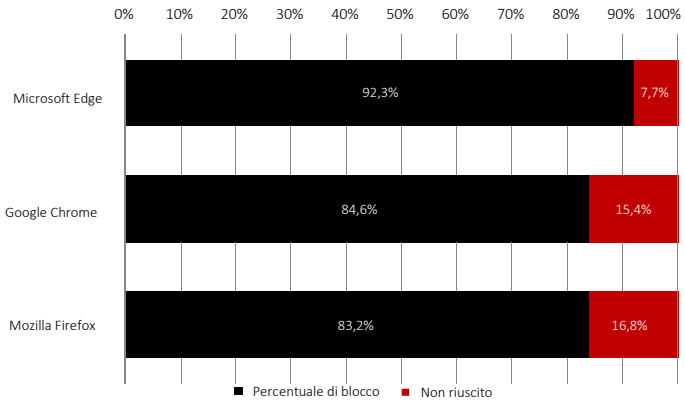
Q2 2021 Web browser e phishing

Panorami

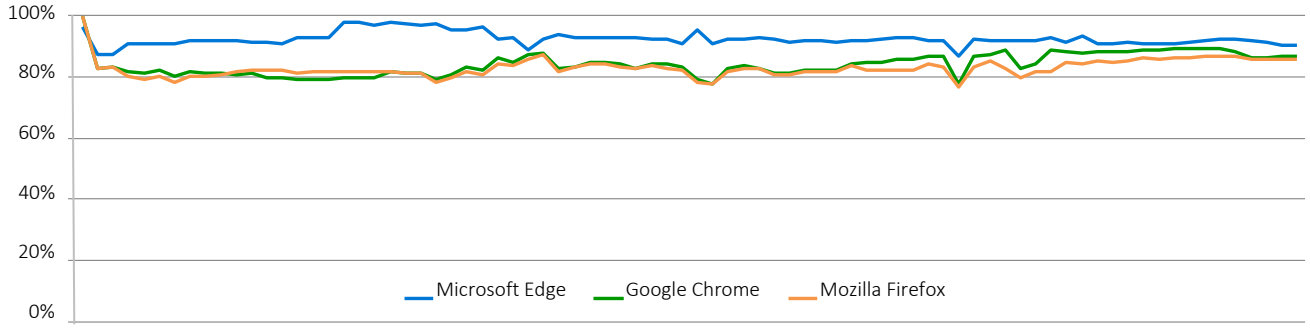
Durante il 2° trimestre del 2021, CyberRatings.org ha eseguito test indipendenti sulla protezione dal phishing offerta dai browser Web. I test si sono svolti per 20 giorni con 80 esecuzioni di test discreti. Per proteggere dal phishing, Microsoft Edge utilizza Microsoft Defender SmartScreen; Google Chrome e Mozilla Firefox utilizzano l'API Google Safe Browsing. Microsoft Edge ha offerto la massima protezione, bloccando il 92,3% degli URL di phishing e fornendo la percentuale più elevata di protezione Zero-Hour (93,5%). Google Chrome ha ottenuto il secondo posto, con il blocco dell'84,6% degli attacchi, seguito da Mozilla Firefox con l'83,2%.



Sommario dei

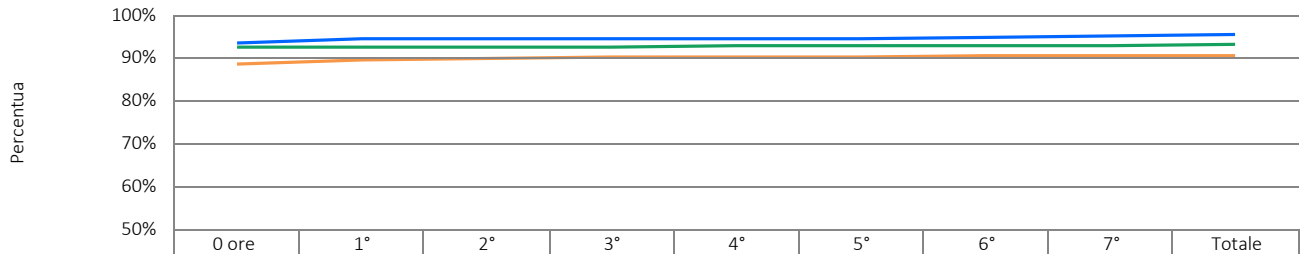
I sistemi di reputazione degli URL riducono il tempo a disposizione dei malintenzionati per raggiungere i loro obiettivi poiché avvisano gli utenti che un determinato URL corrisponde a un sito di phishing noto. Tuttavia, dato che gli utenti visitano numerosi siti Web, molti dei quali sono nuovi, i sistemi di reputazione degli URL non possono semplicemente bloccare tutti i nuovi URL. Sapendo questo, la campagne di phishing cambiano continuamente e la maggior parte dei nuovi attacchi si verifica nelle primissime ore dopo il lancio di un attacco.

Protezione dal phishing nel corso del tempo



Nel corso del test, ogni giorno venivano aggiunti nuovi URL di phishing e gli URL che non erano più raggiungibili o che non veicolavano più attacchi di phishing sono stati rimossi. Ciascun punto dati rappresenta la protezione in un momento specifico. Se un URL è stato bloccato presto, il punteggio del browser riguardo alla coerenza della protezione nel corso del tempo è aumentato. Altrimenti, se il browser non ha bloccato il URL, il punteggio è diminuito.

Percentuale di blocco del phishing nel corso del tempo



	0 ore	1°	2°	3°	4°	5°	6°	7°	Totale
Microsoft Edge	93,5%	94,4%	94,5%	94,5%	94,5%	94,7%	94,9%	95,1%	95,4%
Google Chrome	92,4%	92,6%	92,7%	92,7%	92,8%	92,8%	92,8%	92,9%	93,2%
Mozilla Firefox	88,7%	89,7%	90,0%	90,4%	90,4%	90,4%	90,5%	90,6%	90,6%

Abbiamo misurato la capacità dei browser di bloccare URL dannosi non appena venivano individuati in Internet. I test sono continuati ogni sei ore per determinare il tempo necessario a un rivenditore per aggiungere protezione. La figura qui sopra mostra il tempo di risposta di ciascun browser per bloccare un sito di phishing una volta che la minaccia è stata introdotta nel ciclo di test.

Attacchi di phishing

Il phishing è un tipo di attacco di ingegneria sociale che tenta di convincere una vittima a fornire informazioni personali riservate all'autore dell'attacco. Alcuni esempi di informazioni riservate sono: numeri di carte di credito, numeri di previdenza sociale, credenziali di accesso e password di conti bancari. Le e-mail, i messaggi istantanei, i messaggi SMS e i collegamenti ipertestuali sui siti di reti social sono tutti vettori di attacchi di phishing. Le pagine di destinazione di siti di phishing spesso tentano di sfruttare furtivamente il computer di un visitatore e installare software dannoso (tecnica nota come "exploit drive-by").

Gli attacchi di phishing espongono gli individui e le organizzazioni a notevoli rischi con la minaccia di compromettere o acquisire informazioni personali e aziendali riservate. Il gruppo Anti-Phishing Working Group (APWG) ha segnalato un totale di 396.688 campagne di phishing via e-mail uniche nel quarto trimestre del 2020.[1]

Protezione dal phishing offerta dai browser Web

La protezione dal phishing è fornita da un'applicazione all'interno di un browser Web che richiede la reputazione di un URL a un servizio cloud che esplora Internet per individuare siti di phishing e li aggiunge a un elenco di siti bloccati. In questo modo, quando un browser Web tenta di visitare un URL, la protezione dal phishing del browser (es. Safe Browsing, SmartScreen ecc.) reindirizza l'utente a un messaggio di avviso che spiega che quell'URL è dannoso. Alcuni sistemi di reputazione includono anche ulteriori contenuti formativi. Viceversa, se un sito Web viene valutato come "buono", il browser Web non interviene.

Google e Firefox utilizzano l'API Google Safe Browsing sia per la reputazione degli URL, sia per avvisare gli utenti prima del download di certi tipi di file. Microsoft Edge utilizza Microsoft Defender SmartScreen che fornisce una protezione dagli attacchi basata sugli URL, tramite un servizio di reputazione degli URL integrato e basato sul cloud, ma anche la reputazione delle applicazioni per bloccare i file dannosi.

Numero medio di URL dannosi aggiunti ogni giorno

In media, ogni giorno sono stati aggiunti al test 50 nuovi URL convalidati; in alcuni giorni i numeri variavano in seguito alle fluttuazioni dei livelli di attività criminale.

Ambiente del test

- Microsoft Windows 10 Pro, 21H1

Numero totale di URL dannosi nel test

26.976 URL grezzi, non convalidati sono stati testati più volte con ciascun browser Web, per un totale di 80 cicli di test per ciascuno, condotti senza interruzione per 480 ore (ogni 6 ore per 20 giorni). I nostri tecnici hanno rimosso i campioni che non hanno superato i criteri di convalida, inclusi quelli colpiti da exploit (che non fanno parte di questo test). Alla fine, 996 URL di phishing validi e unici sono stati inclusi nel set finale di 61.605 test sul phishing validi e discreti (20.535 test per ogni browser Web), con un margine di errore del 3,1% con un livello di attendibilità del 95%.

Composizione del test – URL di phishing

I dati in questo rapporto riguardano un arco di tempo di venti (20) giorni fra l'11 e il 31 maggio 2021. Durante il test, i nostri tecnici hanno controllato regolarmente la connettività per garantire che i browser sottoposti al test potessero accedere agli URL di phishing e ai servizi di reputazione dei browser nel cloud.

L'accento era posto sulla novità, con l'aggiunta costante al test di nuovi URL e la rimozione dei siti compromessi.

Modalità di valutazione dei risultati

Abbiamo misurato la capacità di ciascun browser di bloccare URL dannosi non appena venivano individuati in Internet. I tecnici hanno ripetuto questi test ogni sei ore per determinare il tempo necessario a un rivenditore per aggiungere protezione se non l'ha fatto.

Le prestazioni di ciascun browser sono state misurate costantemente e la percentuale di blocco generale di tutti gli URL testati con il browser è stata registrata. La percentuale di blocco generale di ciascun browser è stata calcolata in base al numero di blocchi riusciti diviso per il numero totale di casi di test. Ad esempio, con l'esecuzione di test ogni 6 ore, un URL che è stato online per 48 ore è stato testato otto (8) volte. Un browser che lo ha bloccato in 6 esecuzioni di test (su un numero massimo di 8) ha ottenuto una percentuale di blocco del 75%.

Prodotti testati

- Google Chrome: versioni 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge: versione 91.0.864.19 - 91.0.864.37
- Mozilla Firefox: versione 88.0.1 - 88.0.1

[1] APWG Phishing Activity Trends Report

Autori

Thomas Skybakmoen, Vikram Phatak

Metodologia del test

La versione 1.0 della metodologia del test sulla sicurezza dei browser Web di CyberRatings è disponibile all'indirizzo www.cyberratings.org

Informazioni di contatto

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org