWare secondo i comportamenti, può essere rappresentata nella forma del seguente diagramma circolare:

Numero dei nuovi programmi delle classi RiskWare e PornWare (per comportamento):



Distribuzione di RiskWare e PornWare per comportamento

RiskWare&PornWare	Totale 2008	2007-2	Crescita	2008%	"+/-"
AdTool	13555	50	27010,00%	51,33	47,90%
Porn-Dialer	8311	130	6293,08%	31,48	22,60%
Monitor	1491	611	144,03%	5,65	-36,20%
PSW-Tool	719	131	448,85%	2,72	-6,20%
Downloader	688	104	561,54%	2,61	-4,50%
Server-FTP	396	36	1000,00%	1,5	-1,00%
Прочие	246	47	423,40%	0,93	-2,30%
RemoteAdmin	228	107	113,08%	0,86	-6,50%
Net-Tool	200	73	173,97%	0,76	-4,20%
Porn-Tool	165	13	1169,23%	0,62	-0,30%
RiskTool	139	51	172,55%	0,53	-3,00%

Dialer	113	46	145,65%	0,43	-2,70%
Server-Proxy	67	17	294,12%	0,25	-0,90%
Porn-Downloader	35	15	133,33%	0,13	-0,90%
Tool	26	15	73,33%	0,1	-0,90%
Client-IRC	11	7	57,14%	0,04	-0,40%
Server-Web	7	5	40,00%	0,03	-0,30%
Server-Telnet	5	0		0,02	
WebToolbar	2	0		0,01	
Client-SMTP	1	2	-50,00%	0	-0,10%
Totale	26405	1460	1708,56%	100%	

Fra i comportamenti facenti parte di queste due classi, si evidenziano chiaramente due leader: AdTool (51,33%) e Porn-Dialer (31,48%).

AdTool rappresenta vari moduli pubblicitari che non si possono attribuire ad AdWare perché dotati dei necessari attributi legali, forniti del contratto di licenza d'uso e mostrano la loro presenza sul computer informando l'utente riguardo le loro azioni. La leadership di AdTool era abbastanza prevedibile, tenendo conto del numero di programmi aggiunti simultaneamente nei database anti-virus di questo comportamento (vedi sopra).

Porn-Dialers effettua collegamenti telefonici con i numeri brevi del servizio SMS Premium, cosa che molto spesso porta a procedimenti giudiziari fra gli abbonati e i gestori telefonici.

I programmi del comportamento leader nel 2007, il Monitor, hanno diminuito in modo significativo i propri indici. Di Monitor fanno parte anche i legali keyboard logger, che vengono prodotti e venduti in modo ufficiale ma, qualora siano dotati di funzioni di occultamento della loro presenza nel sistema, possono venire usati come validissimi Trojan. Durante i primi 6 mesi del 2008 hanno perso oltre il 35% andando ad occupare solo il terzo posto fra i tutti programmi potenzialmente indesiderati.

Come prima, sono ancora comportamenti comuni PSW-Tool e Downloader. I primi sono destinati al recupero delle password dimenticate, ma possono facilmente essere usati dai malintenzionati per l'estrazione di tali password dal computer della vittima che non sospetta nulla. I secondi possono venire impiegati dai malintenzionati per scaricare un contenuto maligno sul computer della vittima.

È necessario notare che vi è stata anche una significativa diminuzione della quota dei programmi di comportamento RemoteAdmin (-6,5%).

Piattaforme e sistemi operativi

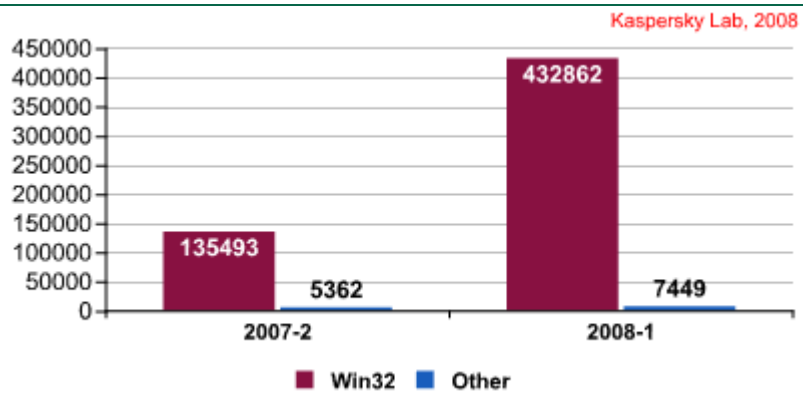
Per la prima volta lo scorso anno abbiamo pubblicato una statistica dettagliata della distribuzione del malware e dei programmi potenzialmente indesiderati secondo i sistemi operativi e le piattaforme.

Il sistema operativo o un'applicazione possono essere attaccati dal malware nei casi in cui esso ha la possibilità di avviare un programma che non fa parte del sistema. Questo è possibile per tutti i sistemi operativi, molte applicazioni di office, programmi di grafica ed elaborazione di immagini, i sistemi CAD/CAM ed altri pacchetti che hanno linguaggi di scripting incorporati.

Nei soli primi sei mesi del 2008 da parte di Kaspersky Lab sono stati registrati programmi di malware e programmi potenzialmente indesiderati per ben 41 diverse piattaforme e sistemi operativi.

Non desta sorpresa che la stragrande maggioranza di tali programmi sia stata progettata per funzionare in ambiente Win32, e che si tratti di file eseguibili binari. Tali programmi costituiscono il 98,31% del totale.

I programmi orientati verso altri sistemi operativi o piattaforme incidono per meno del 2% di tutti i programmi esaminati. Nel primo semestre del 2008 il numero di malware e Win32 è cresciuto del 233% rispetto agli ultimi sei mesi del 2007. Per altre piattaforme ed allegati questa crescita è stata pari solo al 39%, il che è meno dell'indice del 2007 (63%). Così non si è verificato il previsto spostamento degli interessi dei virus writer da Win32 verso altre piattaforme. Al contrario, osserviamo non solo come la precedente crescita del numero di minacce «non-Windows» sia cessata, ma che il numero di tali minacce ha cominciato a diminuire (ricordiamo, che nel secondo semestre del 2007 la loro quota incideva del 4% di tutte le minacce.)



Numero dei nuovi programmi malware e programmi potenzialmente indesiderati, suddivisi per piattaforme

	2007-2	2008-1	Crescita	2007%	2008%	"+/-"
Win32	130131	432862	232,60%	96,00%	98,30%	-2,27
Прочие	5362	7449	38,90%	4,00%	1,70%	2,27
Totale	135493	440311	225,00%			

	I 2008	II 2007	Crescita
Acad	6	5	20%
ALS	1	3	-67%
ASP	39	135	-71%
BAT	765	553	38%
DOS	45	44	2%
HTML	1103	930	19%
HWP	1	0	0%
Ichitaro	1	0	0%
IIS	1	0	0%
IRC	51	86	-41%
J2ME	41	6	583%
Java	17	25	-32%
JS	3311	2240	48%
Linux	28	45	-38%
Mac	14	33	-58%
MSAccess	14	4	250%
MSExcel	94	10	840%
MSIL	327	31	955%
MSOffice	7	3	133%
MSPPoint	42	16	163%
MSWord	135	83	63%
Multi	4	11	-64%

MySQL	1	0	0%
NSIS	27	17	59%
OLE2	1	0	0%
OSX	6	0	0%
Perl	39	37	5%
PHP	155	186	-17%
Python	10	9	11%
RAR	7	12	-42%
Ruby	3	5	-40%
Shell	5	0	0%
SWF	260	3	8567%
SymbOS	34	30	13%
VBS	820	748	10%
Win16	6	7	-14%
Win32	432862	130131	233%
Win9x	5	3	67%
WinCE	3	0	0%
WinREG	15	39	-62%
WMA	5	3	67%
Totale	440311	135493	225%

È evidente che la crescita del numero di nuovi programmi per i vari sistemi operativi e piattaforme è abbastanza differente. Le variazioni più significative verificatesi durante questo semestre sono le seguenti:

Linguaggi script VBS e JS, che lo scorso anno facevano parte del gruppo leader, significativamente hanno rallentato il proprio sviluppo come piattaforma per la diffusione dei virus.
Il numero di programmi maligni per la piattaforma J2ME è cresciuto del 583%. Abbiamo già notato l'aumento del numero di Trojan-SMS, la maggior parte dei quali funziona proprio su questa piattaforma.
Il numero dei malware realizzati come file XLS e che usano, come regola, le vulnerabilità in MS Excel è cresciuto dell'840%. Durante l'ultimo anno è stata rilevata qualche decina di simili vulnerabilità, e tutte sono diventate oggetto di un più largo uso da parte dei virus writer, in primis di quelli cinesi.
Il numero di programmi scritti per la piattaforma .NET è cresciuto del 955%. Questo è un fatto che ci aspettavamo ormai da tempo, ed il 2008 ha mostrato l'inizio di questo processo. In prospettiva ci attendiamo, che questa piattaforma possa diventare la seconda per popolarità, superando fortemente Java Script. Una particolarità aggiuntiva del .NET, che interessa i virus writer, è la possibilità di eseguire i file non solo su computer con SO Windows, ma anche sulla piattaforma mobile di Windows Mobile.
Il numero di codici maligni realizzati come file SWF è cresciuto di oltre l'8500%! Il motivo di tale crescita è stato il riscontro di una vulnerabilità estremamente pericolosa nella gestione di simili file. Il sottobosco della criminalità informatica ha reagito immediatamente ed ha usato SWF come un nuovo metodo per recapitare il malware ai computer degli utenti. Così, nella primavera di quest'anno, in Internet sono comparse oltre duecento cinquanta versioni di file maligni SWF.

Raggruppiamo tutti i sistemi operativi e le piattaforme attaccate nel primo semestre del 2008 secondo una caratteristica comune, e cioè secondo il sistema operativo finale. Per esempio, JS e VBS li aggreghiamo a Windows, ma Ruby e Perl a *nix ecc.

Quindi, di *Nix faranno parte Linux, Perl, PHP, Ruby e Shell;
di Mobile - J2ME, Symbian, WinCE e Python;
degli «altri» - DOS, IIS, Multi e MySQL;
del Mac – OSX e Mac.

	Q-tà	%
Nix	230	0,052
Mac	20	0,005
Mobile	88	0,02
Прочие	51	0,012
Windows	439922	99,912

Conclusioni

L'evoluzione delle minacce nella prima metà del 2008 ha seguito le tendenze del 2007: i virus writer continuano ad impiegare tecnologie non sofisticate, preferendo affidarsi alla quantità piuttosto che alla qualità dei programmi maligni.

Il numero delle nuove minacce segue una progressione geometrica. Questo processo è accompagnato da una riduzione della durata di vita media delle minacce rilevate “in the wild”. Su 1000 nuovi Trojan identificati ogni giorno, solo alcune decine continuano a rappresentare una minaccia per gli utenti una settimana o un mese più tardi. Tutti gli altri spariscono poco a poco e vengono sostituiti da nuove versioni, create per eludere la “sorveglianza anti-virus”.

Comunque, crediamo che questa crescita nel numero dei nuovi programmi maligni debba presto arrestarsi, probabilmente entro l'anno. I volumi ottenuti (circa 500.000 nuovi programmi maligni nell'arco di 6 mesi) saranno confermati, ma la maggior parte delle società anti-virus sarà in grado di venirne a capo.

Oggi, l'industria anti-virus deve risolvere problemi diversi da quelli di un tempo, nello specifico, è indispensabile che gli sforzi vengano concentrati nell'elaborazione di strumenti che consentano un'identificazione precoce delle minacce. Se in passato era sufficiente reagire alle minacce in un tempo di poche ore (o a volte pochi giorni), ora è indispensabile fare ciò in pochi minuti. Ciò significa che gli esperti di anti-virus devono identificare i nuovi programmi maligni in Internet (quindi in qualsiasi punto del pianeta essi siano collocati), analizzarli, produrre gli strumenti necessari di protezione e consegnarli all'utente finale il prima possibile.