# PROTEZIONE OFFERTA DAL BROWSER WEB

## PROTEZIONE DAL MALWARE DI INGEGNERIA SOCIALE

RISULTATI DEL TEST COMPARATIVO

EUROPA

Apple® Safari® 5
Google Chrome™ 10
Windows® Internet Explorer® 8
Windows® Internet Explorer® 9
Mozilla® Firefox® 4
Opera™ 11


VERSIONE DELLA METODOLOGIA: 1.2

MAGGIO 2011

L'accesso o l'utilizzo del presente report dipende da quanto segue:

1. Le informazioni fornite nel report sono soggette a modifiche senza preavviso da parte di NSS Labs.

2. Le informazioni contenute nel report sono considerate da NSS Labs accurate e affidabili al momento della pubblicazione, ma senza alcuna garanzia. La decisione di utilizzare o fare affidamento sul presente report è a esclusivo rischio dell'utente. NSS Labs non è responsabile per eventuali danni, perdite o spese derivanti da errori o omissioni presenti nel report.

3. NSS LABS NON FORNISCE ALCUNA GARANZIA, ESPRESSA O IMPLICITA. NSS LABS NON RICONOSCE ED ESCLUDE QUALSIASI GARANZIA IMPLICITA, INCLUSE QUELLE RELATIVE A COMMERCIABILITÀ, IDONEITÀ PER UNO SCOPO SPECIFICO E NON VIOLAZIONE. IN NESSUN CASO NSS LABS POTRÀ ESSERE RITENUTA RESPONSABILE PER DANNI CONSEQUENZIALI, INCIDENTALI O INDIRETTI O PER EVENTUALI PERDITE DI PROFITTO, RICAVI, DATI, PROGRAMMI DI COMPUTER O ALTRE RISORSE, ANCHE NELL'EVENTUALITÀ IN CUI SIA STATA AVVISATA DELLA POSSIBILITÀ DI TALE DANNO.

4. Il presente report non rappresenta un avallo, una raccomandazione o una garanzia per nessuno dei prodotti (hardware o software) sottoposti a test o per l'hardware e il software utilizzati per testare i prodotti. I test non garantiscono l'assenza di errori o difetti nei prodotti o che questi soddisfino le aspettative, i requisiti, le esigenze o le specifiche dei clienti o che assicurino un funzionamento privo di interruzioni.

5. Il presente report non implica alcun avallo, sponsorizzazione, affiliazione o verifica da parte o in collaborazione con nessuna delle organizzazione citate nel presente report.

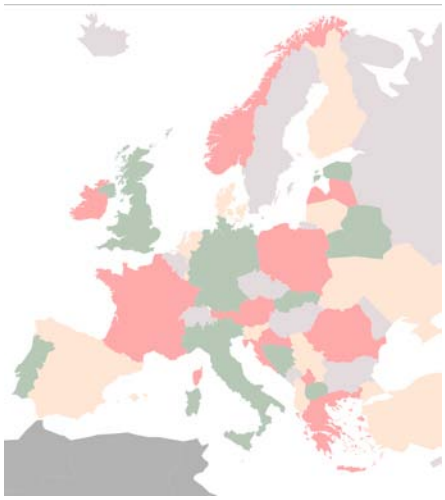
6. Tutti i marchi, i marchi di servizio e le denominazioni commerciali utilizzati nel presente report sono marchi, marchi di servizio e denominazioni commerciali dei rispettivi proprietari.

## INFORMAZIONI DI CONTATTO

**NSS Labs, Inc.**
P.O. Box 130573
Carlsbad, CA 92013 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com

# SOMMARIO RIEPILOGATIVO

## *Test della regione europea*



Nell'aprile 2011, NSS Labs ha effettuato il primo test sulla protezione offerta dai browser Web contro il malware di ingegneria sociale rivolto contro gli utenti europei.[1] Tale malware continua a rappresentare la minaccia più comune alla protezione che gli utenti di Internet devono affrontare. Studi recenti dimostrano che per gli utenti è quattro volte più probabile essere convinti a scaricare malware che rimanere coinvolti in un exploit.[2]

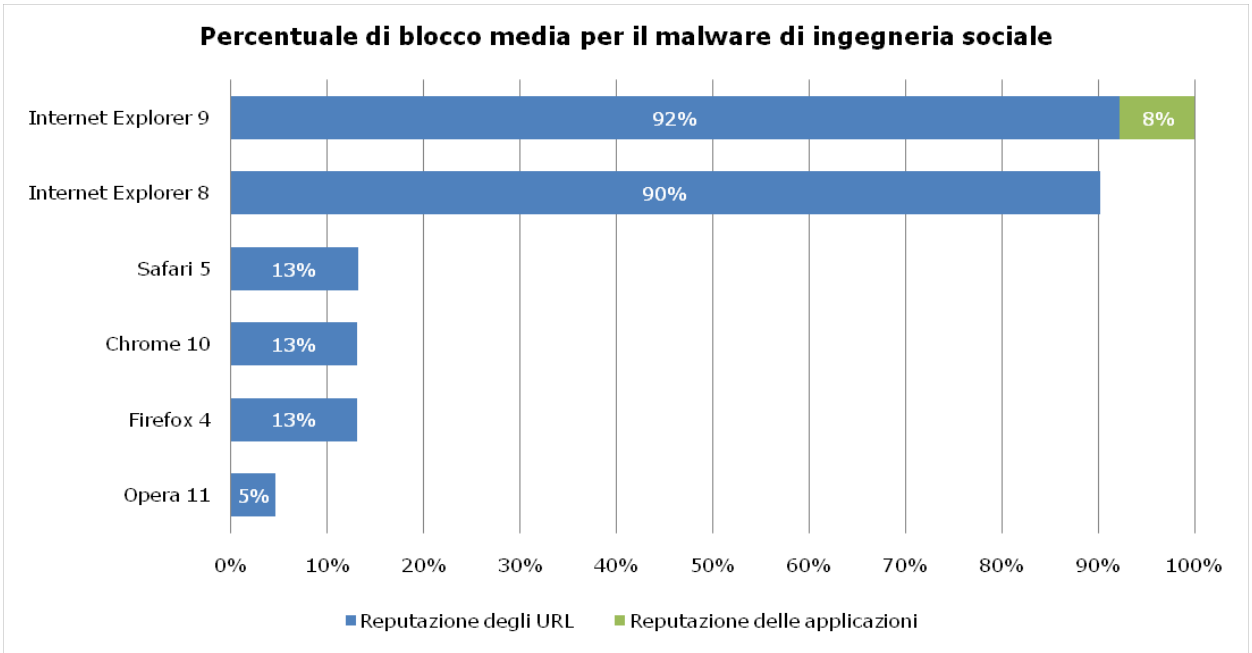
Negli ultimi 12 mesi, gli utenti europei si sono trasformati nel bersaglio degli autori di malware. Nel 2010, gli esperti in ricerche sulle minacce hanno rilevato la presenza di nuove varianti di ZBOT specificamente dirette contro i sistemi bancari di quattro paesi europei. Le aziende coinvolte, che possiedono una clientela di alto profilo, includevano la Banca di Roma del Gruppo UniCredit; la Abbey National nel regno Unito; il gruppo HSBC di Hong Kong; il gruppo FIDUCIA, il più importante provider di servizi IT tedesco nel sistema finanziario cooperativo, e una delle principali banche commerciali francesi, il Crédit Mutuel.

Secondo l'Eurostat, l'ufficio statistico dell'UE, nel 2010 quasi un terzo degli utenti di Internet dell'Unione europea è stato vittima di infezioni malware, sebbene la maggior parte di essi disponesse di un software per la protezione installato. Dei 27 paesi dell'UE coinvolti nella ricerca (per un totale di oltre 200.000 utenti), i più colpiti dalle infezioni malware sono risultati Bulgaria (58%), Slovacchia (47%), Ungheria (46%), Italia (45%) ed Estonia (43%).

Il presente report riguarda gli URL ritenuti particolarmente pericolosi per gli utenti UE ed è basato sulla stessa metodologia Live Testing dei test globali condotti nel primo e terzo trimestre 2009 e nel primo e terzo trimestre 2010 (www.nsslabs.com/browser-security). Il report contiene prove convalidate empiricamente raccolte durante 19 giorni di test eseguiti tutti i giorni, 24 ore su 24, ogni sei ore e suddivisi in 76 diversi cicli di test, ognuno con nuovi URL malware. Ogni prodotto è stato aggiornato alla versione più recente disponibile al momento dell'inizio del test e ha potuto accedere a Internet live.

[1] Nota: questo studio non ha valutato la protezione offerta dai browser in termini di vulnerabilità relative ai plug-in o ai browser stessi.
[2] http://www.virusbtn.com/conference/vb2010/abstracts/Hughes.xml

Questo report è stato creato come parte dei servizi di informazione del test indipendente di NSS Labs. I principali fornitori sono stati invitati a partecipare a titolo gratuito e NSS Labs non ha ricevuto alcun finanziamento per creare tale report.




La protezione del filtro SmartScreen offerta da Windows Internet Explorer 9 si basa su due componenti: reputazione degli URL, inclusa anche in IE8, e reputazione delle applicazioni, introdotta in IE9. IE9 ha rilevato un eccezionale 92% di minacce live con la reputazione degli URL SmartScreen e un ulteriore 8% con la reputazione delle applicazioni. IE9 con SmartScreen offre la migliore protezione contro il malware di ingegneria sociale rispetto a qualsiasi altro browser. La protezione dal malware rivolto contro gli utenti europei ha eguagliato i risultati più completi ottenuti dal test globale del terzo trimestre 2010.

**Windows Internet Explorer 8** ha individuato il 90% delle minacce live, una percentuale straordinaria, corrispondente ai risultati più completi ottenuti dal test globale del terzo trimestre 2010.

**Apple Safari 5** ha identificato il 13% delle minacce live. La protezione offerta era quasi identica a quella di Chrome e Firefox.

**Mozilla Firefox 4** ha rilevato il 13% delle minacce live, un livello decisamente inferiore a quello di Internet Explorer 8 o Internet Explorer 9, con un calo del 6% rispetto alla percentuale di protezione del 19% osservata durante il test globale del terzo trimestre 2010. Questo indica una minore protezione complessiva da parte di Firefox o una vulnerabilità regionale in Europa.

**Google Chrome 10** ha individuato il 13% delle minacce live, decisamente superiore al 3% ottenuto nel test globale del terzo trimestre 2010, dimostrando un considerevole miglioramento.

**Opera 11** ha identificato il 5% delle minacce live, offrendo per la prima volta una protezione apprezzabile dal malware di ingegneria sociale.

# SOMMARIO

# 1 INTRODUZIONE

## 1.1 LA MINACCIA DEL MALWARE DI INGEGNERIA SOCIALE

Gli attacchi di malware di ingegneria sociale rappresentano un notevole rischio per individui e organizzazioni, poiché minacciano di compromettere, danneggiare o acquisire informazioni riservate personali e aziendali. Le statistiche del 2008-2010 dimostrano che si tratta di una tendenza in rapido espansione. Secondo un recente studio condotto da AVG, per gli utenti è quattro volte più probabile essere convinti a scaricare malware che rimanere coinvolti in un exploit.[3] Rilevare e prevenire queste minacce continua a rappresentare una sfida, poiché i criminali utilizzano sempre più il malware come vettore di attacchi informatici. Gli esperti in ricerche antivirus rilevano tra 15.000 e 50.000 nuovi programmi dannosi al giorno. Secondo Kaspersky Lab, ne vengono individuati persino "milioni al mese".[4]

Sebbene non tutti questi programmi dannosi siano attacchi di ingegneria sociale, al Web viene sempre più applicata la tecnica di distribuire rapidamente il malware e di evitare così i programmi di protezione tradizionali. Secondo le statistiche di Trend Micro, attualmente il 53% del malware viene diffuso per mezzo di download Internet, rispetto a solo il 12% tramite posta elettronica.[5]

Dal punto di vista dei cybercriminali, convincere ingannevolmente gli utenti a scaricare e installare malware è un tipo di attacco ottimale, perché il punto debole sfruttato è l'ingenuità delle vittime. L'assenza di dipendenze tecnologiche consente di colpire un più alto numero di utenti. Per gli attacchi drive-by è invece necessario che il computer dell'utente sia vulnerabile all'exploit utilizzato.

I criminali traggono vantaggio dalle relazioni di fiducia implicita che caratterizzano i siti di social networking (Facebook®, MySpace™, Badoo, StudiVZ, Skyrock, LinkedIn® e così via) e dai contenuti forniti dagli utenti (blog, Twitter™, ecc.), che consentono una pubblicazione rapida e garantiscono l'anonimato. La velocità di diffusione di queste minacce rappresenta una sfida complessa anche per i fornitori di soluzioni di protezione.

Per maggiore chiarezza, per gli URL di malware di ingegneria sociale si utilizza la seguente definizione: **collegamento presente in una pagina Web da cui si accede direttamente a un download che consente di scaricare un payload dannoso o, più in generale, un sito Web noto per ospitare collegamenti al malware.** Questi download, ad esempio applicazioni screen saver, aggiornamenti di codec video e così via, sono apparentemente sicuri e sono progettati in modo da convincere l'utente ad agire. I professionisti del settore della protezione definiscono queste minacce anche download "consensuali" o "pericolosi".

[3] http://www.virusbtn.com/conference/vb2010/abstracts/Hughes.xml
[4] Kaspersky, Eugene in http://www.examiner.com/x-11905-SF-Cybercrime-Examiner~y2009m7d17-Antimalware-expert-and-CEO-Eugene-Kaspersky-talks-about-cybercrime.
[5] Cruz, Macky "Most Abused Infection Vector". *Blog Trend Labs sul malware*, 7 dicembre 2008. http://blog.trendmicro.com/most-abused-infection-vector/

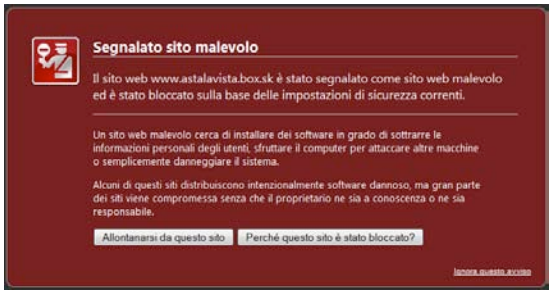
## 1.2 PROTEZIONE OFFERTA DAL BROWSER WEB

I browser Web moderni forniscono un **ulteriore livello di protezione** da queste minacce utilizzando i meccanismi basati sulla reputazione presenti nel cloud per avvisare gli utenti. Questo report esamina la capacità di sei diversi browser Web di proteggere gli utenti dal malware di ingegneria sociale.[6] Ognuno di questi browser possiede tecnologie di protezione aggiunte per contrastare le minacce basate sul Web, ma non tutti hanno adottato lo stesso approccio né dichiarano di coprire la stessa area della superficie di attacco.

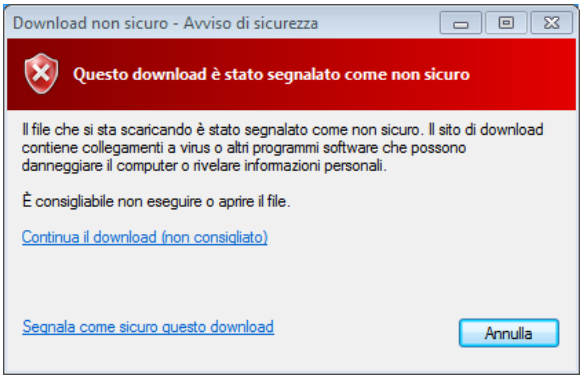
La protezione offerta dal browser prevede due componenti principali. Le fondamenta sono costituite da un sistema basato sulla reputazione e presente nel cloud, che cerca in Internet i siti Web dannosi e ne suddivide i contenuti in categorie. I siti vengono quindi aggiunti a una lista nera o a una lista bianca oppure viene loro assegnato un punteggio (a seconda dell'approccio adottato dal fornitore). Questa suddivisione può essere eseguita manualmente, automaticamente o in entrambi i modi. Alcuni fornitori utilizzano il feedback proveniente dagli agenti degli utenti sugli endpoint dei rispettivi clienti per segnalazioni automatiche al sistema di reputazione, fornendo informazioni importanti per l'attendibilità o, altrimenti, di applicazioni e file scaricati da Internet. La seconda componente funzionale risiede nel browser Web e richiede ai sistemi presenti nel cloud informazioni di reputazione su URL specifici, per poi attivare funzioni di avviso e blocco.

Quando i risultati indicano un sito "pericoloso", il browser Web reindirizza l'utente su un messaggio di avviso o una pagina in cui viene segnalato che l'URL è dannoso. Nel caso in cui l'URL porti a un download, il browser Web indica all'utente che il contenuto è dannoso e che il download deve essere annullato. Se, invece, il sito è considerato "innocuo", il browser Web non intraprende alcuna azione e l'utente non si rende nemmeno conto che è stato eseguito un controllo di sicurezza.

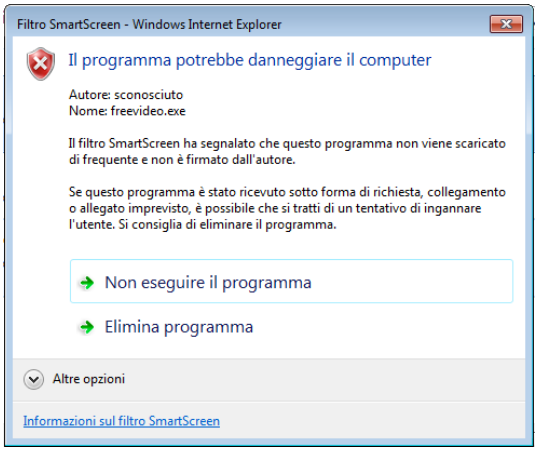
[6] Gli exploit che installano il malware all'insaputa dell'utente (chiamati anche "clickjacking" e "download drive-by") non sono stati inclusi in questo studio specifico.




*Avviso di Firefox 4*




*Avviso di Internet Explorer 8*




*Avviso di reputazione dell'applicazione di IE 9*

# 2 RISULTATI RELATIVI ALL'EFFICACIA

## 2.1 COMPOSIZIONE DEL TEST: URL DANNOSI

I dati di questo report sono stati raccolti durante un periodo di test di 19 giorni, dal 3 al 22 aprile 2011. I PC utilizzati per i test erano connessi a Internet da diverse località europee ed è stato verificato che in ognuno fossero installati i Language Pack appropriati. Nel corso del test, la connettività è stata costantemente monitorata per controllare che i browser, e relativi servizi di reputazione presenti nel cloud, potessero accedere ai siti Internet live oggetto del test. Durante l'intero studio sono stati eseguiti 76 diversi test (uno ogni sei ore) senza interruzione per ciascuno dei sei browser.

Poiché un fattore essenziale era la disponibilità di siti sempre nuovi, il numero di siti valutati è stato superiore a quello dei siti inseriti nel set di risultati. La metodologia di test comparativo di NSS Labs per la protezione dal malware di ingegneria sociale fornisce ulteriori dettagli sugli URL studiati e utilizzati per il set di risultati.

Gli URL dannosi inclusi nel test erano ritenuti una minaccia per gli utenti europei, ovvero individui residenti in paesi europei, tra cui: Austria, Belgio, Danimarca, Francia, Finlandia, Germania, Grecia, Irlanda, Italia, Norvegia, Paesi Bassi, Polonia, Portogallo, Russia, Spagna, Svezia, Svizzera, Regno Unito, Turchia e Ungheria. Tuttavia, anche se l'obiettivo è un utente in Europa, il dominio in cui il malware risiede può trovarsi in qualsiasi parte del mondo. D'altra parte, anche se un URL dannoso risiede in un dominio europeo, non significa che sia destinato a colpire solo utenti europei. Il fattore determinante per stabilire se inserire o meno nel test un URL dannoso è stata la partecipazione a una campagna di malware rivolta contro gli utenti europei. Infine, la sola inclusione in una campagna contro utenti europei non implica che l'URL dannoso non sia stato utilizzato anche in diverse campagne contro utenti di altre regioni.

### 2.1.1 NUMERO TOTALE DI URL DANNOSI INCLUSI NEL TEST

Da un elenco iniziale di 5.000 nuovi siti sospetti, ai fini dell'inclusione sono stati pre-analizzati 706 URL potenzialmente dannosi e disponibili al momento dell'inizio del test. Questi sono stati visitati dai browser durante almeno un ciclo. I campioni che non soddisfacevano i criteri di convalida, inclusi quelli contenenti adware o che non contenevano malware valido, sono stati rimossi. Infine, i 650 URL che hanno superato il processo successivo alla convalida sono stati inseriti tra i risultati, assicurando un margine di errore del 3,84% con un intervallo di confidenza del 95%.

### 2.1.2 NUMERO MEDIO DI URL DANNOSI INCLUSI OGNI GIORNO

Ogni giorno sono stati aggiunti mediamente al set di test 34 nuovi URL. In alcuni giorni, tuttavia, il numero di siti aggiunti al test poteva essere inferiore o superiore, a seconda delle fluttuazioni delle attività criminali.

### 2.1.3 COMBINAZIONE DI URL

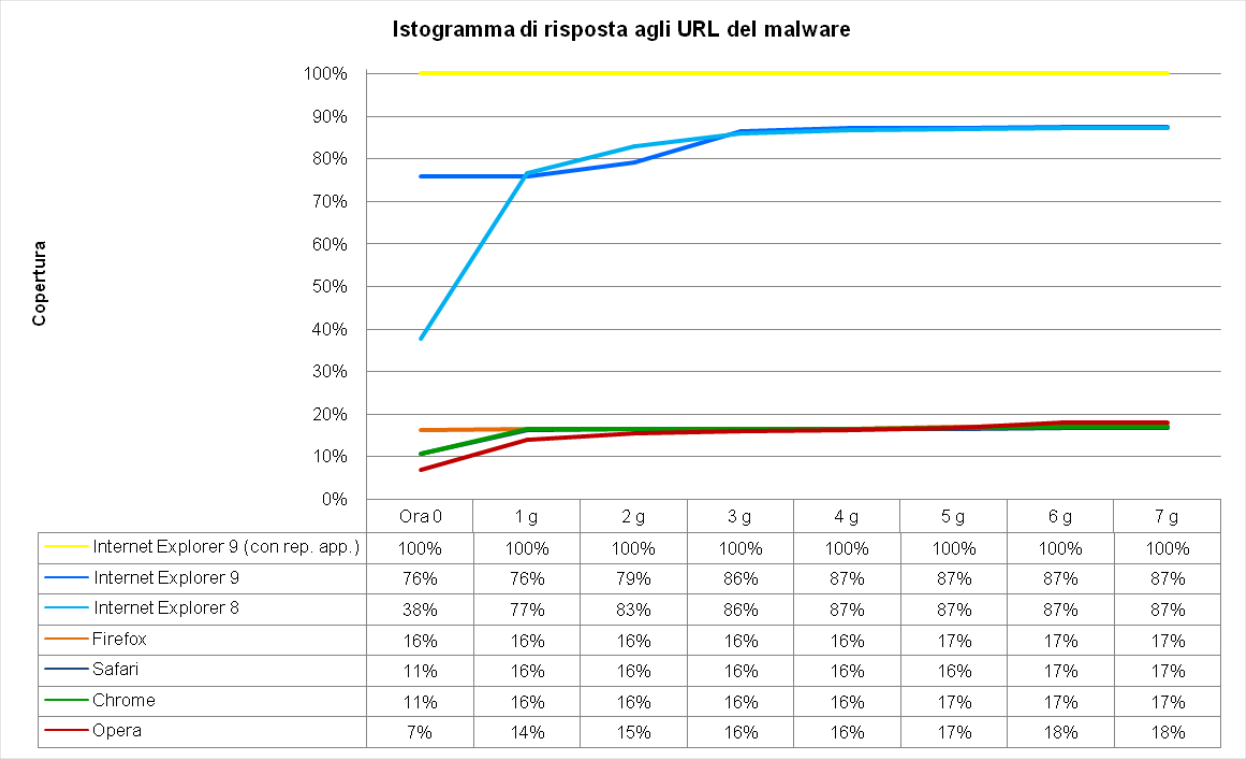
La combinazione di URL utilizzati nel test era rappresentativa delle minacce presenti in Internet dal punto di vista di un utente europeo. È stata prestata attenzione a non far prevalere alcun dominio, in modo che ognuno costituisse non più del 10% del set di test. Di conseguenza, una volta raggiunto questo limite, numerosi siti sono stati eliminati.

## 2.2 BLOCCO DEGLI URL CON MALWARE DI INGEGNERIA SOCIALE

NSS Labs ha valutato la capacità dei browser di bloccare gli URL dannosi con la stessa rapidità con cui venivano individuati in Internet. I browser sono stati sottoposti a test ogni sei ore per determinare quanto tempo occorreva al fornitore per aggiungere la necessaria protezione.

### 2.2.1 TEMPO MEDIO RICHIESTO PER BLOCCARE SITI DANNOSI

Il grafico dei tempi di risposta riportato di seguito indica il tempo occorso ai browser partecipanti al test per bloccare la minaccia introdotta nel ciclo di test. Sono indicate le percentuali di protezione complessive per l'"ora zero" e quindi i singoli giorni fino al blocco. I punteggi di protezione finali ottenuti nel test degli URL sono riepilogati nella colonna "Totale".



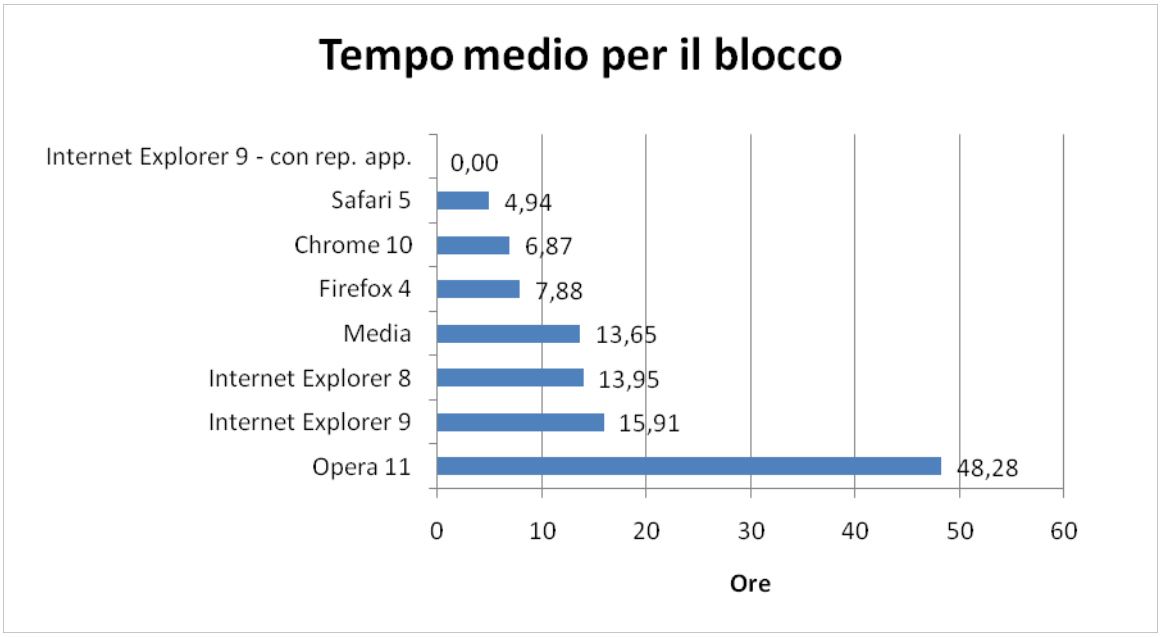

| | Ora 0 | 1 g | 2 g | 3 g | 4 g | 5 g | 6 g | 7 g |
|---|---|---|---|---|---|---|---|---|
| Internet Explorer 9 (con rep. app.) | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| Internet Explorer 9 | 76% | 76% | 79% | 86% | 87% | 87% | 87% | 87% |
| Internet Explorer 8 | 38% | 77% | 83% | 86% | 87% | 87% | 87% | 87% |
| Firefox | 16% | 16% | 16% | 16% | 16% | 17% | 17% | 17% |
| Safari | 11% | 16% | 16% | 16% | 16% | 16% | 17% | 17% |
| Chrome | 11% | 16% | 16% | 16% | 16% | 17% | 17% | 17% |
| Opera | 7% | 14% | 15% | 16% | 16% | 17% | 18% | 18% |

I risultati rivelano notevoli variazioni nella capacità dei diversi browser di assicurare protezione contro il malware di ingegneria sociale. Le tendenze mostrano differenze minime tra Chrome, Firefox e Safari, tutti con una percentuale di protezione del 17%. Il dato non sorprende, poiché tutti e tre condividono il feed Google Safe Browser e hanno avuto il tempo di appianare le precedenti differenze nelle varie implementazioni dei singoli browser.

### 2.2.2 TEMPI DI RISPOSTA MEDI PER BLOCCARE IL MALWARE

Per proteggere la maggior parte degli utenti, il sistema di reputazione del browser deve essere sia veloce che preciso. La tabella riportata di seguito risponde alla domanda su quanto un utente deve attendere prima che un sito dannoso visitato sia aggiunto all'elenco di blocco. Mostra inoltre il tempo medio necessario per bloccare un sito di malware dopo che questo è stato inserito nel set di test, *ma solo se è stato bloccato durante l'esecuzione del test stesso*. I siti non bloccati non sono inclusi, poiché non esiste un metodo matematico che consente di assegnare il punteggio "mai".

Questa tabella risulta utile poiché fornisce un contesto per la *percentuale di blocco complessiva*, ovvero se un browser blocca il 100% del malware, ma per compiere l'operazione impiega 216 ore (9 giorni), in realtà fornisce una protezione minore rispetto a un browser con una percentuale di blocco complessiva del 70%, ma con un tempo di risposta medio di 24 ore.

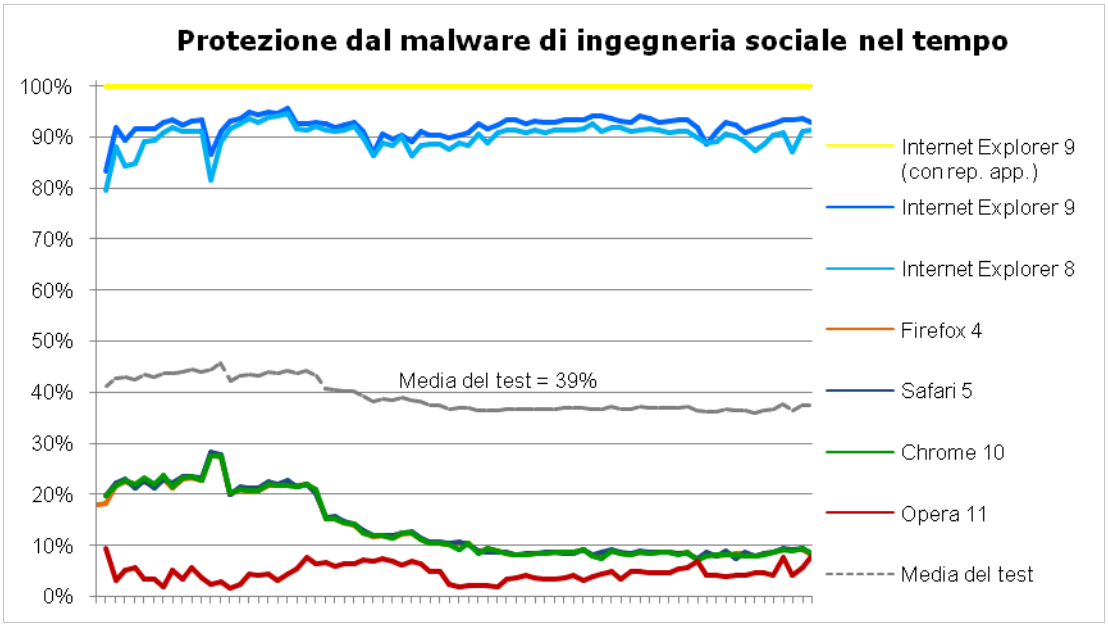



In media, il tempo necessario per bloccare un sito (se viene bloccato) è di 13,7 ore. Di conseguenza, in termini di aggiunta di nuovi blocchi, IE9 (con reputazione delle applicazioni), Safari, Chrome e Firefox si sono dimostrati al di sopra della media. Tutti i browser hanno bloccato almeno un download di malware.

## 2.3 Blocco degli URL con malware di ingegneria sociale nel tempo

I parametri utilizzati per il blocco dei singoli URL rappresentano solo uno dei punti di vista. In termini di scenari di utilizzo quotidiano, gli utenti visitano un'ampia gamma di siti, che può cambiare rapidamente. È quindi possibile che, in un determinato momento, il set di URL dannosi disponibile si evolva e continuare a bloccare tali siti diventa un criterio essenziale per l'efficacia. Di conseguenza, NSS Labs ha sottoposto a test tutti gli URL live ogni sei ore. Le tabelle e i grafici riportati di seguito illustrano le ripetute valutazioni di blocco nel corso di 19 giorni, con 76 cicli di test per ognuno dei sei browser. Ogni punteggio indica la protezione in un determinato momento.

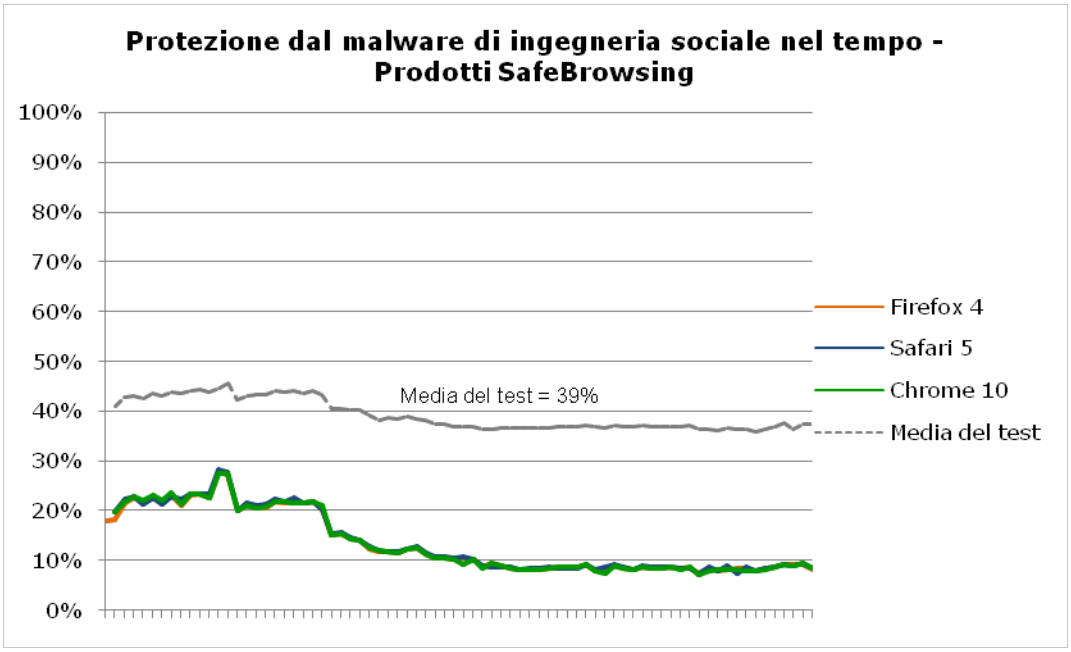
Come illustrato nel grafico, Internet Explorer sia 8 che 9 hanno dimostrato un livello di protezione estremamente elevato. Safari, Firefox e Chrome hanno ottenuto risultati uniformi, sebbene a un livello decisamente inferiore.




La percentuale di protezione media devia dai risultati dei singoli URL per diversi motivi. Innanzitutto, questi dati includono più test di un solo URL, quindi se un URL viene bloccato tempestivamente, il punteggio aumenta. Se invece continua a essere disponibile, il punteggio diminuisce. Di conseguenza, i risultati dei test individuali degli URL devono essere considerati ed esaminati in base al tempo.

## 2.4 PRODOTTI PER UN'ESPLORAZIONE SICURA

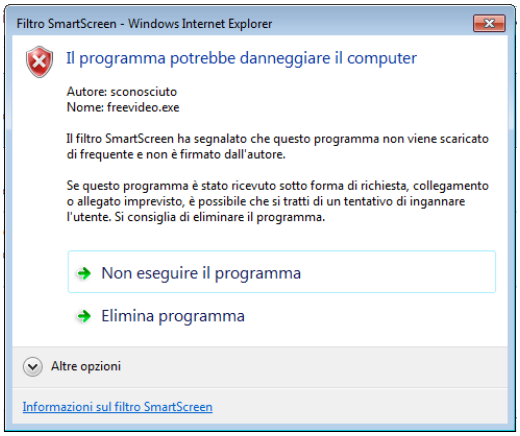
Chrome, Firefox e Safari utilizzano tutti il feed di dati di Google Safe Browsing. I test eseguiti hanno rilevato che tutti e tre i browser offrono un livello di protezione quasi identico contro gli URL malware di ingegneria sociale.



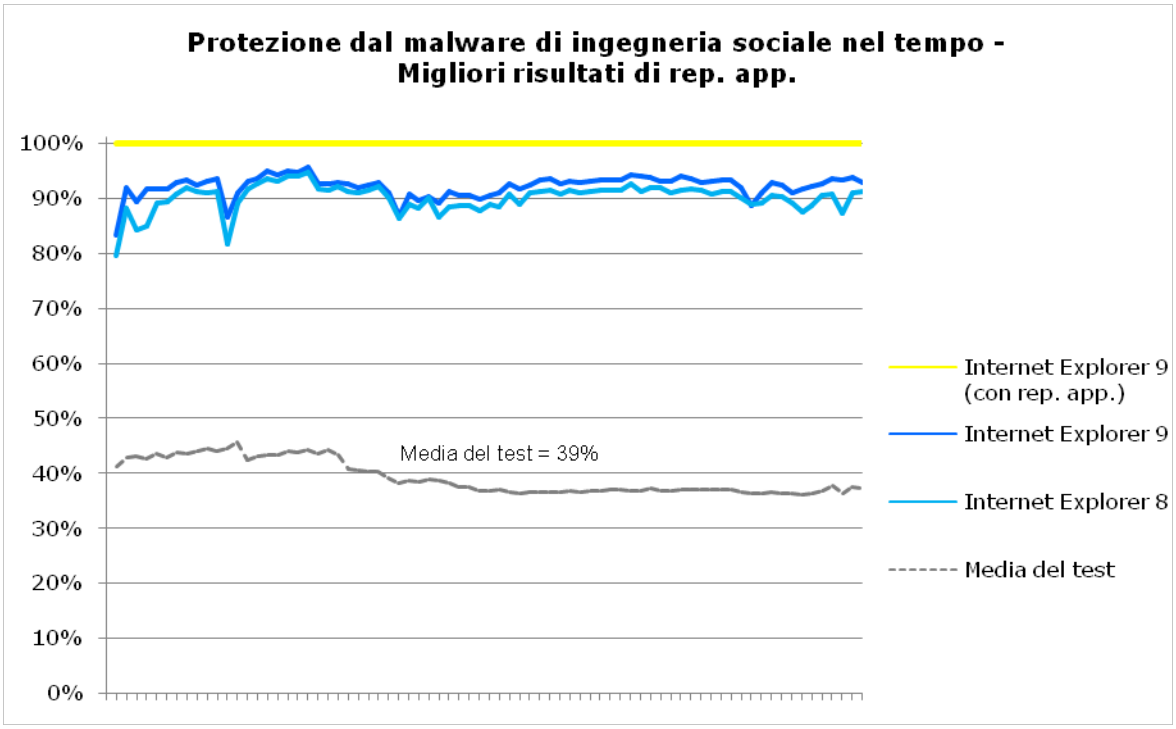

Come citato nella Sezione 2.2.1 e indicato nell'istogramma di risposta agli URL malware, le percentuali di protezione fornite dai prodotti per l'esplorazione sicura sono quasi identiche e dimostrano di convergere mediamente al 17% circa. In effetti, la protezione offerta dai tre browser era in sintonia reciproca, con aumenti e cali analoghi. Questo supporta la convinzione che gli elenchi di blocco di Chrome, Firefox e Safari siano uguali (o molto simili).

## 2.5 IE9 E REPUTAZIONE DELLE APPLICAZIONI DI MICROSOFT

Internet Explorer 9 ha dimostrato un miglioramento del 10% rispetto alla versione 8. L'aggiunta più importante a Internet Explorer 9 è il sistema di reputazione delle applicazioni, che contribuisce per circa l'8% alla protezione aggiuntiva. Questa nuova funzionalità consente agli utenti di distinguere il malware e il software potenzialmente pericoloso dal software innocuo.




Il valore essenziale offerto dalla reputazione delle applicazioni è la capacità di aggiungere contesto, per spingere gli utenti a chiedersi se l'origine del download sia attendibile o meno.




Come dimostrato dai risultati, l'aggiunta della tecnologia di reputazione delle applicazioni potenzia il livello di protezione di Internet Explorer 9 di un ulteriore 8% su 100%.

# 3 CONCLUSIONI

Il malware di ingegneria sociale è un problema diffuso, che colpisce circa un terzo degli utenti europei. L'utilizzo di sistemi di reputazione gratuiti basati su browser per contrastare con maggiore efficacia il malware di ingegneria sociale si basa sull'adozione di tecnologie cloud. Tuttavia, questo test del malware di ingegneria sociale rivolto contro gli utenti dell'UE ha rilevato che non tutte le operazioni quotidiane e le implementazioni dei fornitori conducono agli stessi risultati.

| Test globale trimestre 3 2010 | Bloccato |
|---|---|
| | |
| | |
| Internet Explorer 9 | 99% |
| Internet Explorer 8 | 90% |
| Firefox 3.6.15 | 19% |
| Chrome 6 | 3% |
| Safari 5 | 11% |
| Opera 10 | 0% |

| Test Europa trimestre 2 2011 | Bloccato |
|---|---|
| Internet Explorer 9 (rep. app.) | 8% |
| Internet Explorer 9 | 92% |
| Internet Explorer 9 (TOTALE) | 100% |
| Internet Explorer 8 | 90% |
| Firefox 4 | 13% |
| Chrome 10 | 13% |
| Safari 5 | 13% |
| Opera 11 | 5% |

| Cambiamento |
|---|
| N/D |
| N/D |
| 1% |
| 0% |
| -6% |
| 10% |
| 2% |
| 5% |

Questo test incentrato sull'Europa e i confronti eseguiti con i precedenti test globali condotti da NSS Labs hanno dimostrato che Microsoft continua a migliorare la protezione offerta da IE contro il malware sia in **Internet Explorer 8** (grazie alla tecnologia del filtro SmartScreen®) che in **Internet Explorer 9** (con l'aggiunta della tecnologia SmartScreen di reputazione delle applicazioni). Con SmartScreen attivato e la reputazione delle applicazioni disattivata, IE9 ha raggiunto l'eccezionale percentuale di 89% di blocco degli URL e un livello di protezione nel tempo pari al 92%. L'attivazione della reputazione delle applicazioni insieme a SmartScreen ha aumentato la percentuale di blocco degli URL di Internet Explorer 9 dell'11% (su 100%) all'ora zero e il livello di protezione nel tempo dell'8% (su 100%). Internet Explorer 9 si è nettamente distinto nella protezione contro il malware di ingegneria sociale già prima dell'attivazione della reputazione delle applicazioni insieme a SmartScreen.

Il significato della nuova tecnologia di reputazione delle applicazioni di Microsoft non può essere esagerato. La reputazione delle applicazioni costituisce il primo tentativo di un fornitore di stilare un elenco definitivo di tutte le applicazioni presenti su Internet. L'elenco viene creato e gestito dinamicamente, proprio come Google (o Bing) continua ad ampliare e amministrare una raccolta di contenuti per la ricerca.

**Firefox 4** ha ottenuto una percentuale di protezione del 13%, pari alla protezione offerta da Chrome e Safari, inferiore dell'86% a quella fornita da Internet Explorer 9 e del 77% da quella di Internet Explorer 8. Rispetto al test globale del terzo trimestre 2010, Firefox ha mostrato un peggioramento del livello di protezione che può essere attribuito all'implementazione dell'API v2 per l'esplorazione sicura o alle nuove tattiche utilizzate dai cybercriminali non ancora note al servizio. È stato rilevato un lieve miglioramento dell'1% tra la protezione dell'ora zero (16%) e la protezione finale del giorno 19 (17%).

**Safari 5** ha ottenuto una percentuale di protezione del 13%, pari alla protezione offerta da Firefox e Chrome, con una convergenza a circa il 17% dopo 19 giorni. Tuttavia, rispetto a Firefox, Safari ha presentato un notevole sfasamento nella protezione, con l'11% all'ora zero contro il 16% di Firefox.

Con una percentuale del 13%, **Chrome 10** ha offerto un livello di protezione praticamente identico a Safari e Firefox.

La percentuale di blocco complessiva di **Opera 10**, pari al 5%, si è mantenuta sempre la più bassa del gruppo. Tuttavia, si è verificato un miglioramento rispetto allo 0% ottenuto nei test globali precedenti, da attribuire probabilmente alla collaborazione dell'azienda con la società antivirus AVG.

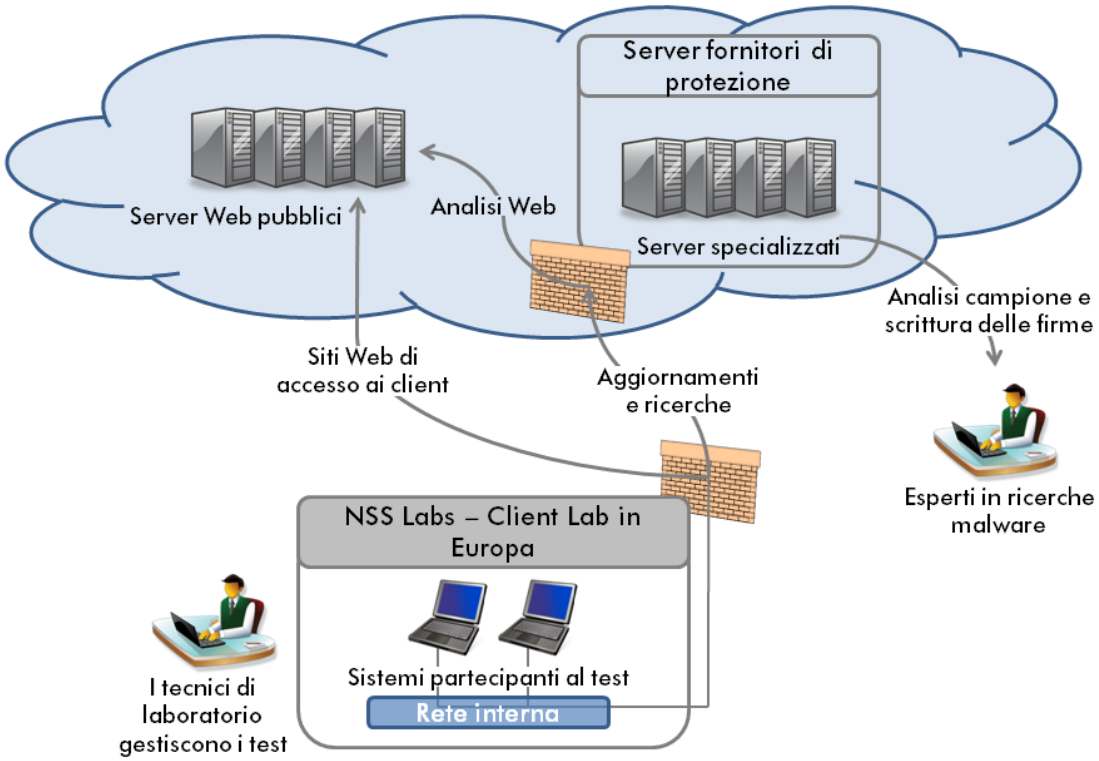
I browser forniscono un livello di protezione contro il malware di ingegneria sociale che si aggiunge ai prodotti per la protezione degli endpoint. Come dimostrato da questo report, non tutti sono uguali. La ridotta protezione complessiva fornita da Firefox, Safari e Chrome è preoccupante. Per ottenere un livello di protezione elevato, gli utenti di Internet Explorer dovrebbero effettuare quanto prima l'aggiornamento a Internet Explorer 9. Infine, è consigliabile che gli utenti si accertino di disporre sempre degli aggiornamenti più recenti di sistema operativo e browser.

# 4 AMBIENTE DI TEST

NSS Labs ha creato una metodologia e un ambiente di test complessi per valutare le capacità di protezione dei browser Internet in condizioni più reali possibili, continuando tuttavia a gestire il controllo e la verifica delle procedure.

Per questo test della protezione offerta dai browser, NSS Labs ha creato un ambiente di test "live" in grado di riprodurre le esperienze dell'utente in condizioni reali.

NSS Labs – Framework del test Live in-the-Cloud




## 4.1 DESCRIZIONE DELL'HOST DEL CLIENT

Tutto il software dei browser sottoposti al test è stato installato in macchine virtuali identiche con le seguenti specifiche:

- Microsoft Windows 7
- Language Pack appropriato, applicato in base all'utente emulato (ad esempio, francese, italiano, spagnolo, tedesco e così via)
- 1 GB di RAM
- 20 GB di spazio sul disco rigido

I sistemi in cui i browser erano installati sono stati controllati prima e durante il test, allo scopo di accertarne il corretto funzionamento. Ai browser è stato consentito un accesso completo a Internet, in modo che potessero visitare siti live effettivi.

## 4.2 BROWSER SOTTOPOSTI AL TEST

I browser, o prodotti sottoposti al test, sono stati ottenuti da NSS Labs in modo indipendente. In linea generale, in tutti i casi sono stati utilizzati i rilasci di software disponibili. Ogni prodotto è stato aggiornato alla versione più recente presente al momento dell'inizio del test. Di seguito è riportato l'elenco dei browser Web sottoposti al test:

- Google Chrome v10.0.648.204
- Windows Internet Explorer 8 (build 8.0.7600.16385)
- Windows Internet Explorer 9 (build 9.0.8112.16421)
- Mozilla Firefox v4.0
- Opera v11.01 Build 1190
- Safari v5.0.5 (7533.21.1)

Una volta iniziato il test, la versione del prodotto è stata bloccata per garantire l'integrità della prova. Il test ha utilizzato l'accesso a Internet per i sistemi di reputazione e la visualizzazione di contenuti live. In generale, esiste una separazione configurabile tra aggiornamenti software e aggiornamenti di database o firme, al fine di ricavare analogie da antivirus, prevenzione delle intrusioni e pratiche software generiche.

## 4.3 DESCRIZIONE DELLA RETE

I browser sono stati sottoposti a test per verificarne la capacità di proteggere il client nei casi di utilizzo "connesso". Di conseguenza, i test hanno considerato e analizzato l'efficacia della protezione offerta dal browser nell'ambito del realistico collegamento di test a Internet live di NSS Labs.

Il sistema host disponeva di una scheda interfaccia di rete (NIC) ed era connesso alla rete tramite una porta di commutazione da 1 Gb. La rete di test di NSS è un'infrastruttura multi-gigabit basata sui commutatori Cisco® Catalyst® serie 6500 (con interfacce gigabit sia in fibra che in rame).

Ai fini di questo test, NSS Labs ha utilizzato fino a 48 sistemi desktop, ognuno dotato di un browser Web, ovvero otto per ogni browser (sei tipi di browser). I risultati sono stati registrati in un database MySQL.

## 4.4 INFORMAZIONI SUL TEST

Questo report è stato creato come parte dei servizi di informazione del test indipendente di NSS Labs. I principali fornitori sono stati invitati a partecipare a titolo gratuito e NSS Labs non ha ricevuto alcun finanziamento per creare tale report.

# APPENDICE A: PROCEDURE DI TEST

Lo scopo di questo test era determinare l'efficacia dei browser Web esaminati nel proteggere gli utenti dalle principali minacce malware presenti oggi in Internet. Uno degli aspetti fondamentali era la tempistica. Considerate la velocità e l'aggressività con cui i criminali diffondono e manipolano i siti Web dannosi, un obiettivo importante era garantire che nel test venissero inclusi siti più "recenti" possibili.

NSS Labs ha sviluppato "Live Testing", una metodologia e un collegamento unici e proprietari, e raccoglie continuativamente minacce basate sul Web da diverse fonti, tra cui partner e server dell'azienda. Prima di essere inserite nella coda di test, le potenziali minacce vengono esaminate con algoritmi. Le minacce vengono inserite e analizzate continuamente. La peculiarità di questa procedura è che NSS Labs convalida i campioni sia prima che dopo il test. Il test effettivo delle minacce, eseguito ogni sei ore, inizia con la convalida dell'esistenza del sito e della conformità alla definizione del test.

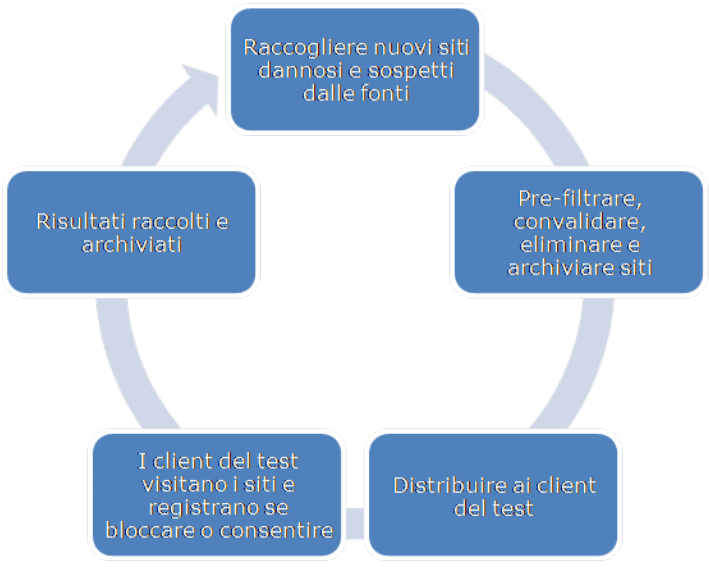
Tutti i test sono stati controllati in modo rigoroso e i risultati sono stati accuratamente registrati e archiviati in occasione di ogni intervallo del test.

## 4.5 DURATA DEL TEST

Il test di NSS Labs sui browser è stato effettuato continuativamente (tutti i giorni, 24 ore su 24) per 19 giorni. Durante l'intero test nuovi URL venivano aggiunti non appena individuati.

### 4.5.1 FREQUENZA DEL TEST

Durante il test, ogni URL è stato eseguito ogni sei ore ricorrendo all'apposito collegamento. Indipendentemente dall'esito positivo o negativo, NSS Labs ha continuato a tentare di scaricare campioni di malware con il browser Web per l'intera durata della prova.




## 4.6 SET DI CAMPIONI PER GLI URL MALWARE

Per questo tipo di test è essenziale disporre di siti malware sempre nuovi. Per avere la certezza di utilizzare gli URL più aggiornati e rappresentativi, NSS Labs riceve un ingente numero di campioni da diverse fonti.

### 4.6.1 FONTI

NSS Labs gestisce una rete propria di spam trap e honeypot. Questi account di posta elettronica con un ingente volume di traffico generano ogni giorno migliaia di messaggi di posta elettronica e diverse centinaia di URL unici. NSS Labs collabora inoltre con altri ricercatori, reti e società di protezione indipendenti che forniscono l'accesso a URL e contenuti dannosi. I set di campioni contengono URL dannosi che vengono distribuiti tramite: posta elettronica, messaggistica immediata, social network e siti Web dannosi. Non è stato utilizzato alcun contenuto proveniente dalle parti sottoposte a test.

Ai fini del test, sono stati identificati e selezionati URL dannosi rivolti contro gli utenti europei, ovvero individui residenti in paesi europei, tra cui: Austria, Belgio, Danimarca, Francia, Finlandia, Germania, Grecia, Irlanda, Italia, Norvegia, Paesi Bassi, Polonia, Portogallo, Russia, Spagna, Svezia, Svizzera, Regno Unito, Turchia e Ungheria. Tuttavia, anche se l'obiettivo è un utente in Europa, il dominio in cui il malware risiede può trovarsi in qualsiasi parte del mondo. D'altra parte, anche se un URL dannoso risiede in un dominio europeo, non significa che sia destinato a colpire solo utenti europei. Il fattore determinante per stabilire se inserire o meno nel test un URL dannoso è stata la partecipazione a una campagna di malware rivolta contro gli utenti europei. Erano state preparate trappole malware in lingue specifiche e gli URL sono stati inclusi solo quando la campagna risultava organizzata in una delle lingue europee interessate. Infine, la sola inclusione in una campagna contro utenti europei non implica che l'URL dannoso non sia stato utilizzato anche in diverse campagne contro utenti di altre regioni.

Dal test sono stati esclusi gli exploit contenenti payload malware (exploit più malware), noti anche come "clickjacking" o "download drive-by". È stato compiuto ogni possibile sforzo per prendere in considerazione campioni che riflettessero una distribuzione realistica del malware dal punto di vista geografico, di categoria e di piattaforma.

NSS Labs gestisce inoltre una raccolta di "URL puliti" che include siti di Yahoo, Amazon, Microsoft, Google, NSS Labs, banche importanti e così via. Questi URL sono stati eseguiti periodicamente nel sistema per verificare che i browser non stessero bloccando i contenuti indiscriminatamente.

## 4.7 URL DEL CATALOGO

Al set di URL presi in considerazione ne sono stati aggiunti di nuovi il prima possibile. La data e l'ora di introduzione di ogni campione è stata scrupolosamente annotata. La maggior parte delle fonti è stata inserita immediatamente e automaticamente, mentre alcuni metodi che hanno richiesto la gestione manuale sono stati elaborati in meno di 30 minuti. Tutti gli elementi inseriti nel set di analisi, indipendentemente dalla relativa validità, sono stati catalogati con un ID NSS Labs univoco. Questo ha consentito di tenere traccia dell'efficacia delle fonti dei campioni.

## 4.8 CONFERMA DELLA PRESENZA DEGLI URL CAMPIONE

Il tempo è un fattore essenziale, poiché l'obiettivo del test è verificare l'efficacia contro i siti di malware più aggiornati possibili. Considerata la natura dei feed e la velocità di cambiamento, non è possibile eseguire una convalida completa di ogni sito prima del test, poiché i siti possono scomparire rapidamente. Di conseguenza, ogni elemento del test è stato analizzato rapidamente per controllare che fosse presente e accessibile su Internet live.

Per essere inclusi nel set di esecuzione, gli URL dovevano risultare live durante l'iterazione del test. All'inizio di ogni ciclo di test, la disponibilità dell'URL veniva confermata controllando che il sito fosse attivo e raggiungibile e che non venisse restituita una pagina Web 404.

Questa convalida veniva eseguita entro pochi minuti dalla ricezione dei campioni inviati dalle fonti. **Nota:** queste classificazioni sono state sottoposte a un'ulteriore convalida dopo il test e, in base ai risultati ottenuti, gli URL sono stati riclassificati e/o rimossi.

### 4.8.1 ARCHIVIAZIONE DEI CONTENUTI DEGLI URL ATTIVI

I contenuti degli URL attivi sono stati scaricati e salvati in un server di archiviazione contrassegnato da un numero ID NSS univoco. Questo ha consentito a NSS Labs di conservare i contenuti degli URL a scopi di controllo e convalida.

## 4.9 ESECUZIONE DINAMICA DEI SINGOLI URL

Un'utilità di automazione client richiede che sia verificata la presenza di ognuno degli URL in base ai risultati del test descritti nella Sezione 5.4 tramite ciascun browser Web incluso nella prova. NSS Labs registra se è stato possibile, o meno, scaricare il malware e se il tentativo di download ha attivato l'invio di un avviso dalla protezione del browser contro il malware.

### 4.9.1 ASSEGNAZIONE DI UN PUNTEGGIO E REGISTRAZIONE DEI RISULTATI

La risposta ricevuta viene registrata come "Allowed" (Consentito) o " Blocked and Warned" (Bloccato con invio di avviso).

- **Esito positivo:** secondo NSS Labs, l'esito è positivo se il browser Web *riesce* a impedire il download del malware e a inviare *correttamente* un avviso.
- **Esito negativo:** secondo NSS Labs, l'esito è negativo se il browser Web *non riesce* a impedire il download del malware e *non* invia alcun avviso.

## 4.10 ELIMINAZIONE

Durante il test, i tecnici di laboratorio esaminano gli URL e i contenuti ed eliminano dal set di esecuzione quelli non conformi. Ad esempio, un URL classificato come malware e sostituito dall'host Web con una pagina iniziale generica viene eliminato dal test.

Se durante l'esecuzione del test un URL campione non risulta disponibile per il download, questo verrà eliminato dal test per l'iterazione in corso. NSS Labs verifica continuamente la presenza (disponibilità per il download) di ogni campione e, in base ai risultati ottenuti, lo aggiunge/rimuove dal set di test. Se un campione di malware non risulta disponibile per un'iterazione del test, ma lo diventa per l'iterazione successiva, questo verrà riaggiunto al set di test. I campioni non disponibili non vengono inclusi nel calcolo degli esiti positivi o negativi di un browser Web.

## 4.11 CONVALIDA SUCCESSIVA AL TEST

La convalida successiva al test consente a NSS Labs di riclassificare e persino rimuovere i campioni che sono risultati non dannosi o non disponibili prima dell'inizio del test. Per eliminare e convalidare il malware, NSS Labs ha utilizzato due diversi sandbox commerciali (CWSandbox di Sunbelt e Norman® Analyzer). Un'ulteriore convalida è stata eseguita utilizzando, a seconda delle esigenze, strumenti proprietari, strumentazione di sistema e analisi del codice.

## APPENDICE B: INFRASTRUTTURA DEL TEST

Un ringraziamento speciale è rivolto ai partner per l'infrastruttura di test che hanno fornito gran parte delle attrezzature, del software e del supporto che hanno reso possibile il test: