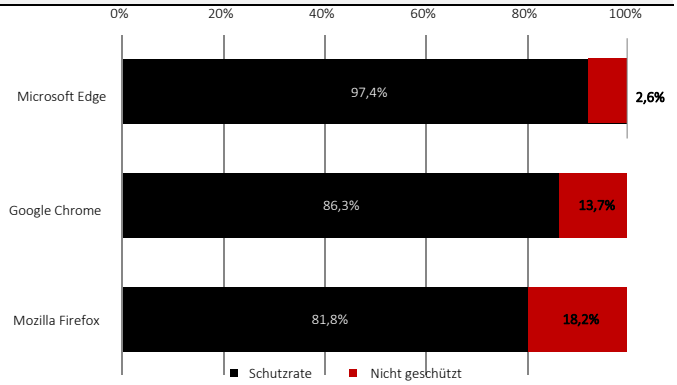
Q2 2021 Webbrowser vs. Schadsoftware

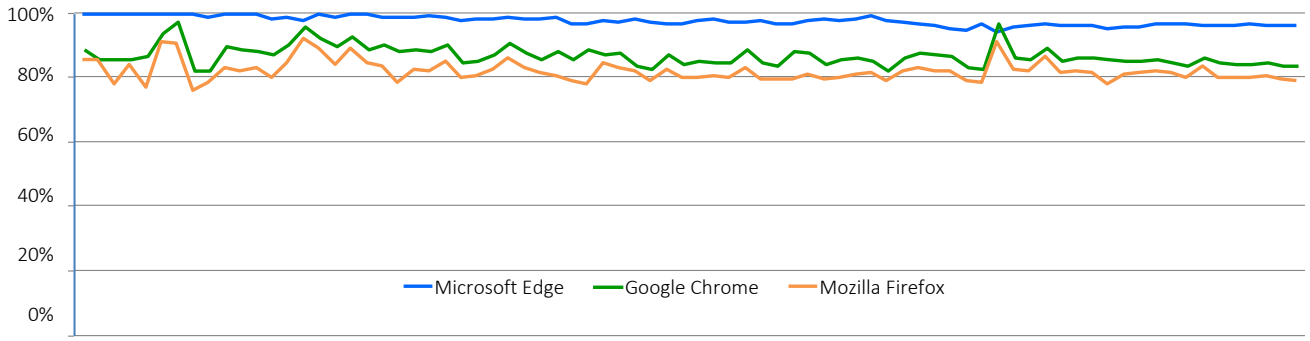
Übersicht

Im zweiten Quartal 2021 führte CyberRatings.org einen unabhängigen Test zum Thema „Schutz vor Schadsoftware durch Webbrowser“ durch. Die Tests liefen 20 Tage lang und umfassten 80 diskrete Testdurchläufe. Zum Schutz vor Schadsoftware kommt bei Microsoft Edge der Microsoft Defender SmartScreen zum Einsatz; Google Chrome und Mozilla Firefox verwenden die Google Safe Browsing API. Microsoft Edge bot beim Test den höchsten Schutz, blockierte 97,4 % aller Schadsoftware und bot gleichzeitig die höchste Zero-Hour-Schutzrate (97,7 %). Google Chrome bot mit durchschnittlich 86,3 % den zweithöchsten Schutz, gefolgt von Mozilla Firefox mit 81,8 %.



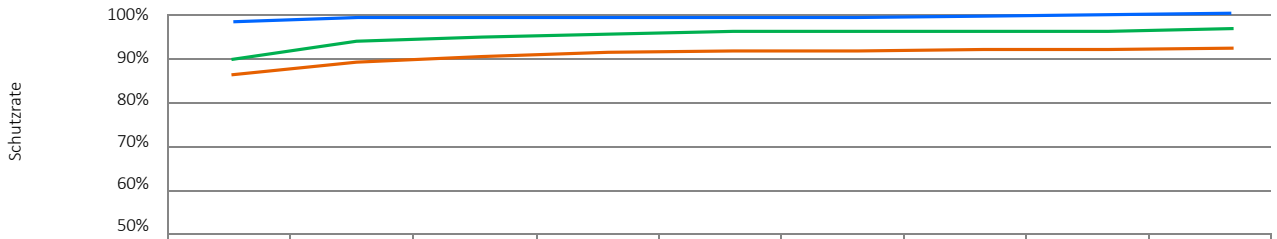
Die Fähigkeit, potenzielle Opfer zu warnen, wenn sie gerade dabei sind, eine bösartige Website aufzurufen, versetzt Webbrowser bei der Bekämpfung von Schadsoftware in eine einzigartige Lage. Websites, die Anwender durch Täuschung (soziale Manipulation) zum Herunterladen von Schadsoftware verleiten, sind nicht lange im Netz. Daher ist es wichtig, dass solche Websites so schnell wie möglich entdeckt und ins Reputationssystem übertragen wird. Ein gutes Reputationssystem muss daher gleichermaßen genau und auch schnell sein, um hohe Abfangquoten zu erzielen.

Schutz vor Schadsoftware im Laufe der Zeit



Während des Tests wurde ständig neue Schadsoftware hinzugefügt. URLs, die entweder nicht mehr erreichbar waren oder Schadsoftware gehostet haben, wurden entfernt. Jeder Datenpunkt wird aus Messungen berechnet, die zu einem bestimmten Zeitpunkt aufgezeichnet wurden. Wurde die Schadsoftware frühzeitig blockiert, bekam der Browser eine höhere Bewertung für Schutz im Laufe der Zeit. Wenn der Browser die Schadsoftware nicht blockierte, sank hingegen die Schutzbewertung.

Schadsoftware-Schutzrate im Laufe der Zeit.



	0 Std.	1 Tag	2 Tage	3 Tage	4 Tage	5 Tage	6 Tage	7 Tage	Gesamt
Microsoft Edge	97,7%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%
Google Chrome	86,4%	90,6%	91,7%	92,5%	92,9%	93,1%	93,1%	93,1%	93,6%
Mozilla Firefox	82,8%	85,9%	87,1%	88,0%	88,3%	88,4%	88,6%	88,7%	89,1%

Zusammenfassung

Die obige Abbildung zeigt, wie lange jeder Browser brauchte, um Schadsoftware zu blockieren, sobald ein Schadsoftwaremuster in den Testzyklus eingeführt wurde. Die zentrale Schutztechnologie von Microsoft Edge ist der SmartScreen, der URL-basierten Schutz vor Angriffen über einen integrierten, cloudbasierten URL-Reputationsdienst sowie eine Anwendungsreputation zum Blockieren schädlicher Dateien bietet. Google Chrome und Mozilla Firefox verwenden die Google Safe Browsing API für die URL-Reputation, zum Warnen von Anwendern vor dem Herunterladen bestimmter Dateitypen oder zum Blockieren dieser Dateitypen.

Angriffe durch Schadsoftware

Angriffe durch soziale Manipulation täuschen bewusst Anwender, damit sie zum Herunterladen von Schadsoftware verleitet werden: Gestohlene E-Mail- und Social-Media-Konten nutzen das implizite Vertrauen zwischen Kontakten aus und gaukeln den Opfern vor, dass Links zu schädlichen Dateien vertrauenswürdig sind. Andere Täuschungsversuche umfassen Pop-up-Warnungen, die Anwender darauf hinweisen, dass Anwendungen (wie Adobe Flash Player) installiert werden müssen, oder die Warnung, dass der Computer des Anwenders infiziert ist oder eine Aktualisierung benötigt.

Sobald die Schadsoftware installiert ist, sind die Opfer anfällig für den Diebstahl von Anmeldedaten und Identitäten, oder ihre Bankkonten werden gefährdet usw.

Schutz vor Schadsoftware durch Webbrowser

Zum Schutz vor Schadsoftware durchsuchen cloudbasierte Reputationssysteme das Internet nach schädlichen Websites und kategorisieren dann entsprechend Inhalte. Die Webbrowser stellen dann bei den cloudbasierten Reputationssysteme eine Anfrage nach bestimmten URLs, Dateien oder Anwendungen. Wenn die Ergebnisse darauf hindeuten, dass Schadsoftware vorhanden ist, leitet der Webbrowser den Anwender zu einer Warnmeldung weiter, die darauf hinweist, dass eine URL, Datei oder Anwendung schädlich ist. Manche Reputationssysteme beinhalten auch zusätzliche Informationsangebote.

Google Chrome und Mozilla Firefox verwenden die Google Safe Browsing API sowohl für die URL-Reputation als auch für die Anwendungsreputation, um schädliche Dateien zu blockieren. Bei Microsoft Edge kommt der Microsoft Defender SmartScreen zum Einsatz, der über einen cloudbasierten Reputationsdienst für die URL-Reputation und die Anwendungsreputation zum Blockieren schädlicher Dateien bietet.

Durchschnittliche Anzahl der täglich hinzugefügten Schadsoftwaremuster

Im Durchschnitt wurden pro Tag 49 neue validierte Schadsoftwaremuster zum Testsatz hinzugefügt; an manchen Tagen schwankte die Zahl, da nicht jeden Tag gleich viele kriminelle Aktivitäten auftraten.

Gesamtzahl der getesteten schädlichen Muster

18.621 rohe, nicht validierte Muster wurden bei jedem Webbrowser mehrfach getestet, und zwar in insgesamt 78 Testzyklen, die ohne Unterbrechung über 468 Stunden (alle 6 Stunden über 20 Tage) durchgeführt wurden. Unsere Techniker entfernten Muster, die die Validierungskriterien nicht erfüllten, einschließlich solcher, die durch Exploits unbrauchbar waren (nicht Teil des Tests). Letztendlich wurden 950 eindeutige, gültige Schadsoftwaremuster in den endgültigen Satz von 48.672 diskreten, gültigen Schadsoftware-Tests (16.224 Tests pro Webbrowser) aufgenommen, was eine Fehlermarge von weniger als 3,2 Prozent (<3,2 %) bei einem Konfidenzniveau von 95 % ergibt.

Wie wir getestet haben – Schadsoftwaremuster

Die Daten in diesem Test beziehen sich auf einen Testzeitraum von zwanzig (20) Tagen zwischen 11. und 31. Mai 2021. Während des Tests überwachten CyberRatings' Techniker routinemäßig die Konnektivität, um sicherzustellen, dass die getesteten Browser auf Schadsoftware als auch auf Reputationsdienste in der Cloud zugreifen konnten.

Der Schwerpunkt lag auf Aktualität der Muster, wobei ständig neue Muster in den Test aufgenommen und tote Muster entfernt wurden.

Wie wir die Ergebnisse bewertet haben

Wir haben die Fähigkeit der einzelnen Browser gemessen, Schadsoftware so schnell zu blockieren, wie sie auch im Internet entdeckt wurde. Die Techniker wiederholten die Tests alle sechs Stunden, um festzustellen, wie lange ein Anbieter brauchte, den Schutz bereitzustellen oder ob er es überhaupt tat.

Die Leistung aller Browser wurde kontinuierlich gemessen, und die Gesamtschutzrate aller mit den Browsern getesteten Schadsoftwaremuster wurde aufgezeichnet. Die Gesamtschutzrate jedes Browsers wurde berechnet als die Anzahl der erfolgreichen Blockierungen geteilt durch die Gesamtzahl der Testfälle. Wenn beispielsweise alle 6 Stunden Tests durchgeführt werden, wurde ein Schadsoftwaremuster, das 48 Stunden lang online war, acht (8) Mal getestet. Ein Browser, der es bei 6 (von maximal 8) Testläufen blockierte, erreichte eine Schutzrate von 75 %.

Testumgebung

- Microsoft Windows 10 Pro, 21H1

Getestete Produkte

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

Autoren

Thomas Skybakmoen, Vikram Phatak

Testmethodik

CyberRatings Webbrowser-Sicherheitstestmethodik v1.0 ist verfügbar unter www.cyberratings.org

Kontaktinformationen

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

info@cyberratings.org
www.cyberratings.org