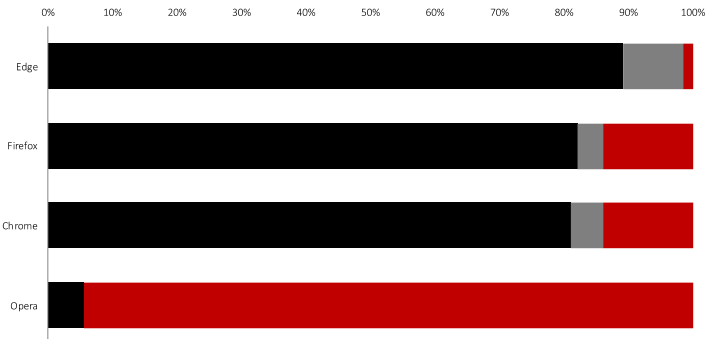
T2 2020 REPORT DI TEST COMPARATIVO

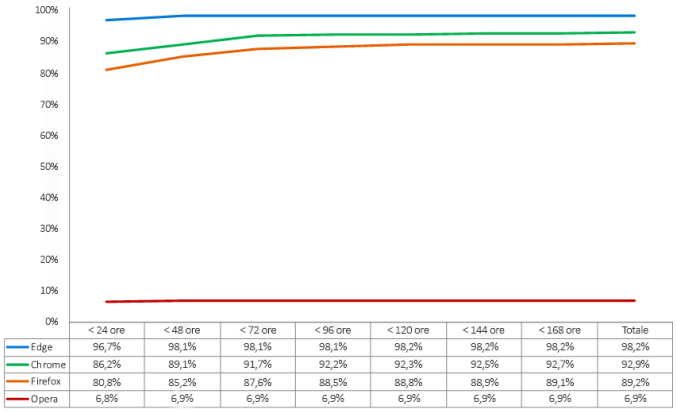
Panoramica

Durante il 2° trimestre del 2020, NSS Labs ha eseguito un test indipendente sulla protezione da malware offerta dai browser Web: 32.267 test discreti (per ciascun browser Web) impiegando 1.065 campioni unici per un periodo di 34 giorni. Per garantire protezione da malware, Microsoft Edge utilizza Microsoft Defender SmartScreen; Google Chrome e Mozilla Firefox utilizzano l'API Google Safe Browsing, mentre Opera utilizza Yandex.

Microsoft Edge ha offerto la migliore protezione, bloccando il 98,5% dei malware e fornendo allo stesso tempo la frequenza più elevata di protezione dagli attacchi zero-hour (96,7%). Firefox è risultato secondo come livello di protezione, bloccando una media dell'86,1%, seguito da Google Chrome con l'86,0%. Opera ha bloccato il 5,6%.



Riepilogo dei risultati

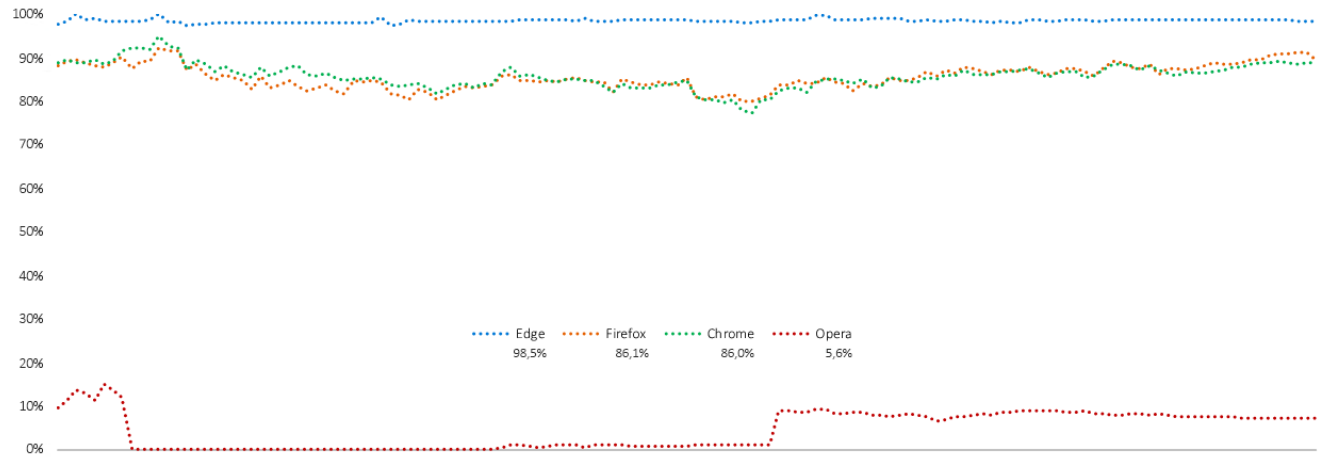


	< 24 ore	< 48 ore	< 72 ore	< 96 ore	< 120 ore	< 144 ore	< 168 ore	Totale
Edge	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Chrome	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Firefox	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Opera	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

I sistemi di reputazione abbreviano il tempo a disposizione degli utenti malintenzionati per raggiungere i propri obiettivi impedendo agli utenti di selezionare un URL, un file o un'applicazione pericolosa o avvisandoli di tale condizione. Tuttavia, gli utenti visitano di continuo nuovi siti Web, scaricando file e installando applicazioni. I sistemi di reputazione non possono limitarsi a bloccare tutti gli elementi nuovi. Questa consapevolezza porta gli utenti malintenzionati a modificare continuamente le campagne di malware; la maggior parte degli attacchi si verifica infatti nelle prime ore successive all'avvio di una campagna. Ne consegue che la chiave per una protezione efficace risiede nella classificazione rapida e accurata dei contenuti.

NSS Labs ha valutato la capacità dei browser di bloccare rapidamente i malware appena individuati su Internet. Abbiamo continuato a testare URL, file e applicazioni dannosi ogni sei ore per determinare quanto tempo impiegasse un fornitore ad aggiungere protezione, nei casi in cui ciò avveniva.

Protezione da malware nel tempo



Per tutta la durata del test sono stati aggiunti nuovi malware. URL, file e applicazioni che non erano più raggiungibili o che ospitavano malware sono stati rimossi. Ogni punto dati viene calcolato in base alle misurazioni registrate in un momento specifico. Se il malware veniva bloccato prima, il punteggio del browser per l'uniformità della protezione aumentava nel tempo. In alternativa, se il browser non bloccava il malware, il punteggio diminuiva.

L'attività di test è stata condotta in base a Web Browser Test Methodology v4.0 (disponibile all'indirizzo www.nsslabs.com).

Informazioni generali

Gli attacchi SEM (Social Engineered Malware) utilizzano una combinazione dinamica di social media, account di posta elettronica violati, notifiche false di problemi al computer e altri messaggi ingannevoli per invitare gli utenti a scaricare il malware. I criminali informatici utilizzano la violazione degli account di posta elettronica per trarre vantaggio della fiducia implicita tra i contatti e ingannare le vittime, facendo loro credere che i link a file dannosi siano al contrario affidabili. Gli account di social media violati vengono utilizzati in modo analogo agli account di posta elettronica violati. Nel caso dei social network, tuttavia, il cerchio si amplia: amici e persino amici di amici rischiano di essere tratti in inganno.

Le tattiche di ingegneria sociale possono impiegare messaggi popup, ad esempio avvisando gli utenti che è necessario installare applicazioni come Adobe Flash Player o che i loro computer sono stati infettati o richiedono aggiornamenti. Una volta installato il malware, le vittime sono vulnerabili a furti d'identità, compromissione dei conti bancari e altre conseguenze potenzialmente devastanti.

Protezione da malware offerta dai browser Web

Per garantire protezione da malware, i browser utilizzano sistemi di reputazione basati sul cloud, che setacciano Internet alla ricerca di siti Web dannosi e ne categorizzano i contenuti, aggiungendoli a elenchi di contenuti bloccati o consentiti oppure assegnando loro un punteggio (a seconda dell'approccio del fornitore).

Tali tecniche di categorizzazione possono essere eseguite manualmente o automaticamente. Il secondo componente funzionale alla protezione da malware comporta la richiesta da parte del browser Web di informazioni sulla reputazione da parte dei sistemi di reputazione basati sul cloud riguardo URL, file o applicazioni specifici, e quindi l'emissione di avvisi o il blocco del malware.

Se i risultati indicano la presenza di malware, il browser Web reindirizza l'utente a un messaggio di avviso sulla pericolosità dell'URL, del file o dell'applicazione. Alcuni sistemi di reputazione includono anche contenuti formativi aggiuntivi. Al contrario, se il contenuto è indicato come "non dannoso", il browser Web non esegue alcuna azione e l'utente rimane inconsapevole del controllo di sicurezza appena eseguito dal browser.

Google e Firefox utilizzano l'API Google Safe Browsing per verificare la reputazione dell'URL e per bloccare il download di alcuni tipi di file da parte degli utenti o per avvisarli. Microsoft Edge utilizza Microsoft Defender SmartScreen, che include il servizio di reputazione delle applicazioni per fornire protezione dalle minacce di phishing e malware. Opera utilizza una combinazione di elenchi di blocco di Netcraft,[1] PhishTank[2] e Metamask[3], oltre a un elenco di blocco del malware di Yandex.[4]

Inoltre, Microsoft Defender SmartScreen è stato incorporato come funzionalità del sistema operativo nell'aggiornamento di Windows 10 dell'ottobre 2017. La versione per il sistema operativo della protezione SmartScreen rappresenta uno scudo per tutti i browser, i client di posta elettronica, i dispositivi USB e altre applicazioni ed è parte integrante della protezione da malware del sistema operativo. Gli utenti possono, quindi, sfruttare la protezione dagli URL e dalle applicazioni/dai file offerta dal browser, oltre alla protezione del sistema operativo.

Composizione del test - Campioni di malware

I dati del presente report coprono un periodo di test di 34 giorni, tra il 21 aprile 2020 e il 25 maggio 2020. Tutti i test sono stati eseguiti presso la struttura di test di Austin, in Texas. Durante il test, i tecnici di NSS hanno monitorato regolarmente la connettività, per assicurarsi che i browser sottoposti a test potessero accedere al malware e ai servizi di reputazione nel cloud.

L'accento è stato posto sulla novità; è stato così valutato un numero di campioni maggiore rispetto a quello dei campioni conservati all'interno del set di test risultante, dal momento che venivano aggiunti continuamente al test nuovi campioni e i campioni esaminati venivano rimossi.

Numero totale di campioni dannosi sottoposti a test

Un totale di 1.844 campioni non elaborati e non convalidati è stato sottoposto a test più volte con ciascun browser Web, per un totale di 182.676 test discreti condotti senza interruzione per 822 ore (ogni 6 ore per 34 giorni). I tecnici di NSS hanno rimosso i campioni che non hanno superato i criteri di convalida, inclusi quelli contaminati dall'utilizzo (non inclusi nel test). Alla fine, 1.065 campioni di malware unici validi sono stati inclusi in 129.068 test della presenza di malware discreti validi (32.267 per ogni browser Web), con un margine di errore inferiore al 2 percento (<2%) e un livello di confidenza del 95%.

[1] http://www.netcraft.com/

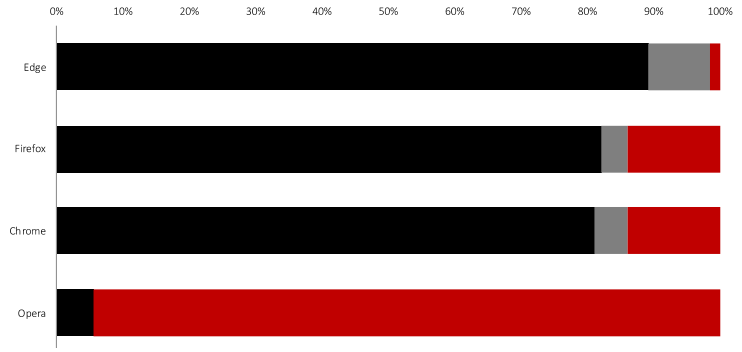
[2] http://www.phishtank.com/

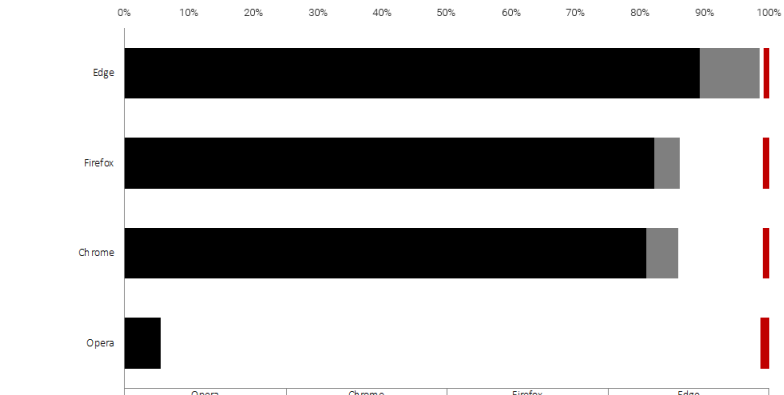
[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

Frequenza di blocco del malware

La capacità di avvisare le potenziali vittime della possibilità di imbattersi in un sito Web dannoso colloca i browser Web in una posizione unica nella lotta al malware frutto di ingegneria sociale. Dal momento che i siti contenenti malware hanno una durata breve, è essenziale che il sito venga individuato, convalidato, classificato e aggiunto al sistema di reputazione più rapidamente possibile. In quanto tale, un buon sistema di reputazione deve essere accurato e rapido per ottenere frequenze elevate di rilevazione. Gli sviluppatori dei browser comprendono chiaramente questa relazione. In ultima analisi è stata bloccata una maggiore quantità di malware nelle prime 24 ore di rilevazione che successivamente.





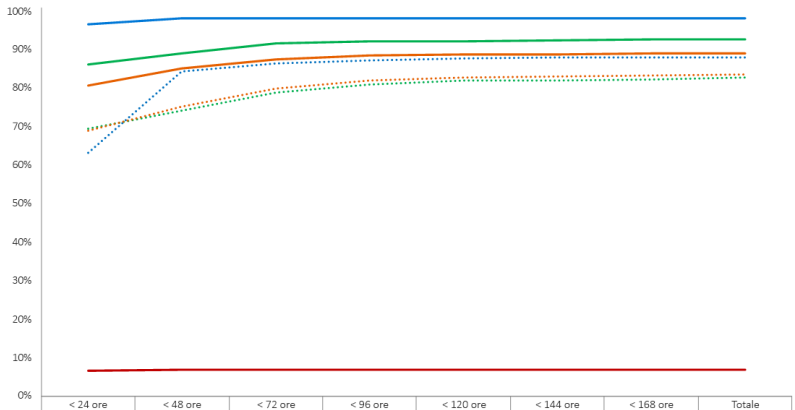
	Opera	Chrome	Firefox	Edge
Rep. URL	5,6%	80,9%	82,1%	89,2%
Rep. URL + App	0,0%	5,0%	4,0%	9,3%
Rep. URL + App + Sist. op.	93,1%	13,1%	13,0%	0,7%
Non rilevati	1,4%	0,9%	0,9%	0,8%

La tecnologia di protezione principale all'interno di Edge è SmartScreen, che fornisce una protezione basata su URL dagli attacchi tramite un servizio di reputazione degli URL integrato e basato sul cloud, oltre che della reputazione delle applicazioni per il blocco dei file dannosi. SmartScreen con la reputazione delle applicazioni ha bloccato il 98,5% per Edge. Mozilla Firefox e Google Chrome utilizzano l'API Safe Browsing. Firefox ha bloccato l'86,1%. Google Chrome ha bloccato l'86,0%. Opera, che utilizza una combinazione di elenchi di blocco di diverse origini, ha bloccato il 5,6%.

Inoltre, Microsoft Defender SmartScreen ha bloccato un'ulteriore percentuale di file dannosi del 93,1% per Opera, del 13,1% per Chrome, del 13,0% per Firefox e dello 0,7% per Edge quando abbiamo tentato di eseguirli.

Istogramma di protezione da malware

La protezione immediata dai nuovi malware è di importanza fondamentale. Quando i siti che ospitano malware vengono individuati, essi sono chiusi, spesso in un lasso di tempo relativamente breve. I prodotti che non riescono ad aggiungere protezione in modo tempestivo possono richiedere troppo tempo per contrastare una minaccia. L'istogramma indica il tempo impiegato da ogni browser per bloccare i malware una volta che il campione è stato introdotto nel ciclo di test. In una finestra di sette giorni, le frequenze di protezione cumulativa vengono calcolate ogni giorno fino al blocco delle minacce.



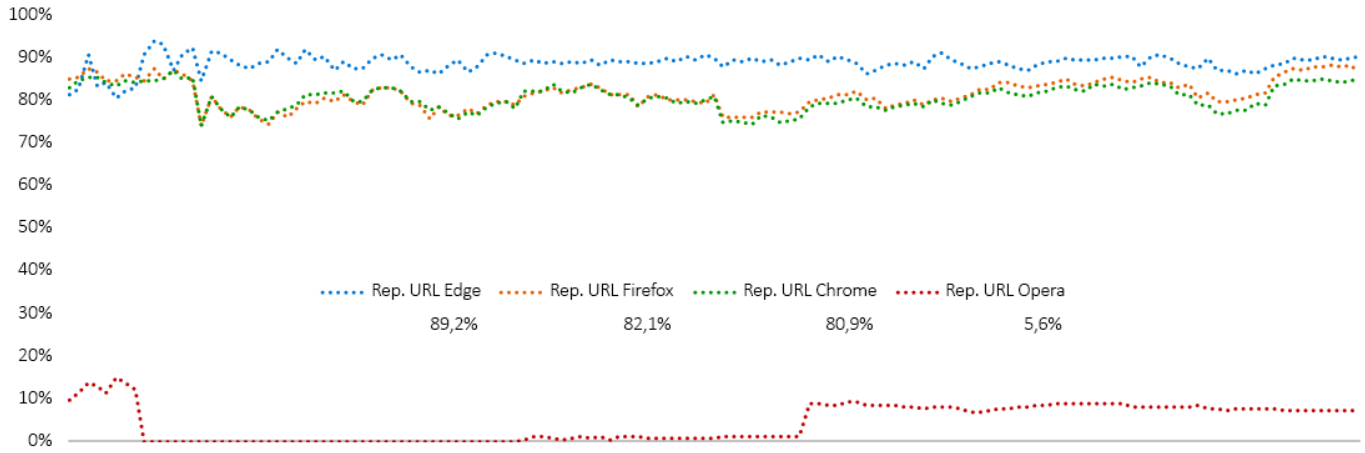
	< 24 ore	< 48 ore	< 72 ore	< 96 ore	< 120 ore	< 144 ore	< 168 ore	Totale
Edge con rep. app	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Edge con rep. URL	63,4%	84,5%	86,5%	87,3%	87,8%	88,1%	88,1%	88,1%
Chrome con rep. app	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Chrome con rep. URL	69,7%	74,4%	79,0%	81,0%	82,0%	82,2%	82,4%	82,7%
Firefox con rep. app	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Firefox con rep. URL	69,1%	75,3%	80,0%	82,1%	82,9%	83,0%	83,4%	83,6%
Opera con rep. URL	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Durante il test, Microsoft Edge ha dimostrato una frequenza di protezione da malware iniziale del 96,7%. Google Chrome e Mozilla Firefox hanno raggiunto un livello di protezione iniziale rispettivamente dell'86,2% e dell'80,8%. La frequenza di protezione iniziale di Opera è stata del 6,8%. Alla fine del settimo giorno di test, tutti i browser Web hanno registrato un incremento della protezione. L'incremento di Microsoft Edge è stato del 4,5%, al 98,2%. L'incremento di Google Chrome è stato del 6,7%, al 92,9%; l'incremento di Mozilla Firefox è stato dell'8,4%, all'89,2%; l'incremento di Opera è stato dello 0,1%, al 6,9%.

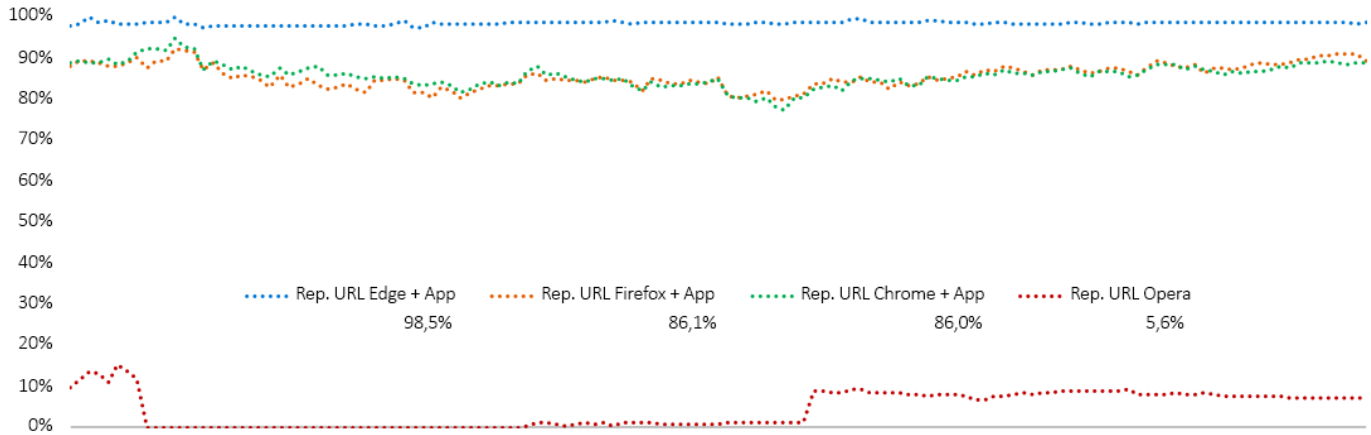
Uniformità della protezione nel tempo

Per tutta la durata del test sono stati aggiunti nuovi malware. URL, file e applicazioni che non erano più raggiungibili o che ospitavano malware sono stati rimossi. Ogni punto dati viene calcolato in base alle misurazioni registrate in un momento specifico. Se il malware veniva bloccato prima, il punteggio del browser per l'uniformità della protezione aumentava nel tempo. In alternativa, se il browser non bloccava il malware, il punteggio diminuiva.

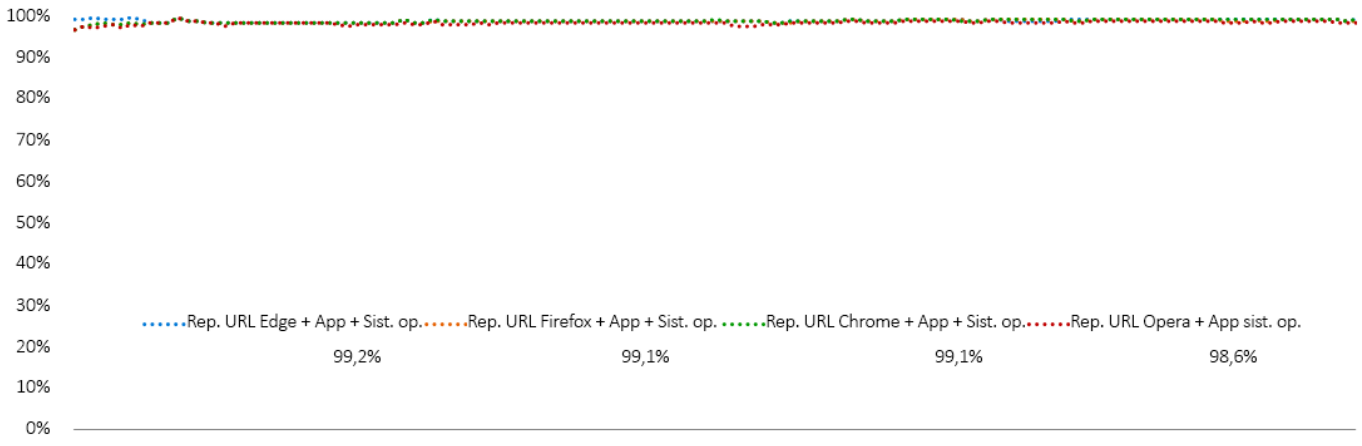
Il test ha evidenziato tre livelli di protezione: reputazione dell'URL, reputazione delle applicazioni nel browser e reputazione delle applicazioni nel sistema operativo. La reputazione dell'URL ha offerto una protezione ragionevolmente valida.



L'aggiunta della reputazione delle applicazioni ha aumentato il livello di protezione.



La reputazione del sistema operativo ha offerto una protezione aggiuntiva. La condizione ottimale è che il browser Web blocchi il malware in modo che non raggiunga mai il sistema operativo. Tuttavia, il test indica che la reputazione del sistema operativo si è rivelata altamente efficace.



Ambiente di test

- BaitNET™ (NSS Labs Proprietary)
- 64-bit Microsoft Windows 10 Pro (versione 1909 build: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (Kernel versione 4.19.0-kali5-amd64)
- VMware vCenter (versione 6.7u2 build 6.7.0.30000)
- VMware vSphere (versione 6.7.0.20000)
- VMware ESXi (versione 6.7u3 build 14320388)
- VMware Tools 10.3.5
- Wireshark versione 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (build 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Prodotti sottoposti a test

- Google Chrome: versione 81.0.4044.113 - 81.0.4044.138
- Microsoft Edge: versione 83.0.478.10 - 84.0.516.1
- Mozilla Firefox: versione 75.0 - 76.0.1
- Opera: versione: 67.0.3575.137 - 68.0.3618.125

Autori

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Metodologia di test

NSS Labs Web Browser Security (WBS) Test Methodology v4.0 è disponibile all'indirizzo www.nsslabs.com.

Recapiti

NSS Labs, Inc.

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746

info@nsslabs.com

www.nsslabs.com