



2008: il web si tinge di giallo

Il 2008 è stato un anno per alcuni aspetti innovativo dal punto di vista della sicurezza informatica. L'utilizzo di rootkit e di exploit è ancor più radicato negli attacchi che sono veicolati per la maggior parte attraverso le pagine web. I sistemi operativi alternativi a Windows guadagnano sempre più spazio, ma incontrano anche alcune difficoltà

IL PROBLEMA DEI ROOTKIT

L'anno che si sta per chiudere ha fatto registrare nuovi record nel mondo della sicurezza informatica. **Il 2008 si è chiuso ponendo alcuni paletti** che necessariamente le società di sicurezza devono tenere in considerazione per poter pensare di essere ancora competitive e, soprattutto, per poter pensare di tenere il passo dei malware writer.

L'utilizzo sempre più massiccio di tecniche di infezione basate su rootkit ha messo in evidenza le debolezze dei software di sicurezza che non riescono a tenere il passo di fronte a questa tipologia di attacchi, con la conseguenza che sempre più computer rimangono infetti e i software di sicurezza installati non riescono ad individuare l'ospite non voluto.

Il 2008 è iniziato subito nel peggiore dei modi. Gli strascichi degli attacchi di fine 2007 da parte del worm Storm si sono allungati per tutto l'inizio dell'anno successivo e si sono sovrapposti ad un altro tipo di attacco che ha colto l'intero mondo della sicurezza informatica di sorpresa.

L'anno in questione verrà ricordato probabilmente come l'anno del **MBR rootkit**, anche conosciuto come **Mebroot**: un rootkit che infetta il Master Boot Record dell'hard disk per garantirsi l'avvio alla partenza del sistema operativo.

Segnalato per la prima volta dallo sviluppatore del tool antirootkit GMER, seguono poi numerose analisi da parte delle società di sicurezza. Alla fine di Gennaio la società russa Dr.Web e la società inglese Prevx sono le prime società di sicurezza a rilasciare un tool di rimozione per questo rootkit.

La particolarità del MBR rootkit risiede, come citato precedentemente, **nell'infezione del Master Boot Record, il settore di avvio del disco rigido che consiste nei primi 512 bytes.**

Nel momento in cui il computer viene avviato, attraverso il MBR infetto il rootkit prende il controllo dell'Interrupt 13h, responsabile della gestione dell'accesso a basso livello al disco

rigido. Analizzando il flusso dei dati che passano, il malware modifica in memoria il kernel di Windows facendo sì che il driver del rootkit venga caricato.

Una volta eseguito nel sistema, **il rootkit è in grado di bypassare eventuali firewall installati e di connettersi all'esterno, aprendo backdoor e scaricando nuove infezioni all'interno del PC.**

La difficoltà nell'intercettare l'infezione sta nella particolarità delle modalità di infezione.

Agli occhi di un software antirootkit tutto sembrerebbe normale. **Non esiste alcuna voce nel registro di sistema** che avvii un servizio malevolo, neanche nascosta. Infatti il rootkit non prevede alcuna modifica del registro di sistema per auto avviarsi.

Non esiste alcun file all'interno del sistema, o meglio nessun file visibile. Questo perché il rootkit salva il proprio driver negli ultimi settori disponibili dell'hard disk, settori che non sono utilizzati dal sistema e che non sono indicizzati dal file system. L'MBR rootkit accede a basso livello al disco rigido e scrive il proprio driver lì dove difficilmente è possibile trovarlo.

Non è possibile leggere il Master Boot Record alla ricerca dell'infezione. Il rootkit attivo in memoria, infatti, intercetta qualsiasi tentativo di lettura del MBR e ne restituisce la copia originale

```
Int13h_Hook:
xor     bx, bx
mov     eax, [bx+4Ch] ; get Original Int 13h Pointer
mov     es:old_Int13h, eax ; store it in a variable
mov     word ptr [bx+4Ch], offset hook ; hack pointer
mov     word ptr [bx+4Eh], es
push   es
push   offset loc_40 ; boot Hard Drive
```

pre-infezione, non il vero ed infetto MBR.

Questo rootkit, visto per la prima volta in-the-wild, è stato sviluppato partendo da un proof-of-concept, un codice-esempio **pubblicato online nel 2005 dalla società di sicurezza eEye.**

BootRoot, questo il nome del codice sviluppato dalla società, voleva essere una dimostrazione di come un rootkit potesse prendere il controllo del

sistema operativo partendo dal Master Boot Record.

Purtroppo, gli unici ad aver preso spunto da questo codice, sono stati i malware writer che ne hanno fatto una vera e propria fonte di guadagno.

MBR Rootkit, o Mebroot, è stato uno dei rootkit più proficui dell'anno. In sei mesi, secondo le ricerche effettuate dal **FraudAction Research Lab** di **RSA**, il malware ha collezionato i dati di login e altre informazioni private di circa **100.000 banche in tutto il mondo**, infettando centinaia di migliaia di PC.

Mebroot, comunque, non è stato l'unico rootkit a mettere in evidenza le lacune dei software di sicurezza.

A Maggio 2008 viene aperto il sipario su un nuovo e misterioso rootkit che aveva fatto parlare di sé nei mesi precedenti: **Rustock.C**.

La famiglia dei rootkit Rustock è conosciuta da molto tempo nel mondo della sicurezza informatica. **Rustock è stato uno dei rootkit più diffusi e, contemporaneamente, uno dei più tecnicamente avanzati.** Diviso in tre macro-varianti – A, B e C – ad ogni mutazione Rustock ha portato delle novità tecniche ogni volta capaci di ingannare gran parte dei software antirootkit.

Si parla nell'underground di Rustock.C da **Dicembre 2006**, di un nuovo rootkit capace di eludere gran parte degli antirootkit esistenti. I primi riscontri dell'esistenza arrivano a Novembre 2007 ma **il vero rootkit viene pubblicamente scoperto a Maggio 2008 dalla società russa Dr.Web.**

Un lasso di tempo particolarmente ampio durante il quale **il rootkit può aver infettato e reso parte di botnet un numero imprecisato di PC.** Non è la prima volta che il mondo della sicurezza informatica vede la diffusione *in sordina* di un'infezione. Il rootkit **Gromozon** ne è un esempio: diversi mesi di libera uscita prima che le società si accorgessero dell'esistenza del malware.

Rustock.C potrebbe essere facilmente considerato **uno dei rootkit più avanzati al momento tra i**

rootkit in the wild, cioè tra i rootkit diffusi online.

Il driver utilizza un **avanzato sistema di codifica che rende particolarmente arduo il compito di analizzarne il codice da parte dei ricercatori delle società di sicurezza.** L'intero corpo del malware è cifrato con l'algoritmo **RC4** e compresso con **aPlib**.

La chiave utilizzata per cifrare il codice è generata in maniera univoca per ogni PC infettato. I valori utilizzati per generare la chiave sono presi dal bus PCI. Grazie a questo speciale design **ogni copia generata di Rustock.C è in grado di funzionare esclusivamente sul PC per il quale è stata creata.**

Anche nel caso di Rustock.C **non esiste una voce all'interno del registro di sistema utilizzata per avviare il malware.** L'infezione è particolarmente subdola: il rootkit ha funzionalità di file infector, cioè **copia il suo codice all'interno di altri driver di sistema.** I driver attaccati sono i driver del sistema operativo presenti all'interno della voce

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Minimal
```

Il rootkit sposta l'infezione da un driver all'altro, ripulendo sempre il driver infetto e infettando il successivo, **evitando così che il codice del malware rimanga fisso su un unico driver.**



Qualunque tentativo di leggere il driver infetto risulterà in un nulla di fatto, **perché il rootkit filtra i file system driver fastfat.sys e ntfs.sys** mostrando ad ogni lettura il driver pulito dall'infezione.

Anche Rustock.C, come tutta la famiglia dei rootkit Rustock, è stato utilizzato per inviare spam. **Il PC infetto diventa uno zombie facente parte di una botnet.**

Il “vecchio” Rustock.B è stato tra i rootkit più diffusi, in parte responsabile anche della saturazione dei server DNS in Italia che ha causato la paralisi di gran parte della connettività italiana.

Ad oggi i sorgenti di Rustock.B sembrerebbero essere stati venduti e sono state isolate varianti più o meno modificate.

Sia con Rustock.C che con l’MBR Rootkit i malware writer hanno voluto mettere in evidenza come **le attuali misure di sicurezza siano insufficienti a contenere ed isolare gli attacchi.** Situazione sottolineata ulteriormente **all’Xcon conference 2008** questo Novembre dal ricercatore **Wenbing Zheng** che ha mostrato il proprio rootkit denominato **Tophet**, una sorta di evoluzione del MBR Rootkit.

Questi sono tuttavia solo alcuni esempi eclatanti. **Molti sono i malware che nel 2008 hanno fatto uso di tecnologie rootkit**, forti delle lacune dei software di sicurezza.

Srizbi, Storm, Rustock, Cutwail sono solo alcuni dei rootkit le cui relative botnet sono capaci di inviare **milioni di e-mail di spam** al giorno.

Di esempi di rootkit non convenzionali, basati su tecnologie di virtualizzazione o hardware-dipendenti, se ne è sentito molto parlare. **Bluepill, SubVirt, attacchi attraverso l’utilizzo di bug della CPU**, sono alcune delle possibili tipologie di attacco che, seppur al momento non sono utilizzate in attacchi su larga scala, memori del MBR Rootkit non ne è possibile escludere l’eventualità di un utilizzo futuro.

Certo è che, al momento, i malware writer non vedono la necessità di sviluppare questa tipologia di attacchi così sofisticati visto che **il parco giochi del sistema operativo è ancora particolarmente vasto e gran parte delle tecnologie antirootkit sono tristemente insufficienti a contenere gli attacchi.**

In altre parole, **il guadagno** - in termini di soldi - derivante dall’utilizzo delle tecnologie rootkit esistenti applicate ai malicious **software è ancora ottimo e non giustifica lo spostamento a nuove tipologie di attacchi** che prevedono, invece, notevoli conoscenze tecniche e uno sforzo di programmazione non indifferente.

TECNOLOGIA “IN-THE-CLOUD”

Il ritmo con cui nuovi codici maligni vengono rilasciati ogni giorno è un ritmo in incessante progressione. **Vengono isolati migliaia di nuovi malware al giorno**, un ritmo ingestibile per le società di sicurezza che si devono attrezzare con sistemi automatizzati di gestione dei sample per poter reggere l’ondata.

Prevenzione è la parola d’ordine per i software di sicurezza. **Prevenzione basata su tecnologie euristiche.** Tecnologie che necessitano continuamente di sviluppi, modifiche, per poter rendere al meglio.

Le applicazioni sono varie, tutte più o meno valide. Il 2008 è stato l’anno della diffusione delle tecnologie **in-the-cloud**. L’utilizzo di un database collettivo mondiale permette di tenere traccia in maniera molto più rapida ed efficace delle nuove minacce.

Le società di sicurezza configurano la propria “rete” mondiale, dove i client – i computer protetti dai software di sicurezza – non sono più esclusivamente fruitori del servizio, ma **diventano parte integrante e fondamentale della rete, delle sentinelle che permettono di tenere sotto controllo l’intero panorama internazionale.**

F-Secure DeepGuard 2.0, McAfee Artemis, Panda Collective Intelligence, Norton Community Watch percorrono la strada intrapresa già da alcuni anni da **Prevx**.

Ogni volta che un software viene eseguito, il client cerca nel proprio database online se il file è già conosciuto oppure no, e nel caso sia conosciuto come malevolo ne blocca immediatamente l’esecuzione.

Questa applicazione della tecnologia permette chiaramente di **non dover più aggiornare le basi virali, perché tutto il database è costantemente aggiornato online**. I risultati sono stati particolarmente interessanti: i prodotti che utilizzano tale tecnologia hanno visto incrementare il proprio detection rate di numerosi punti percentuale, eliminando così il *gap* che sussiste tra il rilascio di un nuovo malware e l'aggiunta di una firma virale.

Nell'ottica in cui l'attacco tipo è condotto attraverso un malware che muta molto rapidamente – un esempio sono gli installer del MBR rootkit – una tecnologia quale l'utilizzo di database collettivi online diventa quanto mai fondamentale per prevenire infezioni che poi risultano essere, altrimenti, difficili da rimuovere.

USO DI ACCOUNT LIMITATI

Grazie all'utilizzo sempre più diffuso di Windows Vista Microsoft ha re-implementato nella quotidianità l'uso dell'account limitato, tramite lo **User Account Control**. Una pratica chiaramente molto più sicura, soprattutto visto che, fino ad oggi, i sistemi Windows venivano per la gran parte installati e configurati per l'uso tramite account amministratore.

Una novità per molte delle persone che provenivano dalle versioni precedenti di Windows, niente di eclatante per gli utilizzatori di sistemi operativi alternativi quali Mac OS X e Linux.

L'utilizzo di un account limitato è **particolarmente efficace nella lotta contro i malicious software, poiché eventuali codici nocivi sarebbero limitati nell'azione dai controlli del sistema operativo** che ne impedirebbe danni a livello globale nel sistema.

Il limitare i danni grazie all'account limitato significa essere meno esposti agli attacchi di malware, ma **non significa essere totalmente al sicuro**. Sono diversi i punti su cui riflettere riguardo questo argomento.

Configurare un account limitato standard, così come è l'account creato in Windows Vista, significa essere **ancora vulnerabili ad eventuali attacchi di malware**.

Se è vero che limitare l'attacco al solo account dell'utente non permette al malware danni gravi al sistema, è pur sempre vero che **il malware è ancora in grado di poter intercettare le azioni dell'utente** – quindi catturarne informazioni quali ad esempio dati personali per l'accesso a servizi bancari. **È ancora in grado di poter installare rootkit user mode** all'interno del sistema per nascondere eventuali backdoor o trojan che possono comunicare con l'esterno e scaricare ulteriori infezioni.

Queste sono ancora azioni dannose per l'utente, dati sensibili e personali sono **merce preziosa** al mercato nero di Internet e sono venduti a caro prezzo.

Chiaramente, ed è un dato di fatto, **eventuali infezioni in atto all'interno di account limitati sarebbero molto più facilmente individuabili** da eventuali software di sicurezza che verrebbero eseguiti con diritti di amministratore. **Sempre che, ovviamente, all'utente venga il sospetto che il computer possa essere infetto** o si abbia già installato nel sistema un software di sicurezza.

Bisogna pur sempre dire che **è comunque possibile personalizzare l'account limitato** in modo tale da blindare totalmente il sistema – e quindi limitando nella quasi totalità dei casi qualunque tipo di azione di eventuali malware.

Se, tuttavia, questa pratica può essere applicata dagli utenti più esperti, un sistema operativo quale Microsoft Windows - che ha una diffusione in cifre maggiore all'80% - annovera tra i propri utenti una vasta gamma di persone, dai più esperti a coloro che utilizzano il PC per navigare ogni tanto, per leggere la posta elettronica e non si preoccupano minimamente di eventuali problemi relativi alla sicurezza.

Sorge il problema **del bilanciare correttamente sicurezza e semplicità d'uso**, fornire cioè un **compromesso** che possa garantire un certo

marginale di sicurezza e al contempo rende particolarmente facile l'utilizzo del prodotto da parte degli utenti. Uno sbilanciamento da una qualsiasi delle due parti rischia di danneggiare l'intero prodotto.

Sempre tenendo in considerazione il problema del social engineering, dell'ingegneria sociale, che è ancora la fonte principale di infezioni e contro la quale qualsiasi misura di sicurezza risulta inefficace.

EXPLOIT PADRONI DEL WEB

Già da qualche anno si è potuto notare un cambio di direzione nelle modalità con cui le infezioni vengono trasmesse.

Se tempo fa le e-mail, il peer to peer erano i mezzi principali di infezione, **ora il rischio viene dalle pagine web.**

Il 2008 ha visto il proliferare di tool pronti all'uso, script da caricare su server – preferibilmente su network difficilmente rintracciabili – contenenti exploit che vanno a colpire applicazioni vulnerabili.

Secondo alcune statistiche collezionate da **Secunia**, società di sicurezza che mantiene un database di vulnerabilità di applicazioni e sistemi operativi, **98 computer su 100 hanno installate vecchie versioni di programmi vulnerabili** ad alcune tipologie di attacchi. **Solo l'1.91% dei computer sono costantemente aggiornati** e, come tali, più difficilmente sono vittime di attacchi.

I malware writer sfruttano questa situazione, scrivendo exploit – codici utilizzati per attaccare le applicazioni vulnerabili – al fine di far eseguire codice nocivo senza che l'utente si accorga di niente.

14.1	144	205	MSIE
0.00	16	18	FFOX
0.00	4	6	OPERA
0.00	3	5	CHROME
0.00	3	3	OTHER

Se i principali target sono ovviamente i **browser**, non mancano applicazioni quali **Real Player**, **Acrobat Reader**, fino a immagini volutamente malformate per sfruttare bug del sistema operativo.

Toolkit quali **MPack**, **IcePack**, **Neosploit**, **WebAttacker** sono particolarmente diffusi e sono ancor più pericolosi considerando il fatto che, alle pagine web civetta opportunamente create per colpire gli utenti, **si aggiungono spesso siti web più o meno famosi compromessi**, nelle cui pagine vengono inseriti codici javascript offuscati utilizzati per reindirizzare l'utente ai server contenenti gli exploit.

MALWARE ATTACCANO MAC OS X

Al di là di Windows, il sistema operativo che al momento detiene oltre l'**80%** del mercato mondiale, ci sono molti altri sistemi operativi che non restano alla finestra a guardare Redmond.

Tra tutti, il **Mac OS X di Apple è quello che con più probabilità si è affacciato con grinta al mercato**, arrivando ad un buon **5%** che mette in evidenza come il sistema operativo di Cupertino sia considerato **uno delle alternative più valide** in ambito consumer.

Proprio a causa di questo crescente interessamento, anche i malware writer stanno lentamente ampliando il target anche a questo sistema operativo. È possibile vedere come durante il 2007 e il 2008 sia stato riscontrato un **notevole aumento di codici nocivi per il sistema operativo di Apple** e, seppur in numero esiguo e quasi irrilevante rispetto al concorrente Windows, **potrebbe comunque suonare come un preavviso di un possibile cambio di rotta.**

L'architettura su cui si basa Mac OS X, seppur altamente sicura, **soffre degli stessi problemi di cui soffre ora Windows Vista.**

Principalmente è necessario porre l'accento sull'ingegneria sociale, sulla **capacità dei malware writer di ingannare gli utenti facendo eseguire determinate applicazioni con diritti di amministratore.** Finti codec per film o musica

scaricati online, falsi software di sicurezza che fingono di riscontrare infezioni nel sistema e chiedendo poi di essere installati, software di controllo DRM necessari da installare per poter ascoltare un brano o visualizzare un video, crack per applicazioni varie. Le vie sono limitate esclusivamente dalla fantasia.

Con la crescente diffusione di Mac OS X, il sistema operativo di casa Cupertino **rischia di trovarsi ad affrontare gli stessi problemi che deve affrontare ora Microsoft Windows**, cioè l'aver una sempre più vasta gamma di utilizzatori, da chi sa veramente utilizzare il prodotto a chi non si preoccupa delle implicazioni a livello di sicurezza dell'eseguire o meno un software con diritti di amministratore. Con, ovviamente, tutte le conseguenze di eventuali scelte sbagliate.

La facilità con cui si riescono ad estorcere informazioni o convincere le persone a fare qualcosa di sbagliato è spesso disarmante.

A questo va aggiunto il rischio di exploit, di cui si è parlato precedentemente.

Mac OS X Leopard include una **protezione parziale** del sistema operativo ad attacchi provenienti da exploit.

La tecnologia DEP viene applicata solo allo stack lasciando vulnerabile l'heap, mentre **Windows Vista può applicare una protezione globale**. Inoltre, la tecnologia ASLR viene applicata in Windows Vista a tutti i processi ad ogni avvio del sistema. **Mac OS X applica invece l'ASLR solo in determinate occasioni**, solo quando la cache condivisa viene aggiornata, **senza però applicarlo a zone quali heap e stack**.

Mac OS X risulta tanto vulnerabile quanto Windows Vista ad attacchi derivanti da corruzione di memoria, in alcuni casi anche più vulnerabile. Apple dovrebbe correggere questa situazione con il rilascio di **Snow Leopard**.

Al momento esistono circa un centinaio di malware per Mac OS X e si stanno diffondendo software antivirus sia gratuiti che a pagamento.

È errato dire che al momento utilizzare Mac OS X significa essere esposti al rischio malware tanto quanto utilizzare Windows.

Sarebbe incosciente affermare, dopo attente riflessioni, che Mac OS X non abbia bisogno di software di sicurezza né che non rischi infezioni da malware come sta succedendo ora al sistema operativo concorrente Windows.

PAROLA D'ORDINE: PREVENZIONE

Con il **web 2.0**, anche gli attacchi si stanno adattando a questo nuovo *modus vivendi*. **Il web diventa sempre più un campo minato**, da affrontare con attenzione e con gli strumenti giusti.

L'unica vera arma possibile da utilizzare è la **prevenzione**, adottando tecnologie euristiche avanzate che possano bloccare sul nascere attacchi provenienti da exploit e da nuovi malware.

Come già visto, nel 2008 molte società hanno cominciato ad adottare tecnologie euristiche comunitarie. Inoltre, **le società tenderanno a sviluppare nuove tecnologie per la prevenzione di exploit**, un'emergenza sempre più prioritaria.

D'altro canto, il rischio che un malware venga attivato nel sistema **significa sempre più una caccia all'intruso nella quale l'intruso è purtroppo in posizione di vantaggio**, conoscendo spesso gli strumenti con i quali gli operatori di sicurezza analizzano i computer infetti. I rootkit del 2008 citati inizialmente ne sono un palese esempio.

Nel 2009 sarà possibile vedere con molta probabilità l'utilizzo crescente di tecniche di ingegneria sociale adattata ai **servizi di social network quali Facebook**, sempre più diffusi.

La probabilità di imbattersi in pagine web fittizie o compromesse, unita al fatto di non aggiornare i componenti software del pc, aumenterà il rischio di infezioni causate da toolkit pronti all'uso. E questa tipologia di attacchi rischia di essere lentamente portata anche in ambienti Mac OS X, dove c'è ancora molto da esplorare.

FONTI

Giuliani, M. (s.d.). *Master Boot Record Rootkit is here and ITW*. Tratto da Prevx:

<http://www.prevx.com/blog/75/Master-Boot-Record-Rootkit-is-here-and-ITW.html>

Gmer. (s.d.). *Stealth MBR rootkit*. Tratto da Gmer:
<http://www2.gmer.net/mbr/>

RSA. (s.d.). *One Sinowal Trojan + One Gang = Hundreds of Thousands of Compromised Accounts*. Tratto da RSA:
http://www.rsa.com/blog/blog_entry.aspx?id=1378

Dr.Web, L. (s.d.). *Win32.Ntldrbot (aka Rustock.C) no longer a myth, no longer a threat*. Tratto da Dr. Web, Ltd: <http://info.drweb.com/show/3342/en>

HolaHola. (s.d.). *Rustock.C*. Tratto da Rootkit:
<http://www.rootkit.com/newsread.php?newsid=879>

Shevchenko, S. (s.d.). *Rustock.C - Unpacking a Nested Doll*. Tratto da ThreatExpert:
<http://blog.threatexpert.com/2008/05/rustockc-unpacking-nested-doll.html>

Stewart, J. (s.d.). *Top Spam Botnets Exposed*. Tratto da Secure Works:
<http://www.secureworks.com/research/threats/top-botnets/?threat=topbotnets>

Prevx, L. (s.d.). *Prevx Launches Edge to Protect Against Criminal Software Which Bypasses Existing Anti-Virus Protection*. Tratto da MarketWire: <http://www.marketwire.com/press-release/Prevx-927601.html>

F-Secure. (s.d.). *F-Secure Leads Internet Security Industry in Developing 'In-The-Cloud' Technology*. Tratto da F-Secure: http://www.f-secure.com/f-secure/pressroom/news/fs_news_20081022_01_eng.html

Giuliani, M. (s.d.). *Is Limited User Account enough? Not really...* Tratto da Prevx, Ltd.:
<http://www.prevx.com/blog/83/Is-Limited-User-Account-enough-Not-really.html>

Giuliani, M. (s.d.). *Alcuni pensieri su Windows Vista*. Tratto da PC Al Sicuro:
<http://www.pcalsicuro.com/main/2007/01/alcuni-pensieri-su-windows-vista/>

Erasmus, J. (s.d.). *Fiesta 2.4 - Monitoring ITW exploit*. Tratto da Prevx, Ltd.:
<http://www.prevx.com/blog/107/Fiesta---Monitoring-ITW-exploit.html>

Giuliani, M. (s.d.). *You are sure your website isn't infected, aren't you?* Tratto da Prevx, Ltd.:
<http://www.prevx.com/blog/54/You-are-sure-your-website-isnt-infected-arent-you.html>

Balle, J. (s.d.). *1.91% of all PCs are fully patched!* Tratto da Secunia: <http://secunia.com/blog/37/>

Giuliani, M. (s.d.). *Internet Explorer 7 under 0day attack*. Tratto da PC Al Sicuro:
<http://www.pcalsicuro.com/main/2008/12/internet-explorer-7-under-0day-attack/>

Giuliani, M. (s.d.). *Mac OS X è totalmente sicuro?* Tratto da PC Al Sicuro:
<http://www.pcalsicuro.com/main/2008/12/mac-os-x-e-totalmente-sicuro/>

Giuliani, M. (s.d.). *The goal of antimalware products*. Tratto da Prevx, Ltd.:
<http://www.prevx.com/blog/109/The-goal-of-antimalware-products.html>

PCTools. (s.d.). *Threat List*. Tratto da iAntivirus:
<http://www.iantivirus.com/threats/>

Zovi, D. D. (s.d.). *Mac OS Xploitation*. Tratto da <http://conference.hitb.org/hitbsecconf2008kl/materials/D1T1%20-%20Dino%20Dai%20Zovi%20-%20Mac%20OS%20Xploitation.pdf>