Report sullo stato della protezione Microsoft
Volume 8 (luglio - dicembre 2009)

Riepilogo dei principali risultati

Introduzione

Il volume 8 del *Report sullo stato della protezione Microsoft®* fornisce una descrizione dettagliata delle situazioni legate a software dannoso e potenzialmente indesiderato, exploit software, violazioni della sicurezza e vulnerabilità software, sia in prodotti Microsoft che di terze parti. Le conclusioni di Microsoft si basano sull'analisi dettagliata degli ultimi anni, con una particolare attenzione al secondo semestre 2009[1].

Questo documento è un riepilogo dei risultati più rilevanti contenuti nel report. La versione integrale del *Report sullo stato della protezione* contiene inoltre un'analisi dettagliata delle tendenze osservate in oltre 26 paesi/aree geografiche in tutto il mondo con le strategie, i metodi di attenuazione dei rischi e le contromisure che è possibile adottare per gestire le minacce documentate nel report.

È possibile scaricare la versione integrale del *Report sullo stato della protezione*, i volumi precedenti del report e i video correlati dal sito www.microsoft.com/sir.

Il panorama delle minacce informatiche è in costante evoluzione. Di pari passo con l'evoluzione da singoli pirati informatici alla ricerca di notorietà a criminali organizzati che sottraggono dati per un ritorno economico, la preoccupazione dell'opinione pubblica continua a crescere. Microsoft ha creato il Trustworthy Computing (TwC) nel 2002 con l'obiettivo di definire una strategia in grado di garantire ai clienti una maggiore sicurezza, riservatezza e affidabilità nell'utilizzo del computer.

La divisione TwC Security comprende tre centri tecnologici che collaborano a stretto contatto per gestire i problemi legati alla sicurezza e offrire i servizi, le informazioni e le risposte necessari per assicurare una migliore comprensione del mutevole panorama delle minacce, garantire la protezione dei clienti dalle minacce online e condividere informazioni con il più vasto ecosistema correlato alla sicurezza. I tre centri per la sicurezza sono:

- Microsoft Malware Protection Center
- Microsoft Security Response Center
- Microsoft Security Engineering Center

I blog di questi tre centri per la sicurezza e altri blog, come il blog Data Privacy Imperative, sono disponibili sul sito Web www.microsoft.com/twc/blogs.

I dati e l'analisi illustrati in questo *Riepilogo dei risultati principali* e nella versione integrale del *Report sullo stato della protezione* vengono presentati dal punto di vista di questi tre centri e dei relativi partner nei diversi gruppi di prodotti Microsoft.

[1] La denominazione utilizzata nel report per fare riferimento ai diversi periodi presi in considerazione è nsemAA, dove nsem si riferisce al primo (1) o al secondo (2) semestre dell'anno e AA all'anno. Ad esempio, 2°sem09 indica il secondo semestre del 2009 (dal 1° luglio al 31 dicembre), mentre 2°sem08 indica il secondo semestre del 2008 (dal 1° luglio al 31 dicembre).

Risultati principali del Microsoft Malware Protection Center

Tendenze globali del software dannoso e del software potenzialmente indesiderato

I prodotti per la sicurezza Microsoft raccolgono, con il consenso dell'utente, dati inviati da oltre 500 centinaia di milioni di computer in tutto il mondo e da alcuni dei più utilizzati servizi online di Internet. L'analisi di tali dati consente di ottenere un quadro completo e univoco sull'attività di malware e software potenzialmente indesiderato in tutto il mondo.

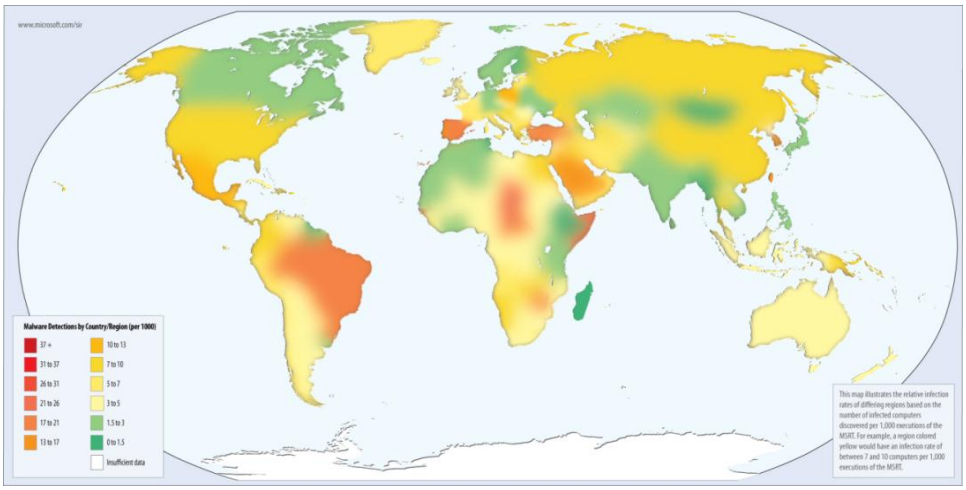
Tendenze geografiche

Figura 1: primi 15 paesi con il maggior numero di computer puliti con prodotti desktop antimalware Microsoft nel secondo semestre 2009 (la versione integrale del *SIR* include i primi 25 paesi)

	Paese/Regione	Computer puliti (2°sem09)	Computer puliti (1°sem09)	Modifica
1	Stati Uniti	15.383.476	13.971.056	10,1% ▲
2	Cina	3.333.368	2.799.456	19,1% ▲
3	Brasile	2.496.674	2.156.259	15,8% ▲
4	Regno Unito	2.016.132	2.043.431	-1,3% ▼
5	Spagna	1.650.440	1.853.234	-10,9% ▼
6	Francia	1.538.749	1.703.225	-9,7% ▼
7	Corea	1.367.266	1.619.135	-15,6% ▼
8	Germania	1.130.632	1.086.473	4,1% ▲
9	Canada	967.381	942.826	2,6% ▲
10	Italia	954.617	1.192.867	-20,0% ▼
11	Messico	915.786	957.697	-4,4% ▼
12	Turchia	857.463	1.161.133	-26,2% ▼
13	Russia	677.601	581.601	16,5% ▲
14	Taiwan	628.202	781.214	-19,6% ▼
15	Giappone	609.066	553.417	10,1% ▲
	nel mondo	41.024.375	39.328.515	4,3% ▲

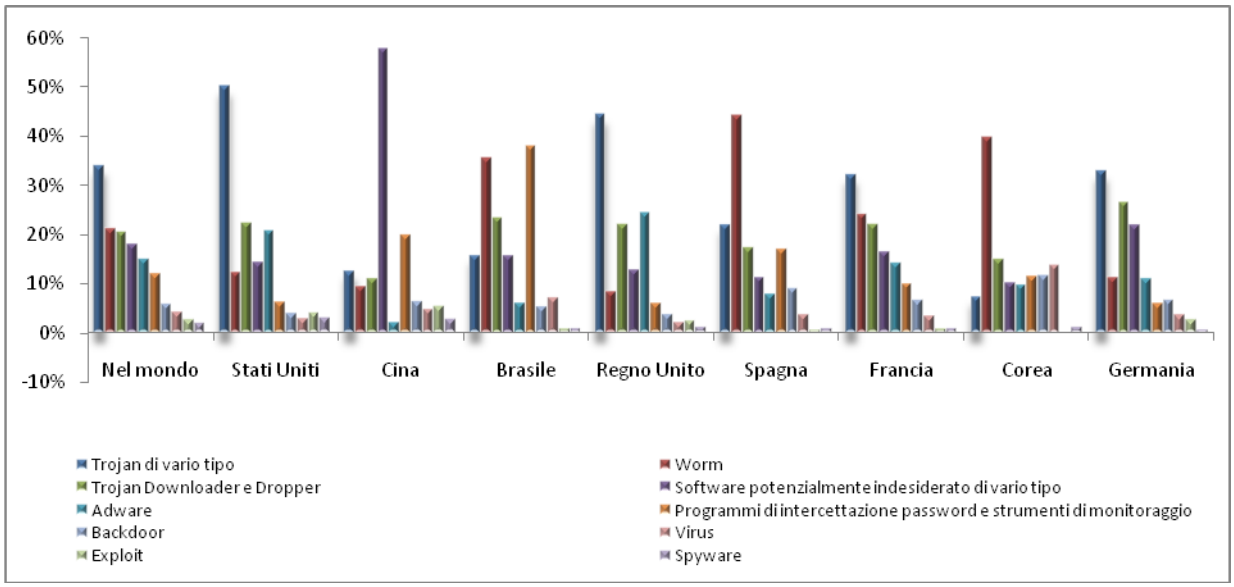
- Il maggiore incremento in termini di numero di computer puliti è stato osservato in Cina e in Brasile, che hanno registrato rispettivamente un aumento del 19,1% e del 15,8% rispetto al primo semestre 2009. Gran parte di questo aumento è stato causato dal rilascio a settembre 2009 di Microsoft Security Essentials, una soluzione antimalware per ambienti domestici, disponibile gratuitamente agli utenti di Microsoft Windows in possesso di licenza. Cina e Brasile sono stati i paesi che per primi hanno adottato Security Essentials.
- In una serie di aree è stata osservata una significativa riduzione dei tassi di infezione:
  - La più significativa riduzione in termini di numero di computer puliti è stata osservata in Turchia, dove si è registrata una riduzione del 26,2%, un risultato che può essere attribuito principalmente alla minore diffusione di Win32/Taterf e Win32/Frethog, due programmi di intercettazione password indirizzati contro i giocatori online.
  - La minore incidenza dei programmi Taterf e Frethog ha influito in modo evidente sulla riduzione della percentuale di computer puliti a Taiwan, dove è scesa al 19,6%.
  - La riduzione del 20% registrata in Italia rappresenta in larga misura il risultato di una drastica riduzione dei rilevamenti della famiglia di trojan horse Win32/Wintrim

Figura 2: tassi di infezione per paese/area geografica nel secondo semestre 2009, espressi in CCM[2], per le aree in tutto il mondo con almeno 1 milione di esecuzioni medie al mese di MSRT nel secondo semestre 2009



Nella versione integrale del *SIR* è disponibile il CCM relativo a oltre 200 paesi/aree geografiche.

Figura 3: categorie di minacce a livello mondiale e in otto aree con il numero maggiore di computer infetti, per incidenza su tutti i computer puliti tramite i prodotti desktop antimalware Microsoft, secondo semestre 2009



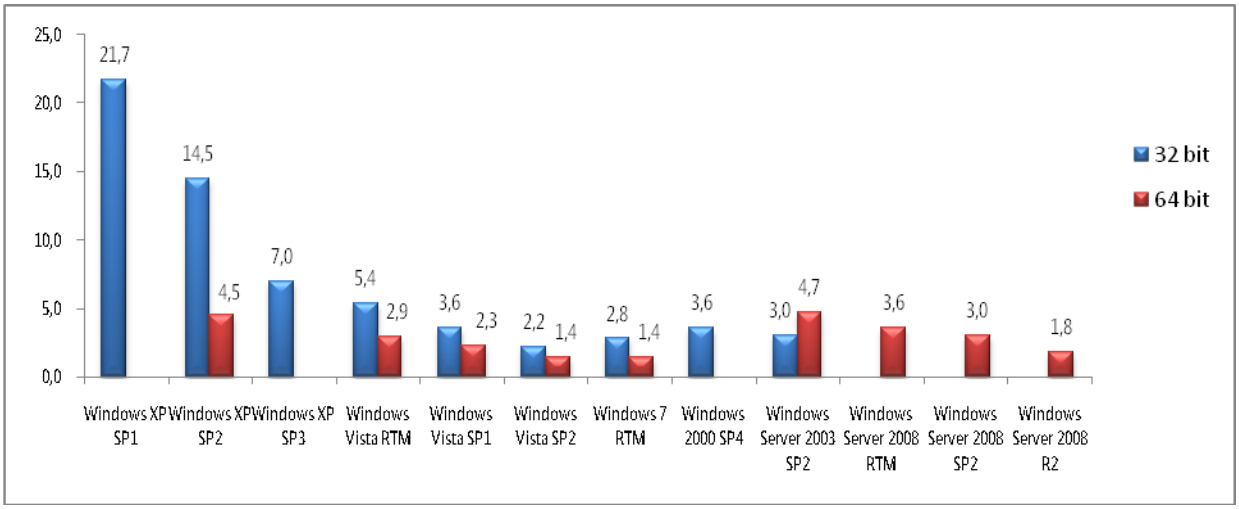
- Gli ambienti delle minacce negli Stati Uniti e nel Regno Unito sono molto simili. Entrambi i paesi presentano quasi la stessa proporzione di categorie di minacce e 7 delle prime 10 famiglie nelle due aree sono identiche. I trojan horse di vario tipo si sono confermati come la categoria più diffusa. Famiglie come Win32/FakeXPA, Win32/Renos e Win32/Alureon si presentano in percentuale elevata in entrambi i paesi.

[2] Per produrre una misurazione coerente delle infezioni da utilizzare per un confronto tra le popolazioni di computer in diverse aree geografiche, i tassi di infezione in questo report vengono espressi mediante una misura metrica denominata CCM (Computers Cleaned per Mille), che rappresenta il numero di computer puliti ogni 1.000 esecuzioni dello strumento MSRT. La lettera M in CCM è l'iniziale della parola latina mille.

- In Cina la maggior parte delle minacce più diffuse è rappresentata da famiglie localizzate, non presenti nell'elenco delle principali minacce degli altri paesi. Tali categorie includono alcune versioni di Win32/BaiduSobar, una barra degli strumenti di un browser in lingua cinese, e programmi di intercettazione password, come Win32/Lolyda e Win32/Ceekat, che prendono di mira diversi giochi online molto diffusi in Cina.
- In Brasile i programmi di intercettazione password e gli strumenti di monitoraggio rappresentano la categoria più diffusa, in larga misura a causa della prevalenza di una serie di programmi di intercettazione password in lingua portoghese indirizzati agli utenti online delle banche brasiliane. Win32/Bancos è il programma di intercettazione password più diffuso.
- In Corea hanno prevalso i worm, in particolare Win32/Taterf, minacce indirizzate ai giocatori online. La prevalenza di Taterf in Corea può dipendere in parte dalla tendenza del worm a diffondersi facilmente in Internet cafè e sale da gioco via LAN, molto diffusi in Corea.

Tendenze del sistema operativo

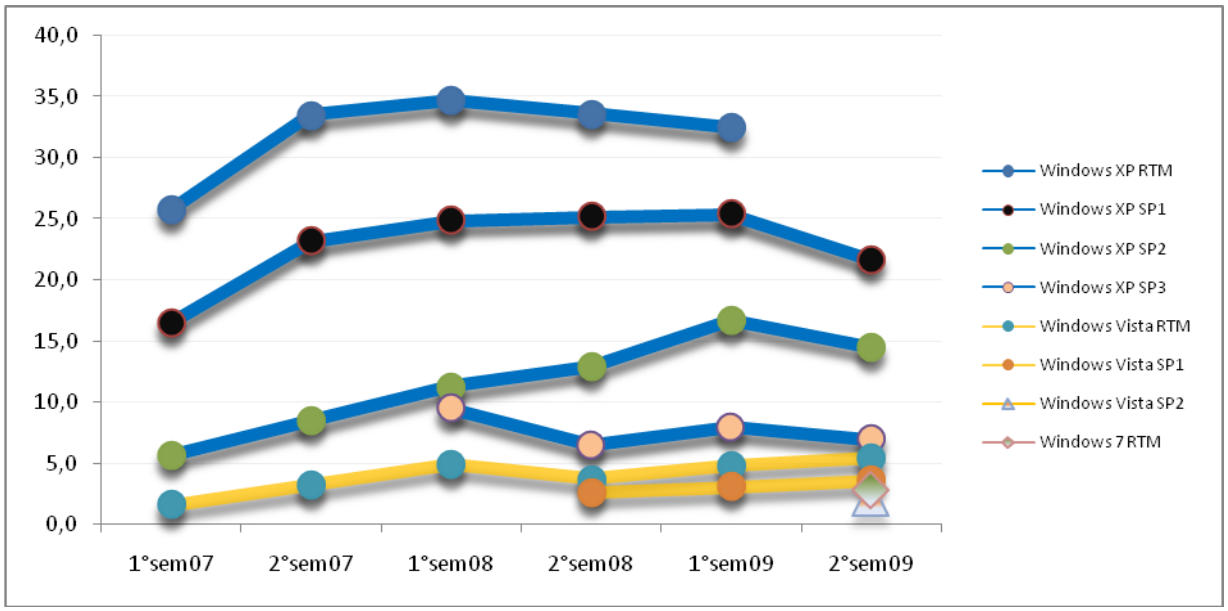
Figura 4: numero di computer puliti per ogni 1.000 esecuzioni di MSRT, per sistema operativo, secondo semestre 2009



- Come nei periodi precedenti, i tassi di infezione per i sistemi operativi e i Service Pack più recenti sono costantemente inferiori rispetto a quelli precedenti, sia per le piattaforme client che per le piattaforme server.
- Microsoft Windows 7, rilasciato nel secondo semestre del 2009, e Microsoft Windows Vista® con Service Pack 2 presentano i tassi di infezione più bassi rispetto a tutte le piattaforme illustrate nel grafico.
    - Le versioni a 64 bit di Microsoft Windows 7 e Windows Vista SP2 hanno registrato percentuali di infezione inferiori (1,4% per entrambi i sistemi) rispetto a tutte le altre configurazioni dei sistemi operativi nel secondo semestre del 2009, anche se nelle due versioni a 32 bit sono state riscontrate percentuali di infezione pari a meno della metà di quelle di Microsoft Windows XP con il Service Pack più aggiornato, SP3.
- Per i sistemi operativi con Service Pack, ogni Service Pack successivo presenta un tasso di infezione inferiore rispetto al precedente.
    - Il tasso di infezione per Microsoft Windows XP con SP3 è pari a meno della metà dei sistemi con SP2 e a meno di un terzo dei sistemi con SP1.
    - Analogamente, Microsoft Windows Vista SP2 presenta un tasso di infezione inferiore rispetto a SP1, che registra un tasso di infezione inferiore rispetto a Microsoft Windows Vista RTM.
    - Per i sistemi operativi server, il tasso di infezione per Microsoft Windows Server® 2008 con SP2 è pari a 3,0, ovvero il 20% in meno rispetto al suo predecessore, Microsoft Windows Server 2008 RTM.

La figura riportata di seguito evidenzia la coerenza di queste tendenze nel tempo, mostrando le percentuali di infezione per le diverse versioni delle edizioni a 32 bit di Microsoft Windows XP e Windows Vista per ciascun semestre, nel periodo compreso tra il primo semestre 2007 e il secondo semestre 2009.

Figura 5: tendenze CCM per le versioni a 32 bit di Microsoft Windows XP e Windows Vista, primo semestre 2007 - secondo semestre 2009



Tendenze delle categorie a livello mondiale

Figura 6: prime 10 famiglie di malware e software potenzialmente indesiderato rilevate dai prodotti desktop antimalware Microsoft nel secondo semestre del 2009 (la versione integrale del *SIR* include le prime 25 famiglie)

	Famiglia	Categoria più significativa	Computer puliti (2°sem09)
1	Win32/Taterf	Worm	3.921.963
2	Win32/Renos†	Trojan Downloader e Dropper	3.640.697
3	Win32/FakeXPA*	Trojan horse di vario tipo	2.939.542
4	Win32/Alureon†	Trojan horse di vario tipo	2.694.128
5	Win32/Conficker†	Worm	1.919.333 [3]
6	Win32/Frethog	Programmi di intercettazione password e strumenti di monitoraggio	1.823.066
7	Win32/Agent	Trojan horse di vario tipo	1.621.051
8	Win32/BaiduSobar	Software potenzialmente indesiderato di vario tipo	1.602.230
9	Win32/GameVance	Adware	1.553.646
10	Win32/Hotbar	Adware	1.476.838

Gli asterischi (*) indicano le famiglie di software di sicurezza non autorizzati.
Il simbolo della spada (†) indica le famiglie note per il download di software di sicurezza non autorizzati.

- In generale, i rilevamenti delle principali minacce sono diminuiti in modo significativo rispetto al primo semestre del 2009.

[3] La fondazione Shadowserver, che registra le infezioni di Win32/Conficker attive, ha segnalato che nel corso dell'ultimo giorno del secondo semestre 2009, 4,6 milioni di computer interessati da infezioni da Conficker sono stati rilevati dai server sinkhole gestiti da Shadowserver, un valore nettamente inferiore rispetto ai 5,2 milioni rilevati l'ultimo giorno del primo semestre 2009. Il calcolo della quantità di malware rilevato e pulito da software antimalware può, talvolta, restituire cifre molto diverse rispetto alle stime basate sulle osservazioni dei computer attivi interessati dalle infezioni e non esiste accordo univoco sul metodo più appropriato da utilizzare.

- Nel primo semestre del 2009 sette famiglie sono state rimosse da almeno 2 milioni di computer con gli strumenti desktop antimalware Microsoft, rispetto alle sole quattro famiglie rilevate nel secondo semestre del 2009.
- Persino Win32/Taterf, la minaccia più diffusa del secondo semestre del 2009, è stata rimossa da quasi 1 milione di computer in meno nello stesso periodo rispetto al primo semestre del 2009.
- I 3,9 milioni di computer infetti da Taterf nel secondo semestre del 2009 sono molti meno rispetto alla principale famiglia del primo semestre 2009, Win32/Zlob, che è stata rimossa da 9,0 milioni di computer durante lo stesso periodo.
- Molti utenti malintenzionati utilizzano i trojan downloader e dropper, come Win32/Renos e ASX/Wimad (rispettivamente la seconda e l'undicesima famiglia più diffusa nel secondo semestre del 2009), per distribuire altre minacce, come botnet, software non autorizzati e programmi di intercettazione password, nei computer.

- In generale il panorama del malware nel secondo semestre del 2009 è contrassegnato da una maggiore eterogeneità delle famiglie con diffusione moderata, da un minor numero di singole famiglie che dominano i primi posti della classifica e da una quantità notevolmente elevata di rimozioni. La rapida adozione di Microsoft Security Essentials può essere in parte responsabile della riduzione delle rimozioni.

Tendenze nella proliferazione dei campioni

Gli autori di malware tentano di eludere il rilevamento rilasciando di continuo nuove varianti, in modo da consentirne una più rapida diffusione rispetto alle nuove firme rilasciate dai produttori di antivirus. Un metodo per determinare quali sono attualmente le famiglie e le categorie di malware più attive consiste nel calcolare il numero di singoli campioni.

Figura 7: singoli campioni inviati al MMPC per categoria, primo semestre 2009 - secondo semestre 2009

Categoria	2°sem09	1°sem09	Differenza
Virus	71.991.221	68.008.496	5,9% ▲
Trojan horse di vario tipo	26.881.574	23.474.539	14,5% ▲
Trojan Downloader e Dropper	9.107.556	6.251.286	45,7% ▲
Software potenzialmente indesiderato di vario tipo	4.674.336	2.753.008	69,8% ▲
Adware	3.492.743	3.402.224	2,7% ▲
Exploit	3.341.427	1.311.250	154,8% ▲
Worm	3.006.966	2.707.560	11,1% ▲
Programmi di intercettazione password e strumenti di monitoraggio	2.217.902	7.087.141	-68,7% ▼
Backdoor	812.256	589.747	37,7% ▲
Spyware	678.273	269.556	151,6% ▲
Totale	**126.204.254**	**115.854.807**	**8,9%**

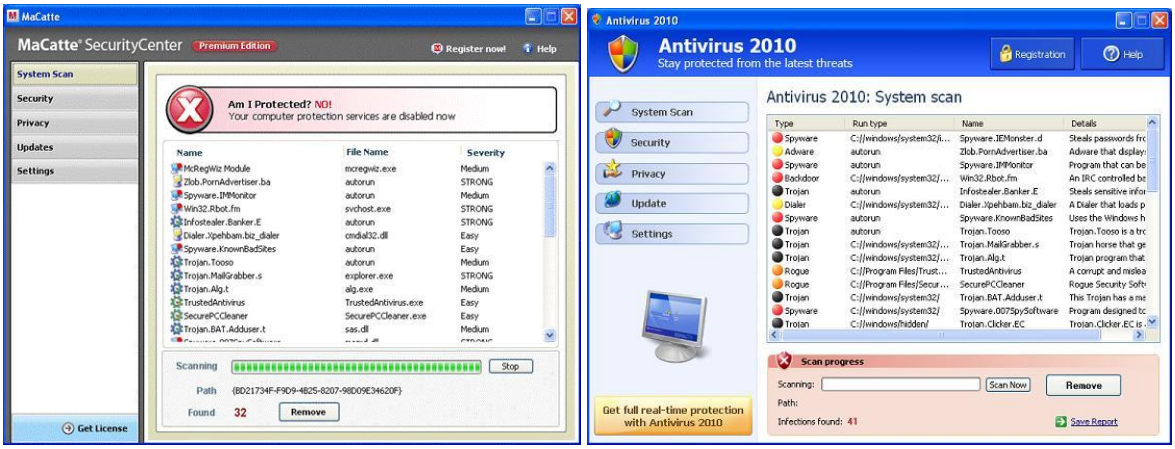
- Nel secondo semestre del 2009 sono stati rilevati oltre 126 milioni di campioni di software dannoso.
- Il calo nella categoria Programmi di intercettazione password e strumenti di monitoraggio è stato causato soprattutto da Win32/Lolyda, passato da 5,7 milioni di casi nel primo semestre del 2009 a meno di 100.000 nel secondo semestre del 2009.
- L'aumento nella categoria Spyware è legato soprattutto alla diffusione di Win32/ShopAtHome, con un numero di campioni unici rilevato nel secondo semestre del 2009 quintuplicato rispetto al periodo precedente.
- La grande quantità di virus rilevata dipende dal fatto che i virus tendono ad attaccare più file diversi, ciascuno dei quali viene considerato come un campione unico. Non si deve quindi considerare il numero di virus specificato come un'indicazione del numero effettivo di varianti di tali famiglie.

Software di sicurezza non autorizzato

Il software di sicurezza non autorizzato, ovvero un software che riporta allarmi falsi o ingannevoli relativi a infezioni o vulnerabilità del computer della vittima dell'attacco e offre la risoluzione dei problemi fasulli in cambio

di una somma di denaro, è diventato uno dei metodi più comuni utilizzati dagli utenti malintenzionati per sottrarre denaro alle vittime.

Figura 8: finte "analisi della sicurezza" eseguite da varianti di Win32/FakeXPA, la famiglia di software di sicurezza non autorizzati più diffusa nel secondo semestre del 2009

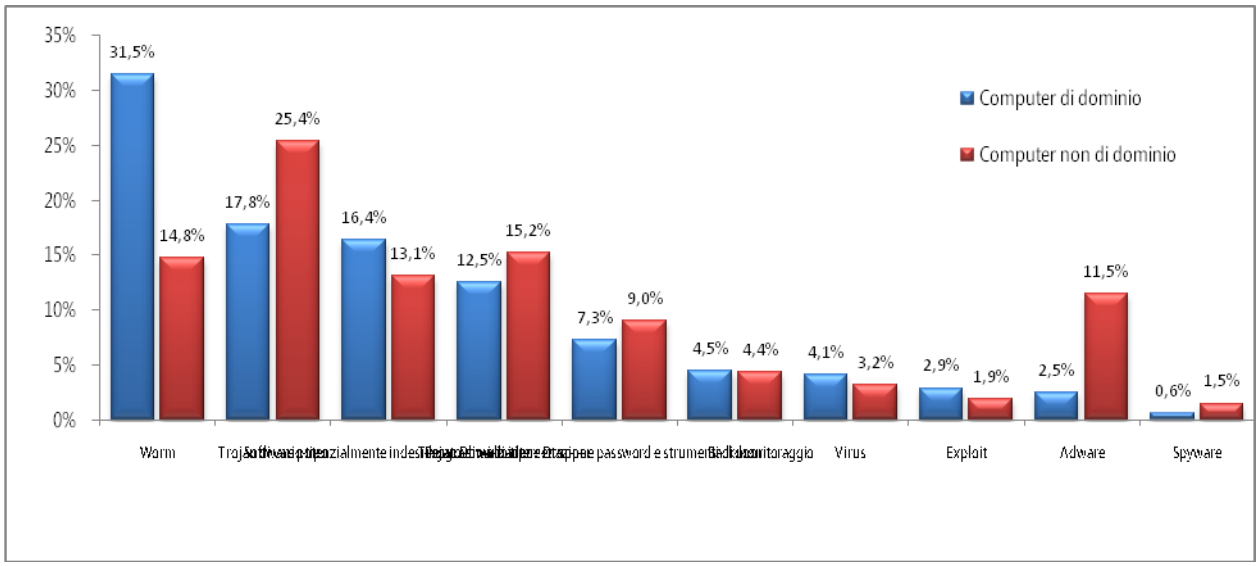


- I prodotti per la sicurezza di Microsoft hanno eliminato software di sicurezza non autorizzati (malware correlato su 7,8 milioni di computer nel secondo semestre 2009, fino a 5,3 milioni di computer nel primo semestre 2009) registrando un aumento del 46,5%, a suggerire che i software di sicurezza non autorizzati garantiscono a chi li distribuisce dei vantaggi maggiori rispetto ad altri tipi di minacce meno diffusi.
- Una delle famiglie di software di sicurezza non autorizzati, Win32/FakeXPA, risulta essere la terza minaccia per diffusione in tutto il mondo in base ai rilevamenti eseguiti dai prodotti per la sicurezza Microsoft nel secondo semestre del 2009. Altre tre di queste famiglie, Win32/Yektel, Win32/Fakespypro e Win32/Winwebsec, si sono classificate rispettivamente undicesima, quattordicesima e diciassettesima.
- Nel report *SIR* completo sono disponibili i dati di diffusione geografica relativi ai rilevamenti da parte di Microsoft dei software di sicurezza non autorizzati, con le famiglie più diffuse per questo tipo di minaccia in ciascuna regione.
- Sul sito http://www.microsoft.com/protect sono stati pubblicati tre nuovi video per il mercato consumer, allo scopo di informare i consumatori sui pericoli crescenti per sicurezza e privacy causati dalla diffusione dei software di sicurezza non autorizzati.

Panorama delle minacce nelle installazioni domestiche e aziendali

I dati sulle infezioni raccolti da prodotti e strumenti antimalware desktop di Microsoft comprendono informazioni sull'eventuale appartenenza del computer a un dominio Servizi di dominio Active Directory®. I domini si utilizzano quasi esclusivamente nelle grandi aziende e i computer che non appartengono a un dominio vengono in genere utilizzati in ambienti domestici o in altri contesti diversi dalle grandi aziende. Se si confrontano i dati relativi alle minacce rilevate dai computer che appartengono o non appartengono a un dominio, si ottengono analisi utili sulle diverse modalità adottate dagli utenti malintenzionati per colpire gli utenti domestici o aziendali e sulle minacce che hanno maggiori possibilità di diffondersi in un ambiente piuttosto che nell'altro.

Figura 9: suddivisione per categoria delle minacce per computer appartenenti o meno a un dominio nel secondo semestre 2009



- I computer che appartengono a un dominio hanno maggiori possibilità di imbattersi in worm rispetto ai computer che non appartengono a domini, a causa soprattutto delle modalità di propagazione dei worm. I worm si diffondono con maggiore efficacia mediante condivisioni di file e volumi di archiviazione rimovibili non protetti, elementi molto più diffusi in ambienti aziendali che domestici.
  - I worm occupano quattro delle prime 10 posizioni delle famiglie di minacce rilevate su computer appartenenti a domini.
  - Win32/Conficker, che utilizza vari metodi di propagazione più efficaci in un ambiente di rete tipicamente aziendale che su Internet, è nettamente il primo dell'elenco.
  - Allo stesso modo, Win32/Autorun, che attacca le unità rimovibili, si è rivelato più comune in ambienti di dominio in cui i volumi di questo tipo vengono utilizzati per lo scambio di file.
- Al contrario, le categorie Adware e Trojan di vario tipo sono molto più comuni in computer non di dominio.

Minacce tramite posta elettronica

I dati riportati in questa sezione sono basati sui messaggi di posta elettronica filtrati da Microsoft Forefront Online Protection for Exchange (FOPE), che offre servizi di filtro per posta indesiderata, phishing e malware a migliaia di clienti aziendali.

I messaggi di posta indesiderata associati alla cosiddetta truffa nigeriana (o truffa "419") e al gioco d'azzardo sono aumentati in modo significativo nel secondo semestre del 2009. In termini percentuali la maggior parte delle altre categorie sono rimaste stabili.

- La truffa nigeriana è un'abile frode basata sulla fiducia, in cui il mittente di un messaggio afferma di disporre di una grande somma di denaro ma di non potervi accedere direttamente per varie ragioni. In genere, le motivazioni specificate riguardano presunti veti burocratici o la corruzione politica. Il mittente chiede alla potenziale vittima un prestito da utilizzare per corrompere i funzionari o pagare le spese per ottenere l'intera somma di denaro. In cambio il mittente promette alla potenziale vittima una parte della somma totale, che in genere ammonta a una cifra molto maggiore di quella richiesta in prestito.
- Questi messaggi sono spesso associati a un articolo "419" del codice penale in vigore in Nigeria e relativo alle truffe, ma spesso citano anche altri paesi dell'Africa occidentale, tra cui Sierra Leone, Costa d'Avorio e Burkina Faso.

Figura 10: messaggi in ingresso bloccati dai filtri FOPE, per categoria, secondo semestre 2008 - secondo semestre 2009

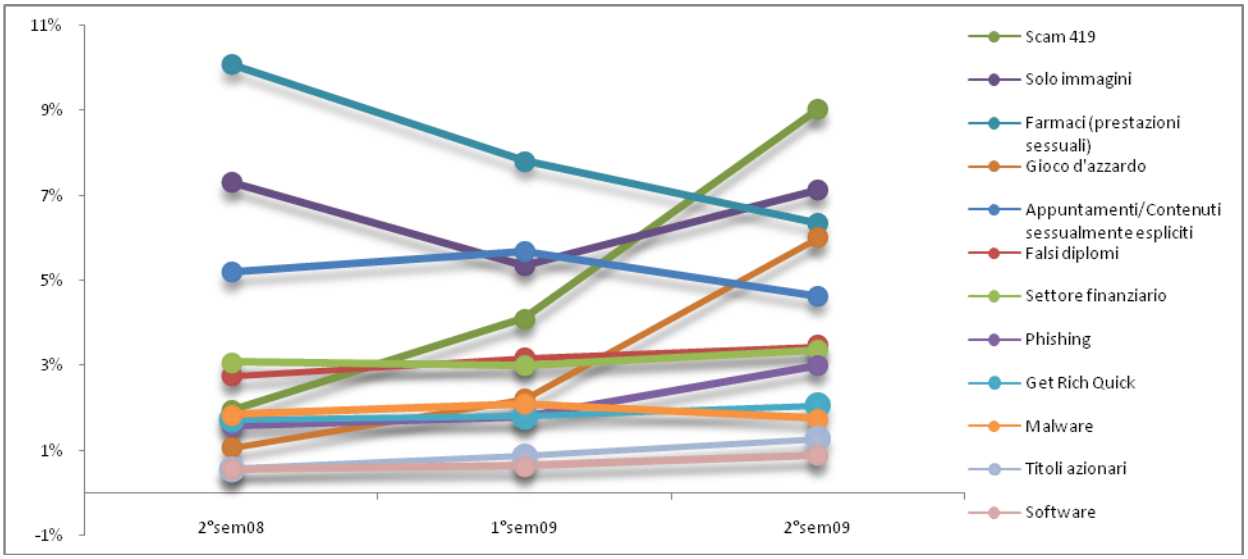
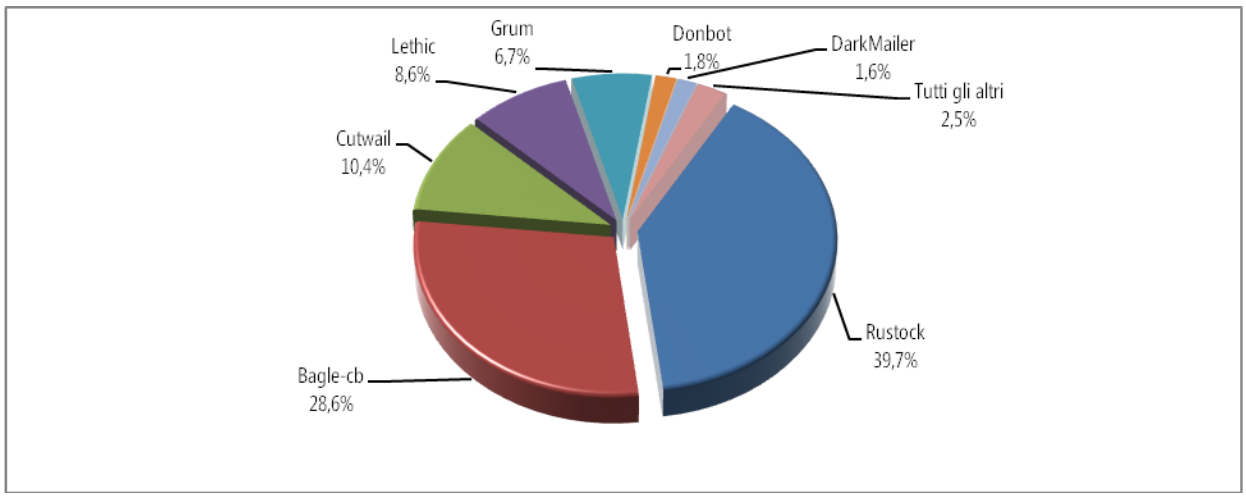


Figura 11: primi 5 paesi per invio di posta indesiderata, in percentuale sul totale della posta indesiderata inviata, nel secondo semestre 2009

	Paese	Percentuale
1	Stati Uniti	27,0%
2	Corea	6,9%
3	Cina	6,1%
4	Brasile	5,8%
5	Russia	2,9%

Le reti di computer infettati da malware botnet che un utente malintenzionato può controllare in modalità remota sono responsabili della maggior parte dei messaggi di posta indesiderata che vengono inviati oggi. Per misurare l'impatto delle botnet sul panorama globale della posta indesiderata, FOPE controlla i messaggi di posta indesiderata inviati da indirizzi IP noti come appartenenti a botnet.

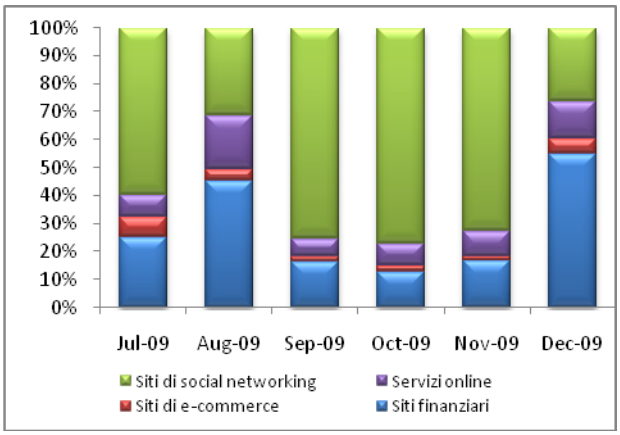
Figura 12: quasi tutti i messaggi di posta indesiderata inviati mediante botnet nel secondo semestre del 2009 si possono far risalire a poche botnet note (per ulteriori informazioni, vedere il report *SIR* completo)



Siti Web dannosi

Come già esposto nei volumi del report SIR precedenti, i siti di social networking sono stati sottoposti al volume totale maggiore di attacchi di phishing, oltre a far registrare il maggior tasso di attacchi di phishing per sito di phishing. Le istituzioni finanziarie hanno ricevuto il volume minore di attacchi di phishing per sito, ma con il volume totale di gran lunga maggiore di siti fraudolenti diversi. Nella figura riportata di seguito è indicata la percentuale degli attacchi di phishing registrati da Microsoft ogni mese nel secondo semestre 2009 per ciascuno dei tipi di istituzione più soggetti agli attacchi.

Figura 13: a sinistra: attacchi per tipo di sito di phishing ogni mese nel secondo semestre 2009; a destra: siti di phishing attivi registrati ogni mese, per tipo di obiettivo, nel secondo semestre 2009



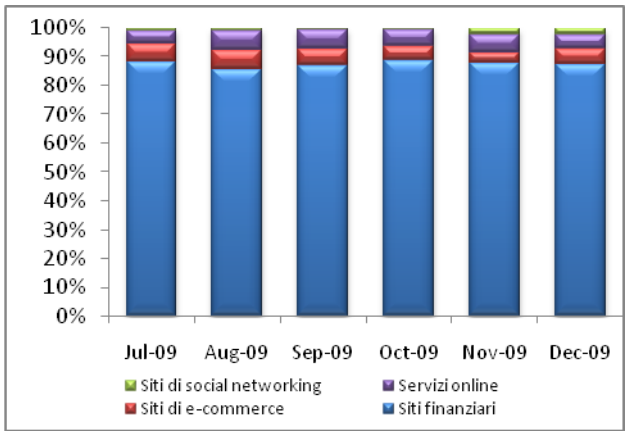
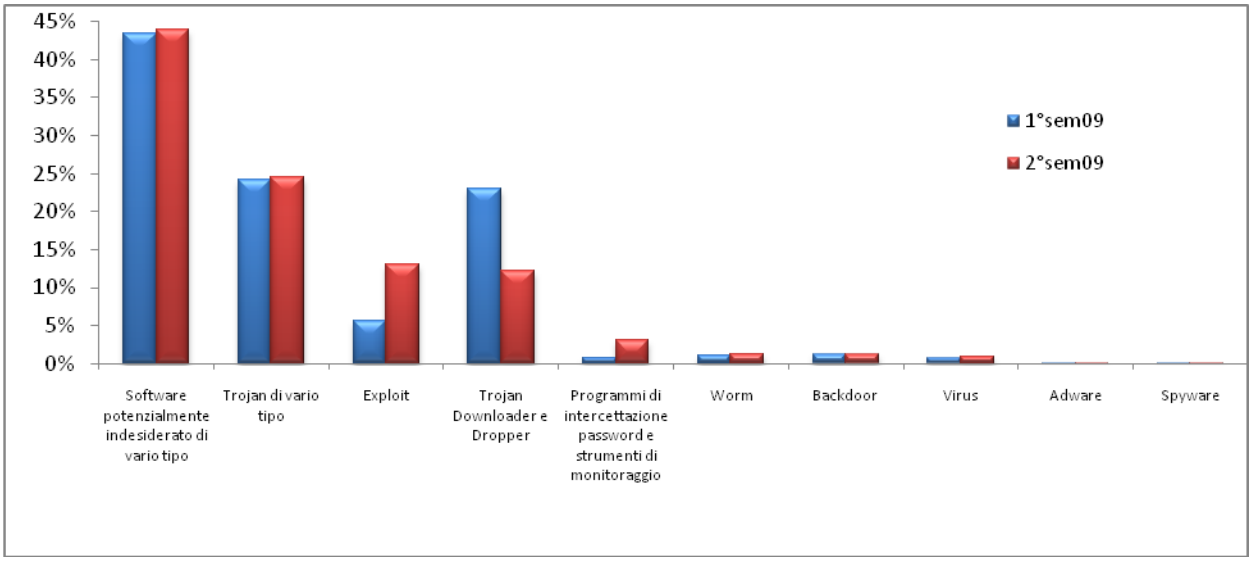


Figura 14: suddivisione per categoria delle minacce ospitate su URL bloccati dal filtro SmartScreen nel primo e nel secondo semestre 2009



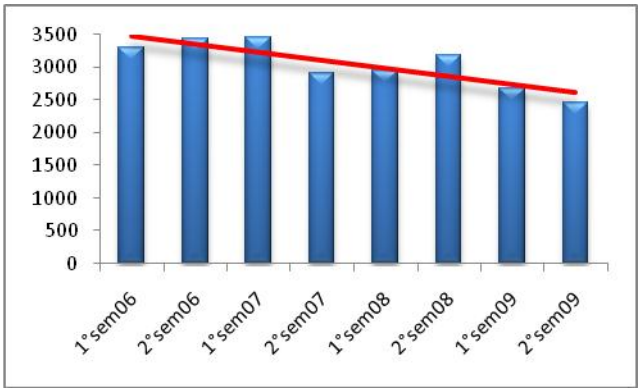
- In entrambi i periodi la classifica è dominata dalle categorie software potenzialmente indesiderato di vario tipo e Trojan di vario tipo.
- La categoria Trojan Downloader e Dropper, che nel primo semestre 2009 era prevalente quanto la categoria Trojan di vario tipo, è calata di circa il 50% nel secondo semestre dell'anno, mentre gli Exploit sono quasi raddoppiati.

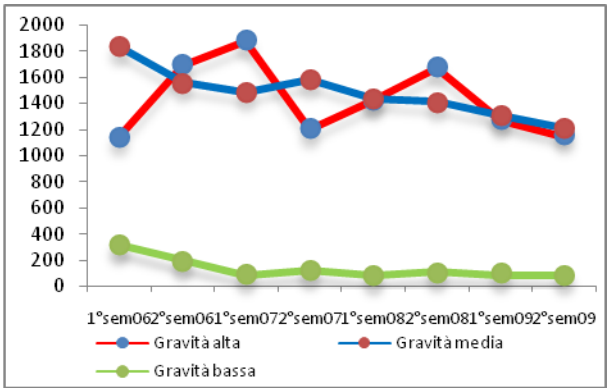
Risultati più significativi rilevati da Microsoft Security Response Center

Segnalazioni di vulnerabilità nel settore

Le *vulnerabilità* sono i punti deboli di un software che consentono a utenti malintenzionati di compromettere l'integrità, la disponibilità o la riservatezza del software. Alcune delle vulnerabilità più gravi consentono a utenti malintenzionati di eseguire codice arbitrario su un computer compromesso. Una divulgazione, nell'accezione in cui il termine viene utilizzato in questo report, è la comunicazione al pubblico della vulnerabilità di un software. Il termine non si riferisce a comunicazioni di tipo privato o limitate a un certo numero di persone.

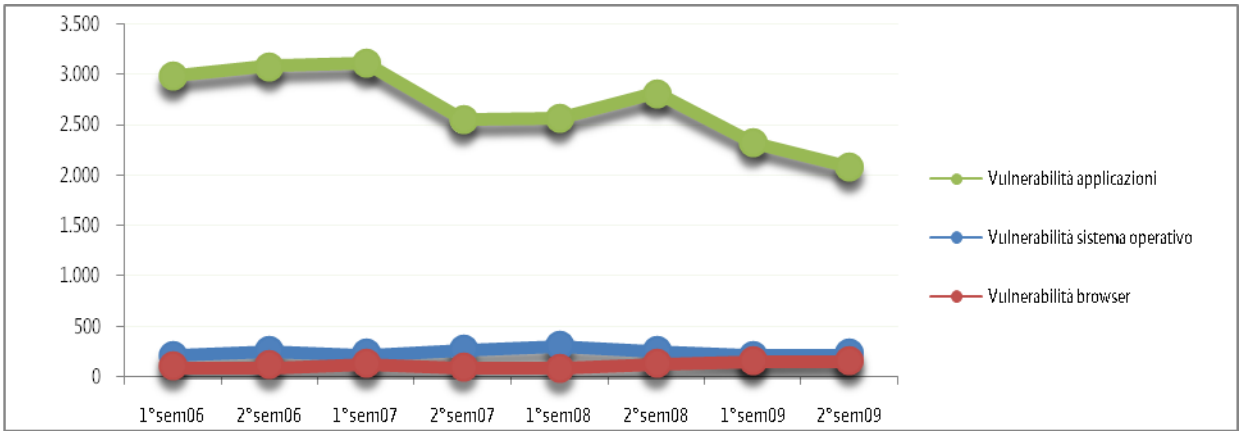
Figura 15: a sinistra: divulgazione di vulnerabilità all'intero settore economico per semestre, primo 2006 - secondo 2009 | a destra: divulgazione di vulnerabilità all'intero settore economico per gravità, primo semestre 2006 - secondo semestre 2009





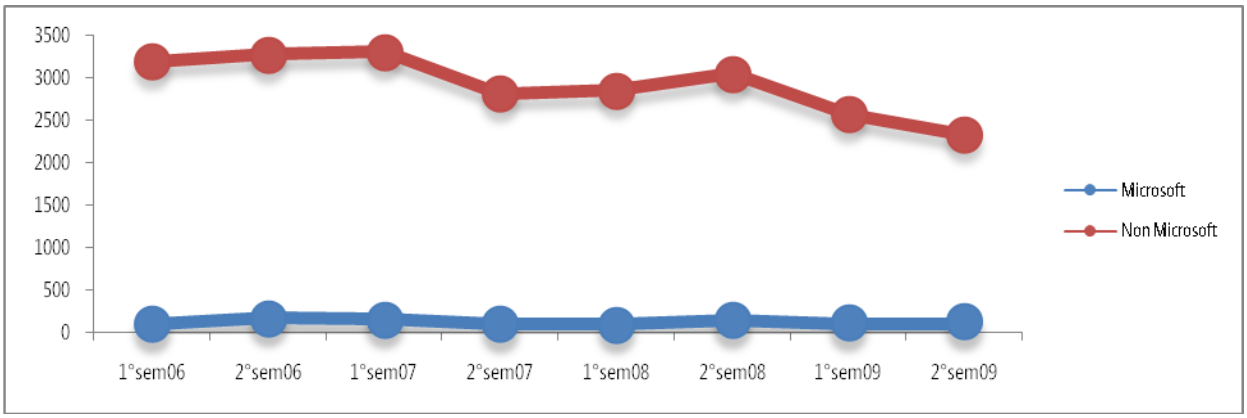
- Le divulgazioni di vulnerabilità sono calate dell'8,4% nel secondo semestre 2009 rispetto alla prima metà dell'anno, confermando una tendenza complessiva di calo moderato iniziata nel 2006.
- Le vulnerabilità di gravità bassa rappresentano solo il 3,5% di tutte le vulnerabilità rilevate nel secondo semestre 2009, in calo del 4,1% rispetto alla prima metà dell'anno.
- Le vulnerabilità di gravità alta divulgate nel secondo semestre 2009 sono state il 9,0% in meno rispetto alla prima metà dell'anno e il 30,7% in meno rispetto al secondo semestre 2008.
    - Continua la predominanza delle divulgazioni di vulnerabilità di gravità alta e media, probabilmente a causa, almeno parzialmente, della tendenza da parte di utenti malintenzionati e ricercatori di soluzioni di sicurezza a esercitare le proprie attività sulle vulnerabilità più gravi.

Figura 16: vulnerabilità di sistemi operativi, browser e applicazioni nell'intero settore, primo semestre 2006 - secondo semestre 2009



- Le vulnerabilità delle applicazioni hanno rappresentato la maggioranza delle vulnerabilità anche nel secondo semestre 2009, sebbene a fronte di una riduzione del numero totale di vulnerabilità delle applicazioni rispetto alla seconda metà del 2008 e al primo semestre del 2009.
- I numeri di vulnerabilità di sistema operativo e browser sono rimasti sostanzialmente stabili e rappresentano solo una piccola frazione del totale.

Figura 17: vulnerabilità divulgate per prodotti Microsoft e non Microsoft, primo semestre 2006 - secondo semestre 2009

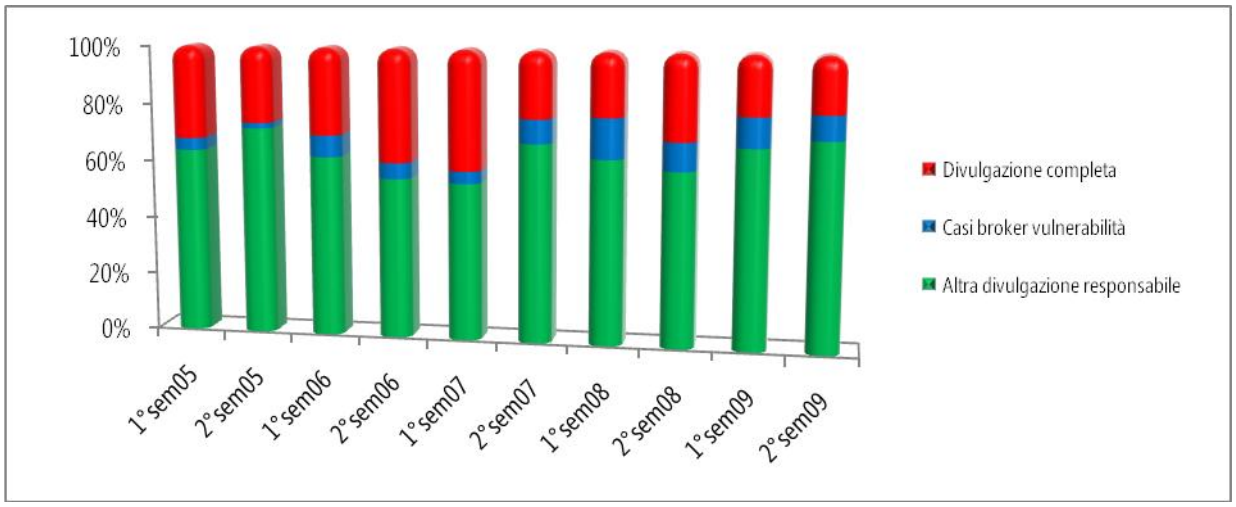


- Le vulnerabilità divulgate per i prodotti Microsoft sono aumentate da 113 nella prima metà del 2009 a 127 nel secondo semestre 2009.
- In generale le tendenze delle vulnerabilità divulgate per i prodotti Microsoft rispecchiano quelle dell'intero settore, con dei picchi tra il secondo semestre del 2006 e il primo del 2007 e ancora nel secondo semestre 2008.

- Negli ultimi quattro anni, le vulnerabilità divulgate per i prodotti Microsoft sono sempre rimaste comprese tra il 3 e il 5% di tutti i rilevamenti del settore.

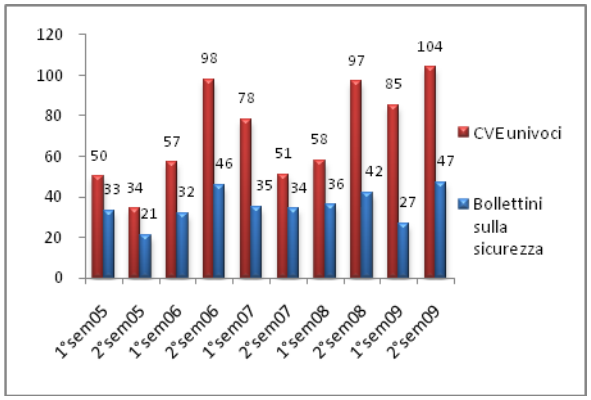
Con l'espressione "divulgazione responsabile" si intende la segnalazione in forma privata delle vulnerabilità al produttore interessato, che può così sviluppare un aggiornamento per la protezione completo in grado di rimediare alla vulnerabilità prima che i dettagli diventino di dominio pubblico.

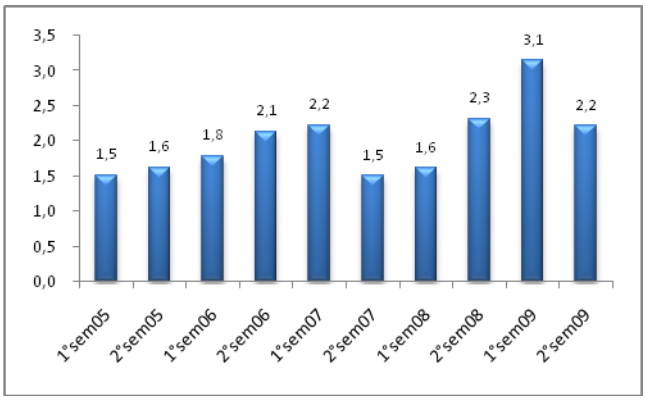
Figura 18: percentuale delle segnalazioni che hanno seguito la procedura di "divulgazione responsabile" rispetto al totale delle segnalazioni riguardanti software Microsoft, primo semestre 2005-secondo semestre 2009



- Nel secondo semestre 2009 l'80,7% delle vulnerabilità segnalate per i prodotti Microsoft hanno seguito la procedura di divulgazione responsabile, in aumento rispetto al 79,5% nel primo semestre 2009 e rispetto a qualsiasi altro periodo registrato precedente.
- La percentuale di divulgazioni segnalate da broker di vulnerabilità è leggermente diminuita dal 10,5% della prima metà del 2009 all'8,6% del secondo semestre dell'anno.

Figura 19: a sinistra: bollettini sulla sicurezza pubblicati e CVE risolti da Microsoft per semestre, primo semestre 2005 - secondo semestre 2009 | a destra: numero medio di CVE risolti per bollettino sulla sicurezza, primo semestre 2005 - secondo semestre 2009



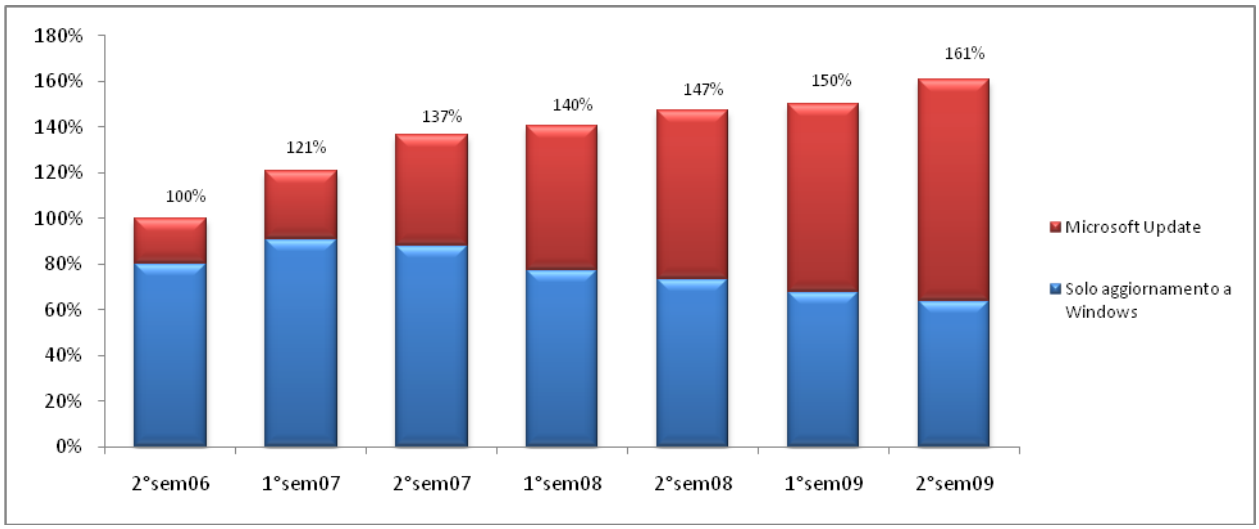


- Nel secondo semestre 2009 Microsoft ha pubblicato 47 bollettini sulla sicurezza con la risoluzione di 104 singole vulnerabilità, individuate nell'elenco delle vulnerabilità ed esposizioni comuni (Common Vulnerabilities and Exposures, CVE).

- Sebbene il numero di bollettini pubblicati sia aumentato rispetto ai 27 del primo semestre 2009, il numero di vulnerabilità risolte per bollettino è diminuito da 3,1 a 2,2

Come illustrato dalla figura riportata di seguito, la diffusione di Microsoft Update si è allargata in modo significativo negli ultimi anni. Il numero di computer che utilizzano il servizio più completo è aumentato di oltre il 17% rispetto al primo semestre 2009.

Figura 20: utilizzo di Windows Update e Microsoft Update, secondo semestre 2006 - secondo semestre 2009, indicizzato rispetto all'uso totale del secondo semestre 2006



- **Windows Update** offre aggiornamenti per i componenti di Microsoft Windows e per i driver dei dispositivi forniti da Microsoft e da altri produttori di hardware. Windows Update distribuisce inoltre aggiornamenti delle firme per i prodotti antimalware di Microsoft e il rilascio mensile di MSRT.
- **Microsoft Update** (http://update.microsoft.com/microsoftupdate) offre tutti gli aggiornamenti disponibili anche in Windows Update e gli aggiornamenti necessari per gli altri prodotti software di Microsoft. Gli utenti possono accedere al servizio durante l'installazione del software mediante Microsoft Update o il sito Web di Microsoft Update. Microsoft suggerisce di configurare i computer in modo da utilizzare Microsoft Update piuttosto che Windows Update, per garantire la ricezione tempestiva di aggiornamenti della sicurezza per i prodotti Microsoft.

Risultati più significativi rilevati da Microsoft Security Engineering Center

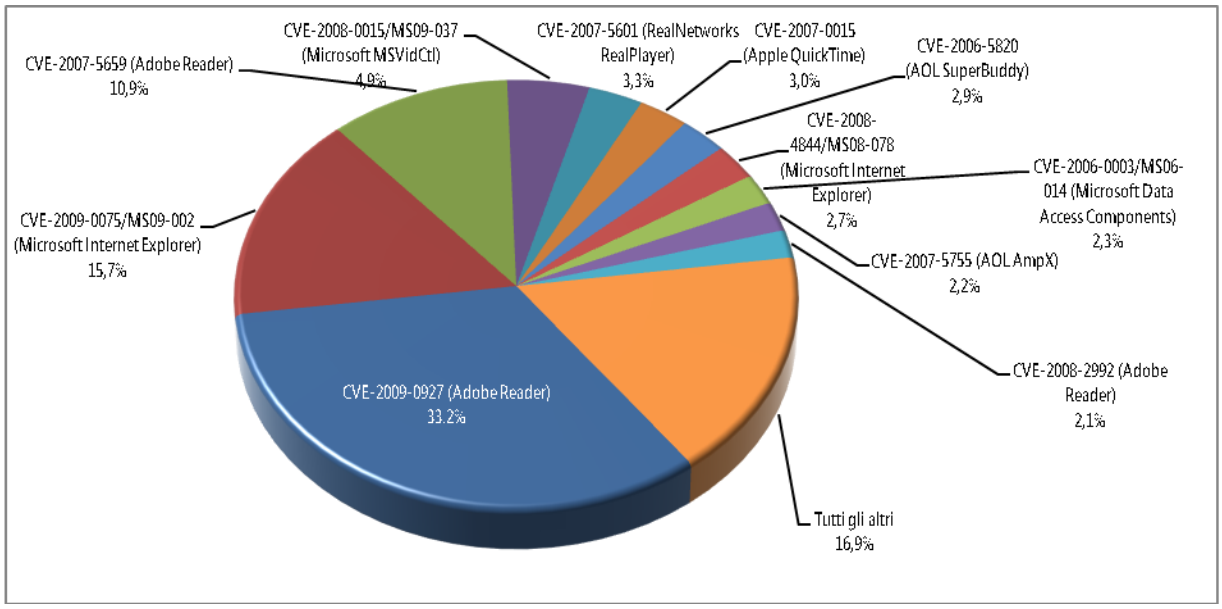
Ricerche sulla sicurezza: tendenze degli exploit

Un *exploit* è del codice dannoso progettato per infettare un computer senza il consenso dell'utente e, spesso, senza che questi possa nemmeno accorgersene. Gli exploit vengono in genere distribuiti mediante le pagine Web, anche se gli utenti malintenzionati usano anche altri metodi di diffusione, come i messaggi di posta elettronica e i servizi di messaggistica immediata. Le informazioni sulle modalità in cui gli autori degli attacchi sfruttano le vulnerabilità di browser e componenti aggiuntivi consentono ai ricercatori della sicurezza di comprendere meglio i rischi correlati ai "drive-by download" e ad altri attacchi basati sui browser.

- Nel passato i creatori di kit per exploit tendevano ad assemblare pacchetti con un numero di exploit variabile da quattro a sei, al fine di aumentare le probabilità di successo di un attacco.

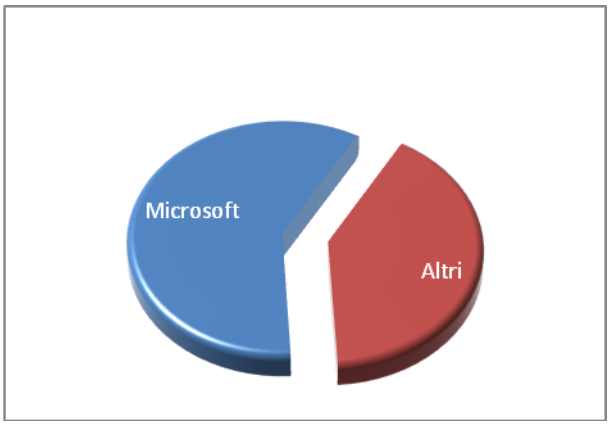
- Questa media è calata a 3,2 exploit per pacchetto nella prima metà del 2009, poiché gli utenti malintenzionati hanno sfruttato una serie di vulnerabilità affidabili e prevalenti in componenti di terze parti, rendendo inutile il ricorso a una maggiore quantità di exploit.
- Questa tendenza si è confermata nel secondo semestre 2009 e il numero medio di exploit per pacchetto è sceso a 2,3.
- Tuttavia, alcuni utenti malintenzionati ancora preferiscono utilizzare molti exploit per pacchetto, con un picco di 23 exploit osservato in un kit nel secondo semestre 2009.

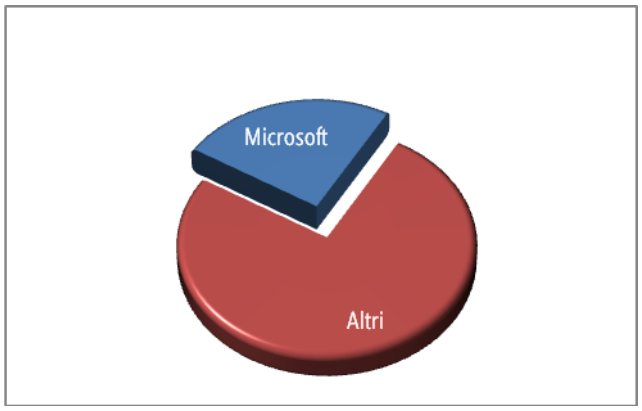
Figura 21: exploit basati su browser rilevati nel secondo semestre 2009, in percentuale



- Il CVE-2007-0071, una vulnerabilità di tipo drive-by download di Adobe Flash Player che nel primo semestre 2009 era la vulnerabilità dei browser più sfruttata, è passato al 23° posto nella seconda metà dell'anno con solo lo 0,4% degli exploit.
  - Variazioni così evidenti come la precedente possono essere correlate alla tendenza dei creatori di kit di exploit a sostituire spesso gli exploit meno recenti con altri più nuovi.
  - Come illustrato dal grafico a destra nella Figura 21, l'incidenza di alcuni degli exploit prevalenti è cambiata in modo significativo da mese a mese nel secondo semestre 2009.
- Una vulnerabilità nella Figura 21 è stata risolta con una patch nel 2006.
- Per tutte le vulnerabilità specificate nella Figura 21 sono stati resi disponibili aggiornamenti della sicurezza prima del periodo di riferimento del SIR.

Figura 22: a sinistra: exploit basati su browser che hanno colpito software Microsoft e di terze parti su computer basati su Microsoft Windows XP nel secondo semestre 2009 | a destra: exploit basati su browser che hanno colpito software Microsoft e di terze parti su computer basati su Microsoft Windows Vista e Windows 7 nel secondo semestre 2009





- Il confronto tra gli exploit che hanno colpito il software Microsoft e gli exploit destinati a software di terze parti (ovvero ai software commercializzati da altri produttori) suggerisce che il panorama delle vulnerabilità di Microsoft Windows Vista e Windows 7 è molto diverso da quello di Microsoft Windows XP.
  - In ambienti Microsoft Windows XP le vulnerabilità dei prodotti Microsoft costituiscono il 55,3% di tutti gli attacchi del campione preso in esame.
  - In ambienti Microsoft Windows Vista e Windows 7 la proporzione delle vulnerabilità dei prodotti Microsoft si riduce in modo evidente, costituendo solo il 24,6% degli attacchi del campione preso in esame.
    - Questa cifra rappresenta comunque un aumento rispetto al 15,5% del primo semestre 2009 (comprende solo Microsoft Windows Vista) a causa dell'aumento degli attacchi da CVE-2009-0075/MS09-002, una vulnerabilità di Internet Explorer 7 che interessa Microsoft Windows Vista RTM e SP1 (ma non Microsoft Windows Vista SP2 o Windows 7). L'exploit è stato risolto con l'aggiornamento della sicurezza Microsoft del gennaio 2009.

Le Figure 23 e 24 nella pagina che segue illustrano le 10 vulnerabilità sfruttate più spesso in Microsoft Windows XP (Figura 23) e in Microsoft Windows Vista e Windows 7 (Figura 24).

Figura 23: le 10 vulnerabilità basate su browser sfruttate più spesso in ambienti Microsoft Windows XP, in percentuale su tutti gli exploit, nel secondo semestre 2009

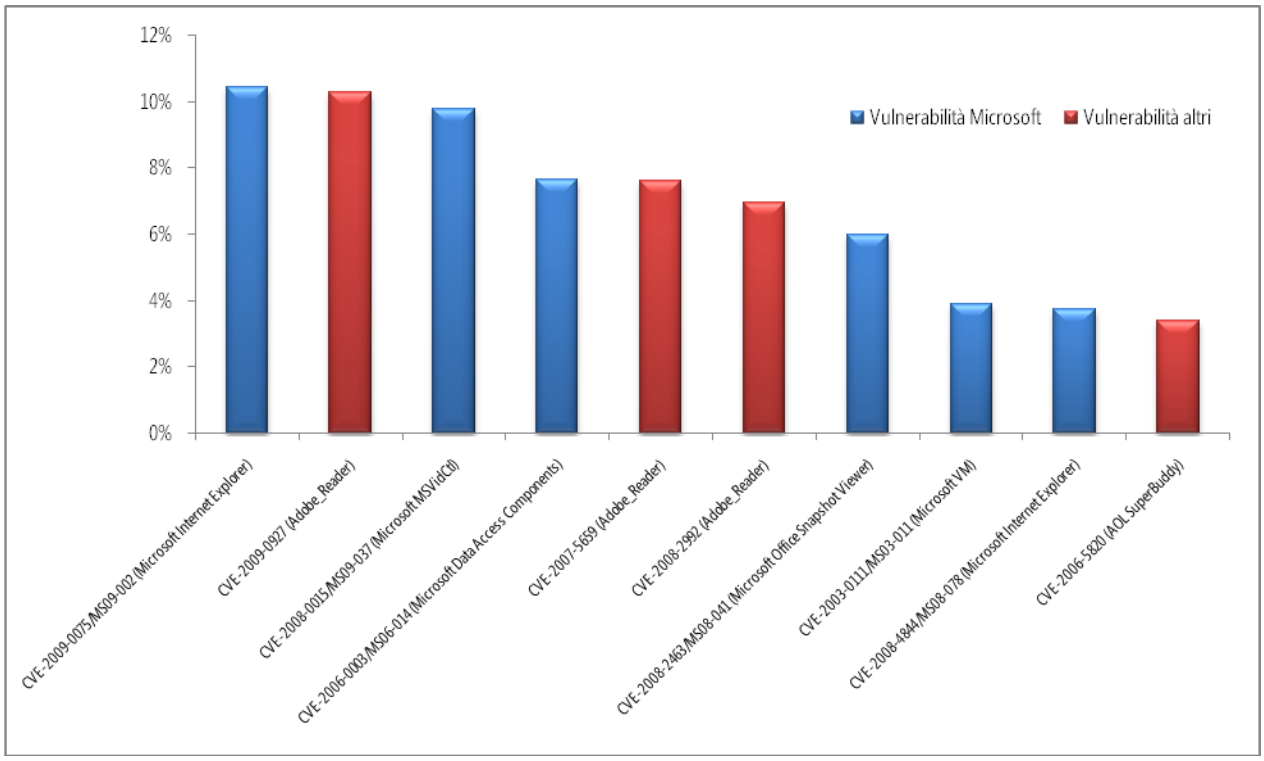
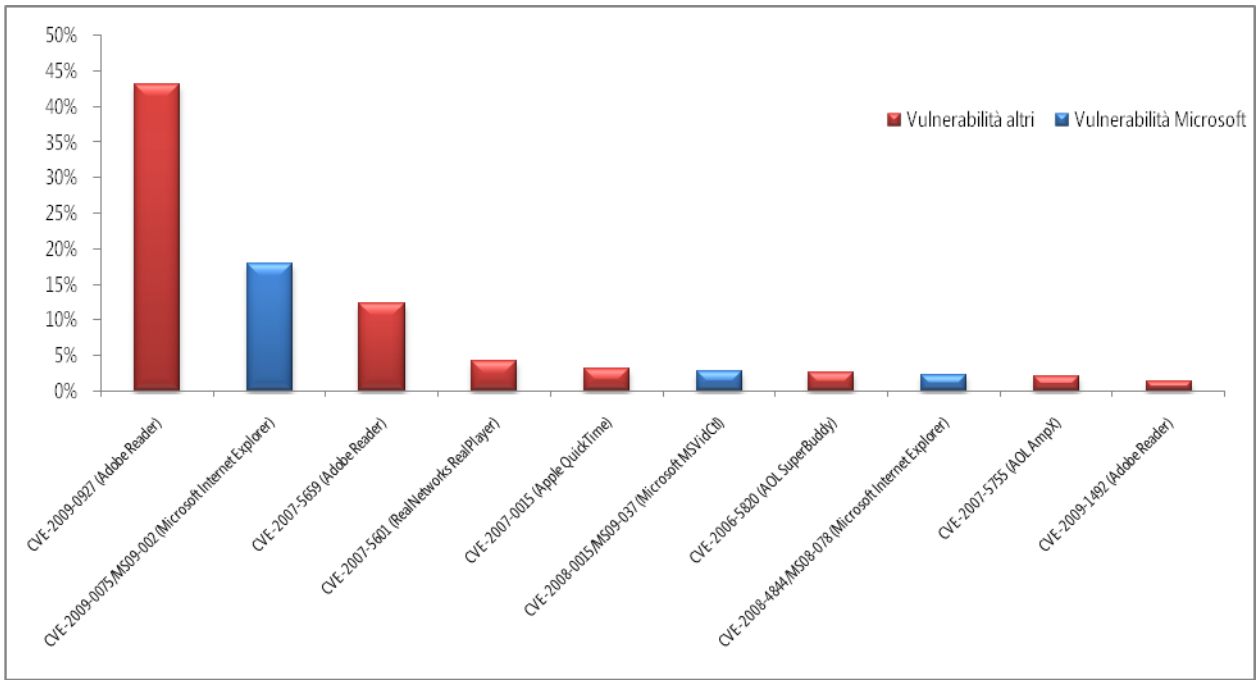


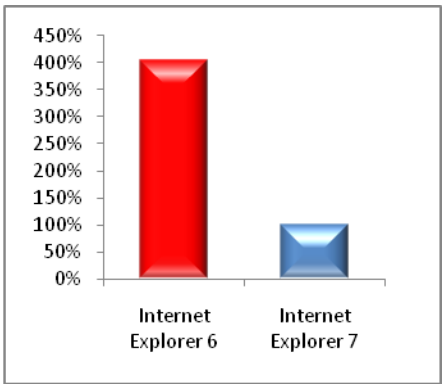
Figura 23: le 10 vulnerabilità basate su browser sfruttate più spesso in ambienti Microsoft Windows Vista e Windows 7, in percentuale su tutti gli exploit, nel secondo semestre 2009



Le pagine di drive-by download in genere sono ospitate in siti Web legittimi a cui un utente malintenzionato aggiunge del codice di exploit. Gli utenti malintenzionati riescono ad accedere a siti legittimi con intrusioni o inviando codice dannoso a un modulo Web protetto in modo inadeguato, ad esempio mediante il campo per i commenti di un blog.

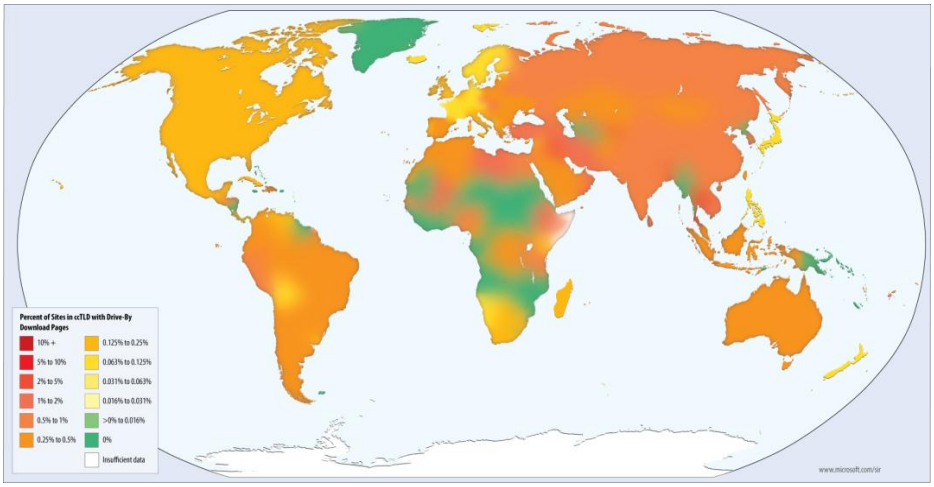
- Un'analisi delle vulnerabilità specifiche colpite da siti di drive-by download suggerisce che la maggior parte degli exploit utilizzati da questi siti dannosi aggrediscono i browser meno recenti, mentre non hanno alcun effetto sui più aggiornati. Come evidenziato dalla figura riportata di seguito, nel secondo semestre 2009 gli exploit che colpiscono Internet Explorer 6 sono comparsi su oltre il quadruplo dei siti di drive-by download rispetto agli exploit che colpiscono Internet Explorer 7.

Figura 25: siti di drive-by download che hanno colpito Internet Explorer 6 e Internet Explorer 7, indicizzati rispetto al totale di Internet Explorer 7, nel secondo semestre 2009



- Con il procedere dell'indicizzazione del Web da parte di Bing, vengono valutati gli elementi o comportamenti dannosi delle pagine.
  - Bing rileva ogni mese una grande quantità di pagine di drive-by download, con alcune centinaia di migliaia di siti che ospitano pagine di drive-by download attive registrati a ogni successiva indicizzazione.
  - Poiché i proprietari dei siti infetti sono spesso essi stessi vittime degli attacchi, i siti non vengono rimossi dall'indice di Bing. Se però si fa clic sul collegamento riportato nell'elenco dei risultati della ricerca, viene visualizzato un avviso che avvisa l'utente che la pagina potrebbe contenere software dannoso.
    - Nel secondo semestre del 2009 circa lo 0,3% delle pagine visualizzate dagli utenti nei risultati delle ricerche di Bing contenevano avviso relativi a siti dannosi.
  - Nel complesso il numero di siti Web infetti registrati da Bing è aumentato nel secondo semestre 2009: lo 0,24% di tutti i siti Web ospitano almeno una pagina dannosa, con una crescita rispetto allo 0,16% del primo semestre 2009. L'aumento dipende probabilmente in parte da alcuni nuovi meccanismi di rilevamento più efficaci adottati da Bing nella seconda metà del 2009.
- Bing ha rilevato siti di drive-by download in tutto il mondo, ma il rischio non è distribuito in modo uniforme per tutti gli utenti di Internet. In alcune aree del mondo gli utenti sono più a rischio che in altre. Nella figura riportata di seguito viene illustrata la porzione di siti Web per ciascun codice paese per dominio di primo livello (ccTLD) individuati come infetti da drive-by download nel secondo semestre 2009.
  - Sono state rilevate pagine di drive-by download su oltre il 2,1% dei siti nel dominio ccTLD .th (associato alla Thailandia) e almeno l'1% dei siti nel dominio ccTLD .cn (Cina).

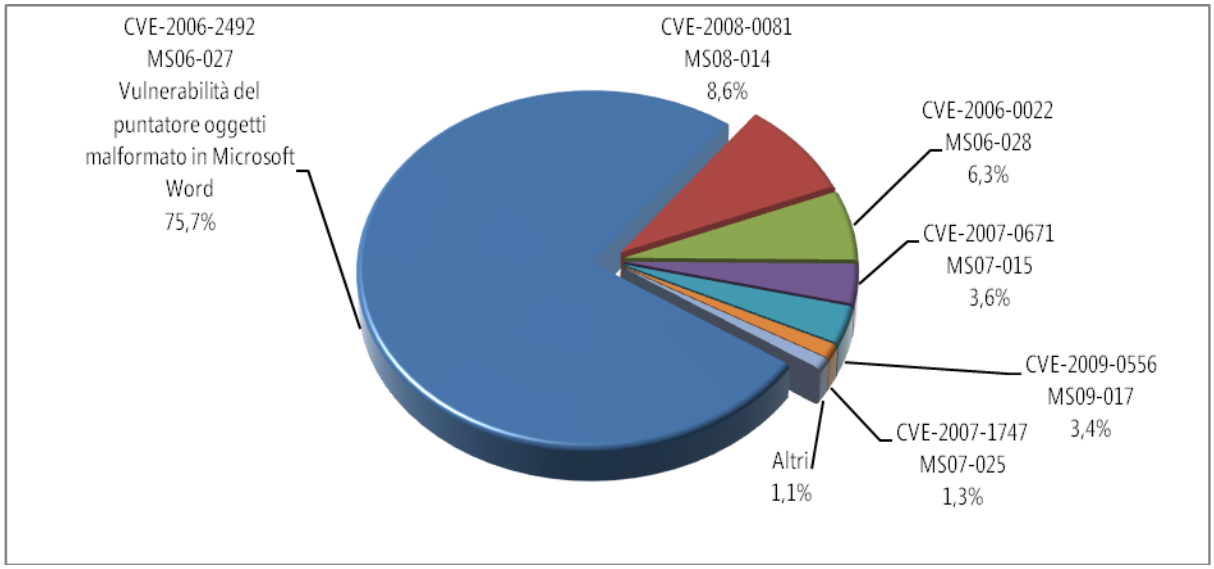
Figura 26: [BingGeo_Heatmap] percentuale dei siti Web per ciascun codice paese per dominio di primo livello (ccTLD) individuati come infetti da drive-by download nel secondo semestre 2009



- In confronto i domini di primo livello generici e sponsorizzati che non sono associati a paesi/regioni particolari non mostrano gli stessi livelli di differenziazione dei domini ccTLD.
  - Il TLD .biz, utilizzato dalle aziende, contiene la percentuale più alta di siti che ospitano pagine drive-by download: nello 0,76% dei siti .biz attivi sono state individuate pagine di questo tipo.
- Le pagine di drive-by download sono state rilevate in tutti i domini TLD generici, sponsorizzati e con codici del paese, ma i server degli exploit sono concentrati in un numero di TLD più ridotto, sopratutto nei domini .com (33,2%) e .cn (19,0%).
  - Nel secondo semestre 2008 il server di exploit più utilizzato al mondo raggiungeva circa 100.000 pagine. Il numero è aumentato a oltre 450.000 pagine nel primo semestre 2009 e a quasi 750.000 nel secondo semestre 2009.
    - Nonostante questo aumento, sono molto pochi i server che erano al vertice dell'elenco del primo semestre 2009 che sono rimasti in posizioni analoghe nel secondo semestre 2009.
- Le reti di distribuzione del malware sono bersagli mobili, con server che scompaiono e appaiono di continuo in luoghi diversi.

Gli autori degli attacchi usano come vettori di trasmissione degli exploit sempre più spesso formati di file comuni (come .doc, .pdf, .ppt e .xls). *Le vulnerabilità dei parser* rappresentano una classe di vulnerabilità in cui l'utente malintenzionato crea un documento specificamente progettato che sfrutta un errore di elaborazione o analisi del formato del file. Molti di questi formati sono complessi ed efficienti e l'autore di un attacco può creare file con una sezione malformata che sfrutta una vulnerabilità del programma.

Figura 27: exploit per i formati di file Microsoft Office rilevati, in percentuale, nel secondo semestre 2009



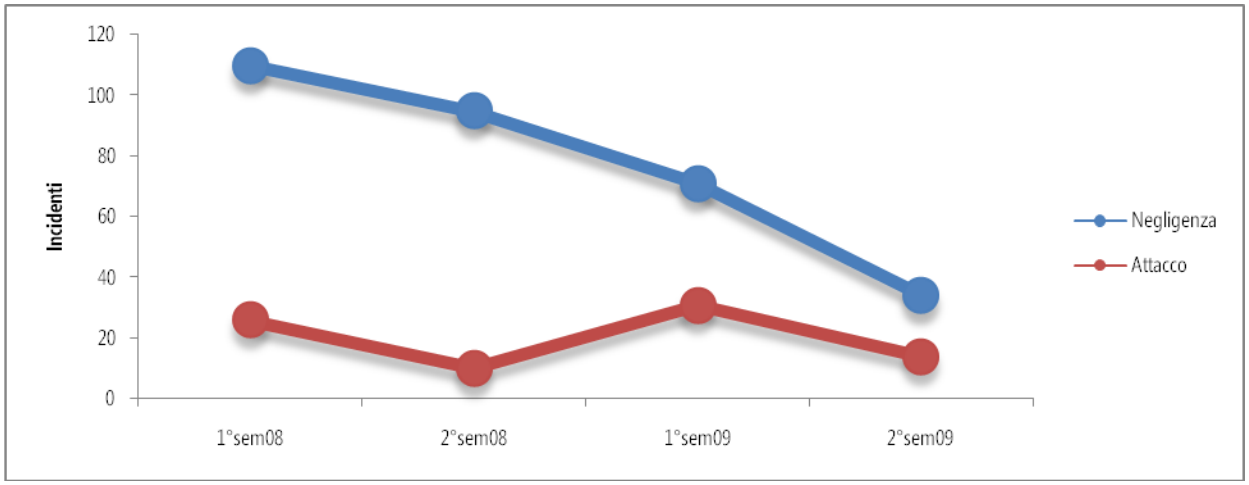
- La maggior parte delle vulnerabilità sfruttate nel campione di dati erano note da alcuni anni ed erano state tutte oggetto di aggiornamenti della sicurezza pubblicati per proteggere i computer dall'exploit. Un terzo di queste erano state identificate per la prima volta nel 2006.
- Il 75,7% degli attacchi sfruttavano una singola vulnerabilità (CVE-2006-2492, la vulnerabilità del puntatore oggetti malformato in Microsoft Word) per cui alla fine del 2009 esisteva una correzione rapida per la sicurezza da oltre tre anni.
- Gli utenti che non aggiornano i programmi di Microsoft Office e il sistema operativo Microsoft Windows con Service Pack e aggiornamenti per la sicurezza sono più esposti al rischio di attacchi. La maggior parte degli attacchi ha colpito computer con installazioni di Microsoft Office non aggiornate da molto tempo.
    - Oltre la metà degli attacchi (il 56,2%) ha colpito installazioni di Microsoft Office mai aggiornate dal 2003.
    - La maggior parte di questi attacchi hanno riguardato gli utenti di Microsoft Office 2003 che non avevano applicato un Service Pack o un aggiornamento per la sicurezza dopo il rilascio della versione originale di Microsoft Office 2003 nell'ottobre 2003.
    - Non è affatto raro che le vittime di exploit di programmi Microsoft Office dispongano di installazioni di Microsoft Windows molto più aggiornate. Quasi i due terzi (62,7%) degli attacchi a Microsoft Office osservati nel secondo semestre 2009 ha riguardato computer che utilizzavano versioni di Microsoft Windows aggiornate nei 12 mesi precedenti.
    - La quantità media di tempo trascorso dall'ultimo aggiornamento del sistema operativo per i computer del campione era di circa 8,5 mesi, rispetto ai 6,1 anni per l'ultimo aggiornamento dei programmi Microsoft Office, quasi nove volte maggiore.
        - I dati aiutano a comprendere come gli utenti che aggiornano con frequenza Microsoft Windows restino comunque esposti a rischio di exploit se non aggiornano con regolarità anche gli altri programmi.

Tendenze delle violazioni della protezione

Eventi di sicurezza che hanno provocato problemi di privacy

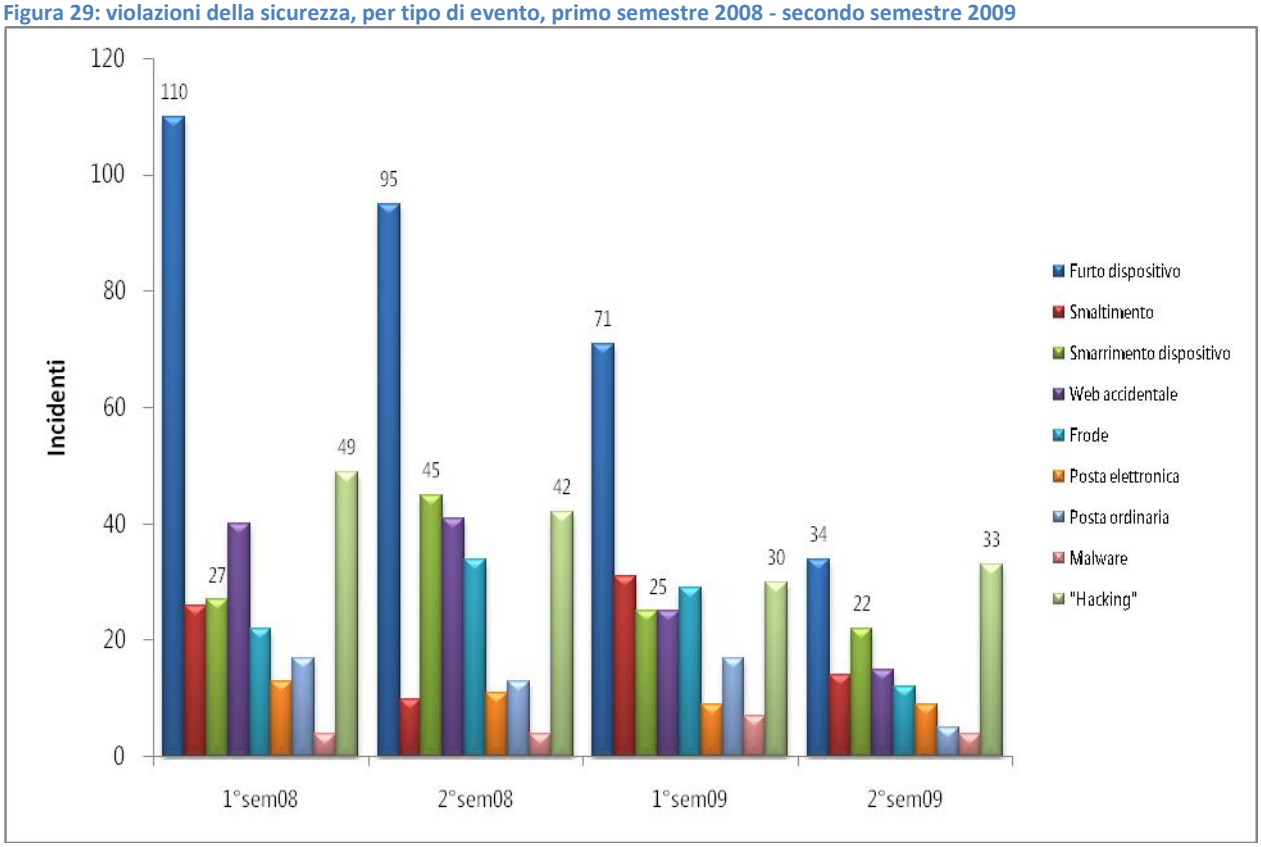
Negli ultimi anni in molti paesi del mondo sono state approvate norme che, in caso di perdite di dati che consentono l'identificazione personale dell'utente da parte di un'organizzazione, prevedono la notifica alle persone interessate. Queste notifiche obbligatorie rappresentano un'occasione unica per approfondire l'analisi su come le misure di protezione delle informazioni adottate debbano affrontare problemi di negligenza oltre che tecnologici[4].

Figura 28: violazioni che derivano da attacchi e negligenza, primo semestre 2008 - secondo semestre 2009



[4] A partire dal 2005, ricercatori volontari sulla sicurezza hanno raccolto e registrato i rapporti pubblicati in vari paesi del mondo e relativi alle violazioni di questo tipo di dati, consolidandoli nel Data Loss Database (DataLossDB) disponibile all'indirizzo http://datalossdb.org.

Figura 29: violazioni della sicurezza, per tipo di evento, primo semestre 2008 - secondo semestre 2009



- Si evidenzia una chiara tendenza al ribasso nel numero assoluto di eventi in ognuna delle singole categorie, con l'eccezione degli attacchi da malware, che restano invariati.
- Furti di dispositivi e supporti e le perdite Web accidentali fanno registrare i cali più vistosi.
- Lo smaltimento non corretto degli archivi aziendali è la causa di un buon numero di eventi. Le organizzazioni possono risolvere questo tipo di violazioni con relativa facilità, ricorrendo a procedure efficaci di distruzione degli archivi cartacei ed elettronici che contengono informazioni riservate.
- Molti associano le violazioni della sicurezza a malintenzionati che cercano e ottengono l'accesso non autorizzato a dati riservati, ma il numero di eventi che hanno avuto come presupposto un attacco (hacking, malware e frodi) negli ultimi anni è molto minore degli eventi che dipendono da semplice negligenza (smarrimento, furto o indisponibilità di dispositivi, divulgazione accidentale o smaltimento non corretto).
- Negli ultimi due anni gli eventi che derivano da negligenza sono decisamente diminuiti, da 110 nel primo semestre 2008 a soli 34 nel secondo semestre 2009.
    - Per proteggere i dispositivi più importanti, le organizzazioni possono adottare ulteriori misure, come controlli all'ingresso degli uffici o programmi di formazione dei dipendenti sulle procedure di sicurezza.
    - L'utilizzo di solide soluzioni di crittografia, come Crittografia unità BitLocker® di Microsoft Windows, può ulteriormente migliorare la situazione. Le norme in materia di divulgazione di molti paesi non obbliga alla notifica in caso di furto o smarrimento di dati crittografati, poiché è molto più difficile per l'autore del furto o del ritrovamento estrarre i dati dal supporto crittografato.

Strategie di prevenzione

Gestione del rischio IT in Microsoft

Al personale IT di Microsoft è affidata la responsabilità delle operazioni quotidiane e della sicurezza della rete globale di Microsoft. In questa nuova sezione del SIR il personale IT di Microsoft condivide molte delle strategie di prevenzione specifiche adottate per gestire il rischio in questo ambiente estremamente complesso, oltre a fornire suggerimenti pratici che i professionisti IT e della sicurezza possono seguire per migliorare la protezione dei propri ambienti. Gli argomenti illustrati comprendono i vari metodi di protezione dell'infrastruttura di rete aziendale e di promozione della consapevolezza e dei comportamenti di "safe computing" all'interno dell'organizzazione.

Microsoft ha inoltre prodotto istruzioni complete indirizzate ai professionisti IT che aiutano a gestire il processo di valutazione, definizione delle priorità e implementazione degli aggiornamenti della sicurezza per i prodotti Microsoft. La Microsoft Security Update Guide (in inglese) è disponibile per il download gratuito all'indirizzo www.microsoft.com/securityupdateguide.

Il *SIR* completo contiene inoltre le strategie di prevenzione e le procedure consigliate alle organizzazioni per prevenire molti dei rischi di sicurezza individuati nel *SIR*.

È possibile scaricare il *SIR* completo all'indirizzo www.microsoft.com/sir.

Aiuta Microsoft a migliorare il report sullo stato della protezione

Grazie per aver letto l'ultimo volume del *Report sullo stato della protezione Microsoft*. Microsoft desidera mantenere il report quanto più fruibile e utile possibile per i clienti. In caso di commenti o suggerimenti su questo volume del report oppure su come sia possibile migliorare i prossimi volumi, contattare Microsoft inviando un messaggio di posta elettronica all'indirizzo sirfb@microsoft.com.

Grazie e cordiali saluti,

Microsoft Trustworthy Computing