

Q2 2021 Web browser e malware

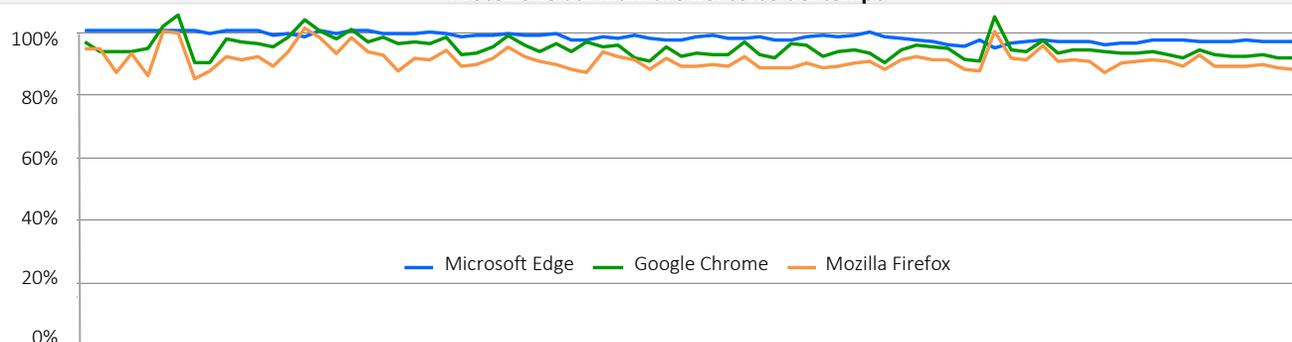
Panorami

Durante il 2° trimestre del 2021, CyberRatings.org ha eseguito test indipendenti sulla protezione dal malware offerta dai browser Web. I test si sono svolti per 20 giorni con 80 esecuzioni di test discreti. Per offrire protezione dal malware, 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 97,4% del malware e fornendo la percentuale più elevata di protezione Zero-Hour (97,7%). Google Chrome ha ottenuto il secondo posto, con il blocco dell'86,3% degli attacchi, seguito da Mozilla Firefox con l'81,8%.



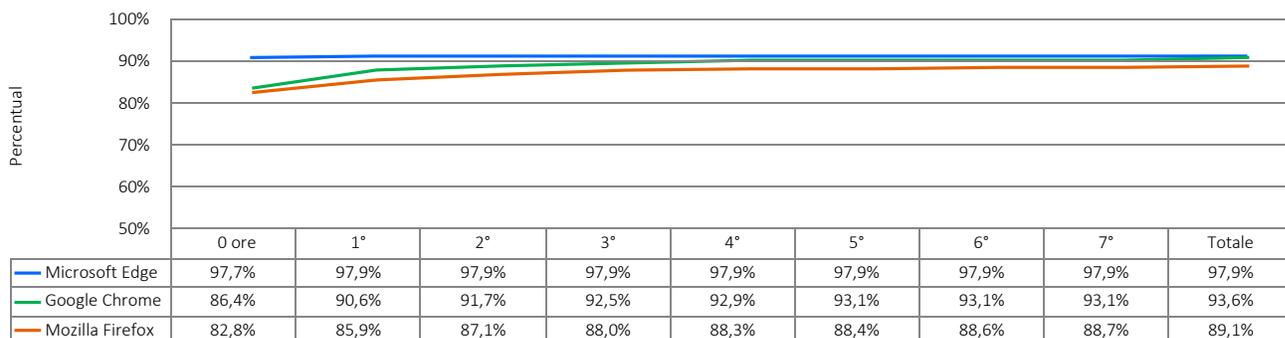
La capacità di avvisare le potenziali vittime che stanno per finire in un sito Web dannoso pone i browser Web in una posizione unica per combattere il malware. I siti Web che inducono (ingegneria sociale) gli utenti a scaricare malware hanno breve durata, perciò è essenziale che il sito venga scoperto e aggiunto al sistema di reputazione il prima possibile. Pertanto, un buon sistema di reputazione deve essere rapido e accurato per ottenere elevate percentuali di identificazione.

Protezione dal malware nel corso del tempo



Nel corso del test, veniva aggiunto costantemente nuovo malware. Gli URL che non erano più raggiungibili o che ospitavano del malware sono stati rimossi. Ciascun punto dati è calcolato in base alle misure registrate in un momento specifico. Se il malware è stato bloccato presto, il punteggio di protezione del browser nel corso del tempo è migliorato. Altrimenti, se il browser non ha bloccato il malware, il punteggio è diminuito.

Percentuale di blocco del malware nel corso del tempo



Sommario dei

La figura qui sopra mostra l'intervallo di tempo impiegato da ciascun browser per bloccare il malware una volta che il campione è stato introdotto nel ciclo di test. La tecnologia di protezione al centro di Microsoft Edge è SmartScreen che fornisce una protezione dagli attacchi basata sugli URL tramite un servizio di reputazione degli URL integrato e basato sul cloud e di reputazione delle applicazioni per bloccare i file dannosi. Google Chrome e Mozilla Firefox utilizzano l'API Google Safe Browsing sia per la reputazione degli URL sia per bloccare o avvisare gli utenti prima del download di certi tipi di file.

Attacchi di malware

Il malware di ingegneria social (SEM) utilizza l'inganno per indurre gli utenti a scaricare malware: Gli account di posta elettronica e social media sabotati sfruttano la fiducia implicita fra i contatti e ingannano le vittime, facendo credere che i collegamenti ai file dannosi siano affidabili. Altri tipi di inganno includono messaggi popup che avvisano gli utenti che devono installare applicazioni (come Adobe Flash Player) o che il computer è infetto o che è necessario un aggiornamento.

Una volta installato il malware, le vittime sono esposte al furto di credenziali o di identità, alla compromissione dei conti bancari ecc.

Protezione dal malware offerta dai browser Web

Per proteggere dal malware, i sistemi di reputazione basati sul cloud esplorano Internet alla ricerca di siti Web dannosi e categorizzano i contenuti di conseguenza. Quindi i browser Web interrogano i sistemi di reputazione basati sul cloud riguardo a URL, applicazioni o file specifici. Se i risultati indicano che è presente del malware, il browser Web reindirizza l'utente a un messaggio di avviso che spiega che quell'URL, applicazione o file è dannoso. Alcuni sistemi di reputazione includono anche ulteriori contenuti formativi.

Google Chrome e Mozilla Firefox utilizzano l'API Google Safe Browsing sia per la reputazione degli URL sia per la reputazione delle applicazioni per bloccare i file dannosi. Microsoft Edge utilizza Microsoft Defender SmartScreen che fornisce protezione dagli attacchi tramite un servizio di reputazione degli URL basato sul cloud e di reputazione delle applicazioni per bloccare i file dannosi.

Numero medio di campioni di malware dannoso aggiunti ogni giorno

In media, ogni giorno sono stati aggiunti al test 49 nuovi campioni di malware 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 campioni dannosi testati

18.621 campioni grezzi, non convalidati sono stati testati più volte con ciascun browser Web, per un totale di 78 cicli di test per ciascuno, condotti senza interruzione per 468 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, 950 campioni di malware validi e unici sono stati inclusi nel set finale di 48.672 test sul malware validi e discreti (16.224 test per ogni browser Web), con un margine di errore inferiore al 3,2% (<3,2%) con un livello di attendibilità del 95%.

Modalità di esecuzione del test – Campioni di malware

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 tecnici di CyberRatings hanno controllato regolarmente la connettività per garantire che i browser sottoposti al test potessero accedere al malware e ai servizi di reputazione nel cloud.

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

Modalità di valutazione dei risultati

Abbiamo misurato la capacità di ciascun browser di bloccare il malware non appena veniva individuato 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 i campioni di malware 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 campione di malware 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

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

© 2021 CyberRatings.org. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, copiata/sottoposta a scansione, archiviata su un sistema di recupero, inviata via e-mail o diffusa in altro modo o trasmessa senza l'esplicito consenso scritto di CyberRatings.org. (di seguito "noi" o "ci").

1. Le informazioni contenute in questo rapporto sono soggette a modifica da parte nostra senza preavviso e decliniamo qualsiasi obbligo di aggiornarle.
2. Le informazioni contenute in questo rapporto sono da noi ritenute accurate e affidabili al momento della pubblicazione, ma non sono garantite. L'utilizzo e la scelta di fare affidamento a questo rapporto sono a esclusivo rischio dell'utente. Non siamo in alcun modo responsabili in caso di danni, perdite o spese di qualsiasi natura derivanti da eventuali errori o omissioni inclusi in questo rapporto.
3. NON FORNIAMO ALCUNA GARANZIA ESPRESSA O IMPLICITA. ESCLUDIAMO TUTTE LE GARANZIE IMPLICITE, INCLUSE LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, IDONEITÀ PER UNO SCOPO SPECIFICO E NON VIOLABILITÀ. IN NESSUN CASO SAREMO RESPONSABILI IN CASO DI DANNI DIRETTI, CONSEGUENZIALI, INCIDENTALI, PUNITIVI, ESEMPLARI O INDIRETTI O DI PERDITA DI PROFITTI, RICAVI, DATI, PROGRAMMI INFORMATICI O ALTRE RISORSE, ANCHE SE AVVERTITI DELLA POSSIBILITÀ DI TALI DANNI.
4. Questo rapporto non costituisce un'approvazione, raccomandazione o garanzia di alcuno dei prodotti (hardware o software) sottoposti al test o dell'hardware e/o software utilizzato per testare i prodotti. Il test non garantisce l'assenza di errori o difetti nei prodotti o che i prodotti soddisfino le attese, i requisiti, le esigenze o le specifiche o che funzioneranno senza interruzioni.
5. Questo rapporto non implica alcuna approvazione, sponsorizzazione, affiliazione o verifica da parte di o con eventuali organizzazioni citate in questo rapporto.
6. Tutti i marchi, marchi di servizio e nomi commerciali utilizzati in questo rapporto sono di proprietà dei rispettivi titolari.