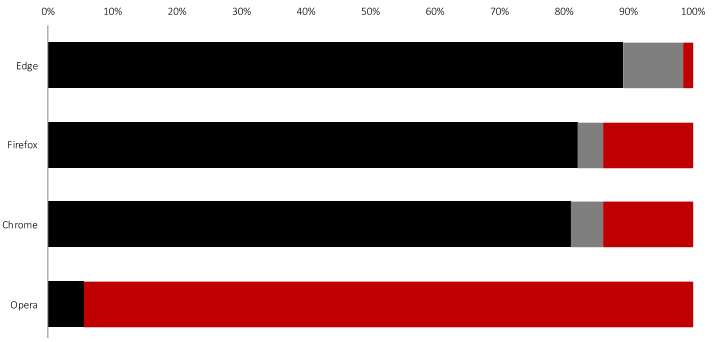
2. Quartal 2020 VERGLEICHENDER TESTBERICHT

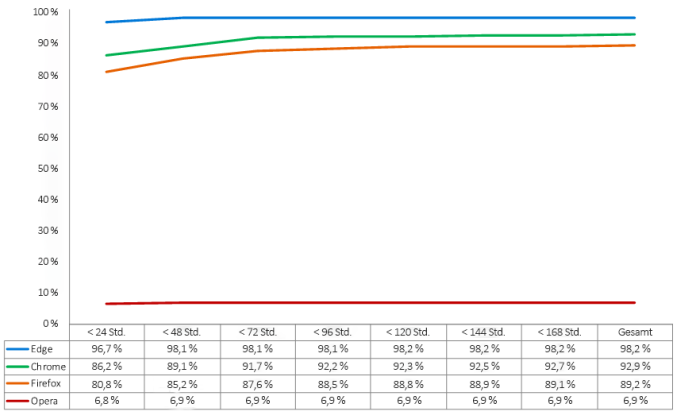
Übersicht

Im 2. Quartal 2020 führte NSS Labs einen unabhängigen Test von Anti-Malware-Browsersoftware durch: 32.267 einzelne Tests (pro Browser) mit 1.065 einmaligen Proben über einen Zeitraum von 34 Tagen. Microsoft Edge schützt sich mit dem Microsoft Defender SmartScreen vor Malware, während Google Chrome und Mozilla Firefox die Google Safe Browsing API verwenden. Opera baut auf Yandex.

Microsoft Edge blockierte 98,5 % der Malware und bot somit den höchsten Schutz. Gleichzeitig überzeugte Microsoft Edge mit der höchsten Zero-Hour-Schutzrate (96,7 %). Firefox folgte direkt dahinter mit 86,1 % blockierter Malware und Google Chrome kam mit 86,0 % auf den dritten Platz. Opera blockte gerade einmal 5,6 % der Malware.



Zusammenfassung der Ergebnisse

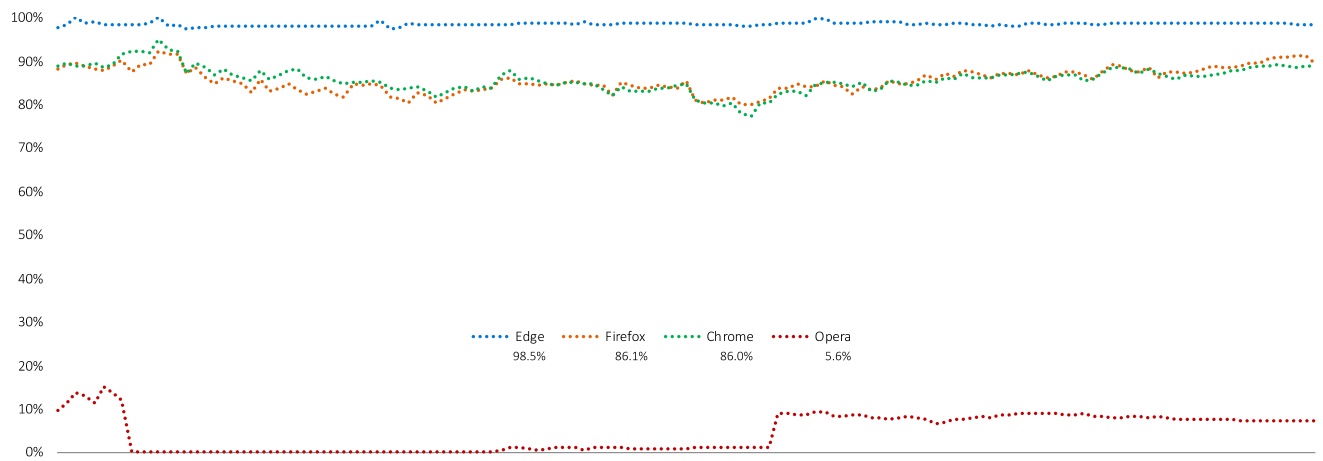


	< 24 Std.	< 48 Std.	< 72 Std.	< 96 Std.	< 120 Std.	< 144 Std.	< 168 Std.	Gesamt
Edge	96,7 %	98,1 %	98,1 %	98,1 %	98,2 %	98,2 %	98,2 %	98,2 %
Chrome	86,2 %	89,1 %	91,7 %	92,2 %	92,3 %	92,5 %	92,7 %	92,9 %
Firefox	80,8 %	85,2 %	87,6 %	88,5 %	88,8 %	88,9 %	89,1 %	89,2 %
Opera	6,8 %	6,9 %	6,9 %	6,9 %	6,9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

Reputationssysteme warnen Benutzer, dass eine URL, eine Datei oder eine Anwendung gefährlich ist, und sorgen so dafür, dass Angreifern die nötige Zeit fehlt, um ihr Ziel zu erreichen. Benutzer besuchen jedoch ständig neue Websites, laden Dateien herunter und installieren Anwendungen. Reputationssysteme können nicht einfach alle neuen Daten blockieren. Malware-Angriff ändern sich ständig und die Mehrzahl der Angriffe erfolgt in den ersten Stunden einer Malware-Kampagne. Die korrekte Klassifizierung von Content ist somit die Voraussetzung für einen erfolgreichen Schutz.

NSS Labs hat die Fähigkeit von Browsern bewertet, Malware umgehend zu blockieren, sobald sie aufgespürt wird. Wir testeten schädliche URLs, Dateien und Anwendungen alle sechs Stunden, um zu sehen, wie lange es dauert, bis ein Anbieter mit einer Schutzfunktion drauf reagiert, bzw., ob er überhaupt reagiert.

Malware-Schutz im Verlauf der Zeit



Während des Tests wurde ständig neue Malware hinzugefügt. URLs, Dateien und Anwendungen, die entweder nicht mehr aufgerufen werden konnten oder von Malware betroffen waren, wurden entfernt. Jeder Datenpunkt wird anhand von Messungen zu einem bestimmten Zeitpunkt berechnet. Wurde die Malware bereits früh blockiert, verbessert sich der Browser-Wert für einen konsistenten Schutz im Verlauf der Zeit. Konnte der Browser die Malware nicht blockieren, verschlechterte sich der Wert.

Tests wurden anhand der Web Browser Test Methodology Version 4.0 (verfügbar auf www.nsslabs.com) durchgeführt.

Dieser Bericht ist vertraulich und ausdrücklich auf die Nutzung durch lizenzierte Kunden von NSS Labs eingeschränkt.

Hintergrund

Social Engineering Malware (SEM)-Angriffe verwenden eine dynamische Kombination gehackter Social Media- und E-Mail-Konten, falscher Benachrichtigungen zu PC-Problemen und sonstiger Betrugsmaschen, um Benutzer dazu zu veranlassen, Malware herunterzuladen. Cyberkriminelle verwenden gehackte E-Mail-Konten, um sich das Vertrauen der Kontakte zu Nutze zu machen, um die Opfer mit scheinbar vertrauenswürdigen Links auf schädliche Dateien zu täuschen. Gehackte Social Media-Konten werden auf die gleiche Weise genutzt. Bei Sozialen Netzwerken ist der Kreis der Betroffenen jedoch noch größer. Freunde und sogar Freunde von Freunden werden getäuscht.

Zu den Social Engineering-Taktiken zählen z. B. Popup-Nachrichten. Sie verweisen darauf, dass Anwendungen, wie z. B. Adobe Flash Player installiert werden müssen, oder dass der PC infiziert ist oder aktualisiert werden muss. Sobald die Malware installiert wurde, werden Benutzer schnell Opfer von Identitätsdiebstahl, einem möglichen Zugriff auf ihr Bankkonto oder sonstigen folgenschweren Angriffen.

Browser-Schutz gegen Malware

Browser verwenden cloudbasierte Reputationssysteme für den Schutz vor Malware. Sie durchsuchen das Internet nach schädlichen Websites und kategorisieren den Inhalt entsprechend, entweder indem sie ihn zu Blockierlisten oder zu Whitelists hinzufügen. Sie können auch eine Bewertung hinzufügen (je nach Ansatz des Anbieters).

Die Kategorisierung kann manuell oder automatisch erfolgen. Der zweite Schritt von Browsern im Kampf gegen Malware ist es, Reputationsinformationen von cloudbasierten Reputationssystemen über bestimmte URLs, Dateien oder Anwendungen abzufragen und vor der Malware zu warnen oder sie zu blockieren.

Verweisen die Ergebnisse auf Malware, zeigt der Browser dem Benutzer eine Warnung an, in der auf eine schädliche URL, Datei oder Anwendung verwiesen wird. Einige Reputationssysteme bieten auch weitere interessante Inhalte zum Thema. Wird der Content als „gut“ eingestuft, unternimmt der Browser nichts. Der Benutzer erfährt nicht, dass der Browser eine Sicherheitsprüfung durchgeführt hat.

Google und Firefox verwenden die Google Safe Browsing API für URL-Reputation und zur Blockierung von Inhalten oder zur Warnung von Benutzern vor dem Herunterladen bestimmter Dateien. Microsoft Edge verwendet Microsoft Defender SmartScreen sowie den Anwendungs-Reputationsservice, um vor Phishing und Malware zu schützen. Opera verwendet eine Kombination von Blockierlisten von Netcraft,[1] PhishTank[2] und Metamask[3] sowie eine Malware-Blockierliste von Yandex.[4]

Mit dem Windows 10-Update im Oktober 2017 wurde zusätzlich Microsoft Defender SmartScreen in das Betriebssystem integriert. Der in das Betriebssystem integrierte SmartScreen-Schutz ist ein Sicherheitsnetz für alle Browser, E-Mail-Clients, USB und sonstige Anwendungen zum Schutz vor Malware.. Benutzer profitieren vom Schutz für Browser-URL, Browser-Anwendung/Dateien sowie vom Schutz des Betriebssystems.

Testaufbau – Malware-Beispiele

Die Daten in diesem Bericht wurden über einen Zeitraum von 34 Tagen zwischen dem 21. April 2020 und dem 25. Mai 2020 gesammelt. Alle Tests wurden in der NSS-Testeinrichtung in Austin, Texas, durchgeführt. Während des Tests überwachten NSS-Techniker routinemäßig die Verbindung, um sicherzustellen, dass die getesteten Browser sowohl Zugriff auf die Malware als auch Zugriff auf die Reputationssysteme in der Cloud hatten.

Der Fokus lag vor allem auf aktuellen Daten. Wir analysierten eine große Anzahl an Fällen, die als Teil des Testsets gespeichert wurden, da wir ständig neue Fälle zum Testen hinzufügten und veraltete Fälle löschten.

Gesamtanzahl der getesteten schädlichen Proben

Insgesamt testeten wir 1.844 rohe, nicht validierte Proben mehrfach für jeden Browser. Daraus ergaben sich insgesamt 182.676 einzelne Tests, die über einen Zeitraum von 822 Stunden (alle 6 Stunden über einen Zeitraum von 34 Tagen) ohne Unterbrechung durchgeführt wurden. NSS-Techniker entfernten Proben, die nicht den Validierungskriterien entsprachen, darunter auch jene, die von Sicherheitsproblemen (ohne Zusammenhang mit diesem Test) betroffen waren. Letztendlich wurden 1.065 individuelle und gültige Malware-Proben in 129.068 einzelnen und gültigen Malware-Tests (32.267 pro Browser) berücksichtigt. Dies führte zu einer Fehlerspanne von weniger als 2 % (<2 %) mit einer statistischen Sicherheit von 95 %.

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

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

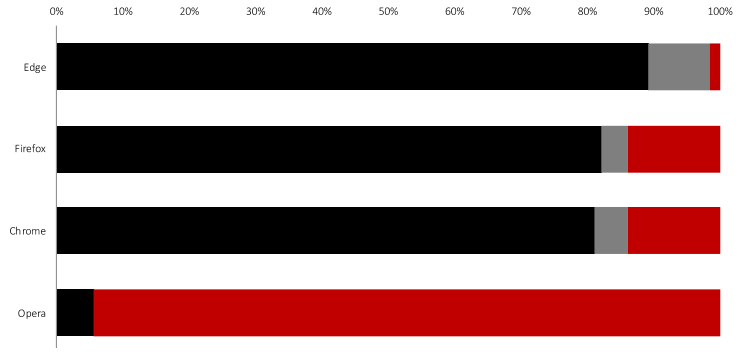
[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

Dieser Bericht ist vertraulich und ausdrücklich auf die Nutzung durch lizenzierte Kunden von NSS Labs eingeschränkt.

Malware-Blockierungsrate

Die Möglichkeit, potenzielle Opfer vor potenziell schädlichen Websites zu warnen, bietet Browsern die einzigartige Chance, gegen Social Engineering-Malware vorzugehen. Malware-Websites sind sehr kurzlebig. Deshalb ist es umso wichtiger, sie schnell zu entdecken, zu validieren, zu klassifizieren und zum Reputationssystem hinzuzufügen. Es versteht sich von selbst, dass gute Reputationssysteme sowohl genau als auch schnell sein müssen, um eine möglichst hohe Anzahl von Bedrohungen aufzuspüren. Browser-Entwickler verstehen dieses Zusammenspiel. In den ersten 24 Stunden wird deutlich mehr Malware blockiert als zu einem späteren Zeitpunkt.



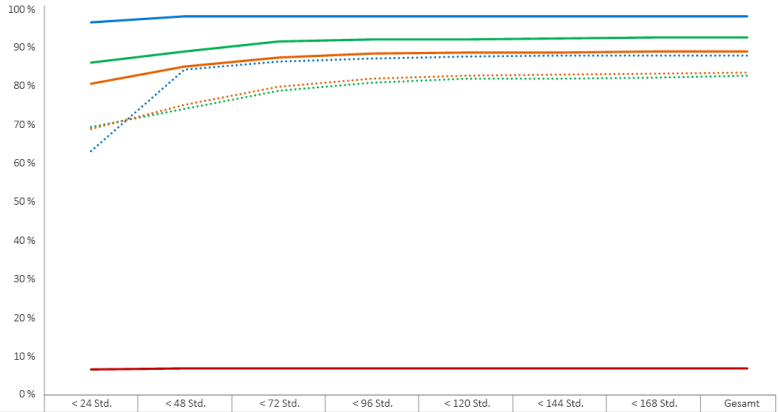
	Opera	Chrome	Firefox	Edge
Rep für URL	5,6 %	80,9 %	82,1 %	89,2 %
Rep für URL + Anwendung	0,0 %	5,0 %	4,0 %	9,3 %
Rep für URL + Anwendung + BS	93,1 %	13,1 %	13,0 %	0,7 %
Nicht blockiert	1,4 %	0,9 %	0,9 %	0,8 %

Die wichtigste Schutztechnologie von Edge ist SmartScreen. SmartScreen bietet URL-basierten Schutz vor Angriffen mithilfe von integrierten, cloudbasierten URL-Reputationssystemen sowie Anwendungsreputation zum Blockieren schädlicher Dateien. SmartScreen blockierte mithilfe von Anwendungsreputation 98,5 % der Bedrohungen in Edge. Mozilla Firefox und Google Chrome verwenden die Safe Browsing API. Firefox blockte 86,1 % der Malware. Google Chrome blockte 86 % der Malware. Opera verwendet eine Kombination aus Blockierlisten diverser Quellen und konnte 5,6 % der Malware blockieren.

Microsoft Defender SmartScreen blockierte zusätzlich 93,1 % der Malware für Opera, 13,1 % für Chrome, 13 % für Firefox und 0,7 % für Edge, als wir versuchten, die Malware zu aktivieren.

Balkendiagramm zum Malware-Schutz

Der umgehende Schutz vor neuer Malware ist das A und O. Malware-Websites werden häufig innerhalb kürzester Zeit deaktiviert, sobald sie entdeckt wurden. Produkte, die nicht rechtzeitig auf Bedrohungen reagieren, sind wahrscheinlich zu spät, um die Bedrohung abzuwenden. Im Balkendiagramm sehen Sie, wie lange die einzelnen Browser brauchten, um Malware zu blockieren, nachdem die Probe im Testzyklus aktiviert wurde. Über einen Zeitraum von 7 Tagen werden täglich kumulative Schutzraten berechnet, bis Bedrohungen blockiert werden.



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

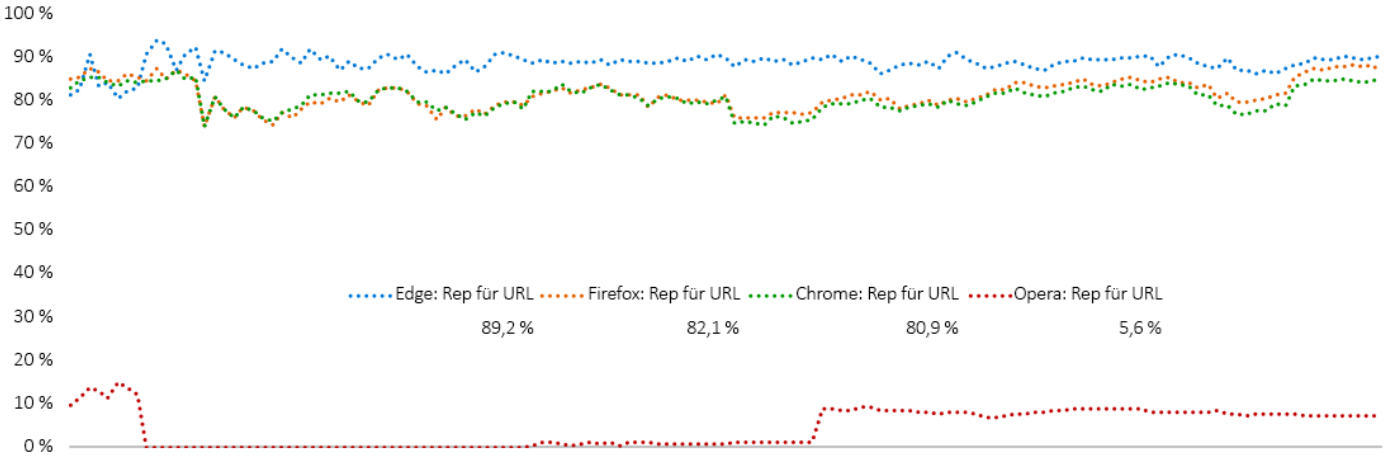
Während des Tests überzeugte Microsoft Edge mit einer anfänglichen Malware-Schutzrate von 96,7 %. Google Chrome und Mozilla Firefox erzielten eine anfängliche Schutzrate von 86,2 % bzw. 80,8 %. Die anfängliche Schutzrate von Opera lag bei 6,8 %. Nach dem 7-Tage-Test konnte bei allen Browsern ein verbesserter Schutz festgestellt werden. Microsoft Edge konnte eine Verbesserung von 4,5 % auf insgesamt 98,2 % verzeichnen. Google Chrome konnte eine Verbesserung von 6,7 % auf insgesamt 92,9 % verzeichnen, während Mozilla Firefox sich um 8,4 % auf insgesamt 89,2 % und Opera um 0,1 % auf insgesamt 6,9 % verbesserte.

Dieser Bericht ist vertraulich und ausdrücklich auf die Nutzung durch lizenzierte Kunden von NSS Labs eingeschränkt.

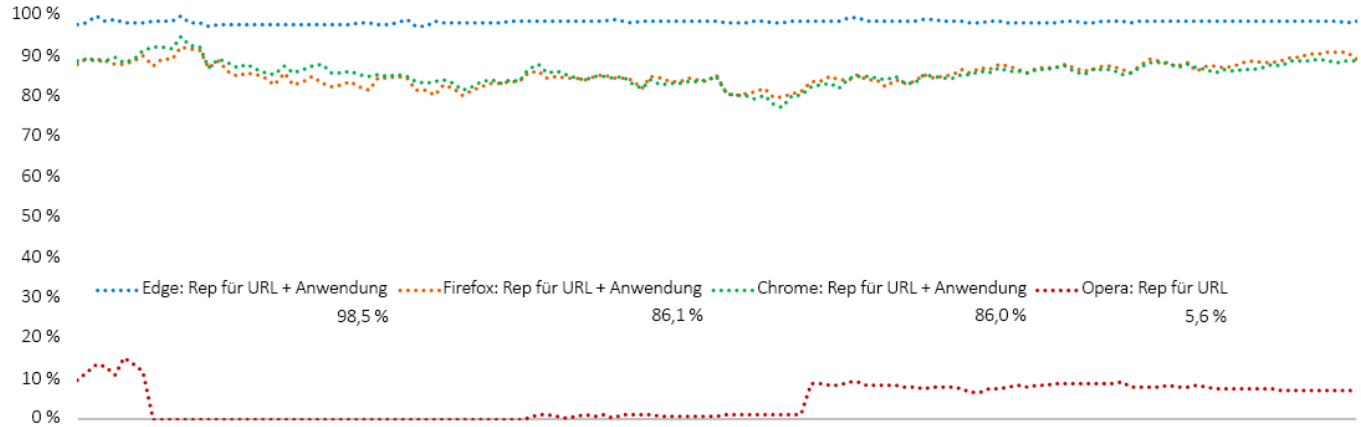
Beständigkeit des Schutzes im Verlauf der Zeit

Während des Tests wurde ständig neue Malware hinzugefügt. URLs, Dateien und Anwendungen, die entweder nicht mehr aufgerufen werden konnten oder von Malware betroffen waren, wurden entfernt. Jeder Datenpunkt wird anhand von Messungen zu einem bestimmten Zeitpunkt berechnet. Wurde die Malware bereits früh blockiert, verbessert sich der Browser-Wert für einen konsistenten Schutz im Verlauf der Zeit. Konnte der Browser die Malware nicht blockieren, verschlechterte sich der Wert.

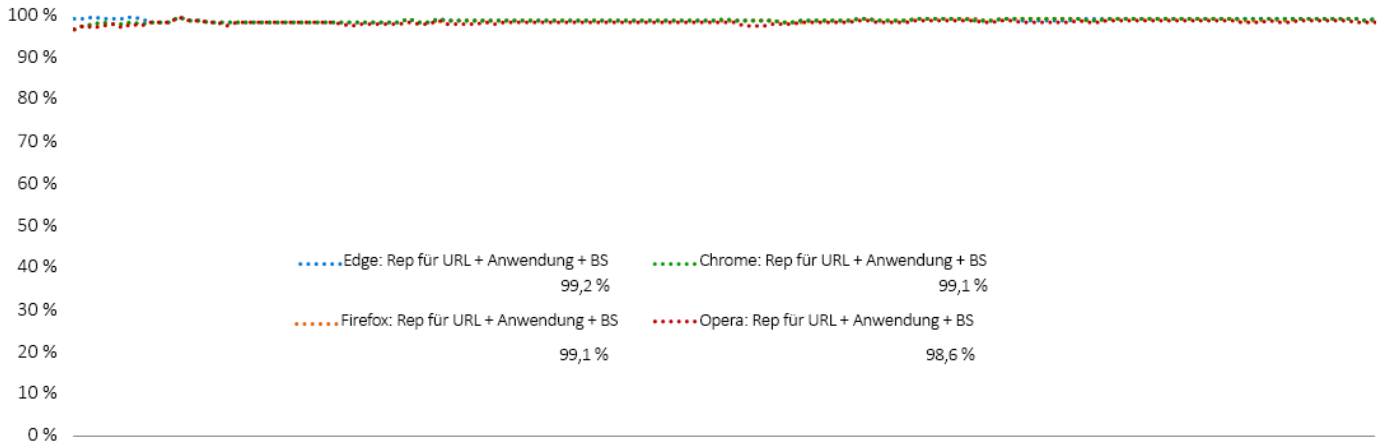
Während der Tests kristallisierten sich drei Aspekte für den Schutz heraus: URL-Reputation, Anwendungsreputation im Browser und Anwendungsreputation im Betriebssystem. Die URL-Reputation bietet einen angemessenen Schutz.



Durch zusätzliche Anwendungsreputation konnte der Schutz erhöht werden.



Die im Betriebssystem integrierte Reputation bietet eine weitere Barriere im Kampf gegen Malware. Idealerweise blockiert der Browser die Malware, damit sie nie bis zum Betriebssystem vordringt. Die Tests haben jedoch ergeben, dass die ins Betriebssystem integrierte Reputation äußerst effektiv ist.



Dieser Bericht ist vertraulich und ausdrücklich auf die Nutzung durch lizenzierte Kunden von NSS Labs eingeschränkt.

Testumgebung

- BaitNET™ (NSS Labs Proprietary)
- 64-Bit Microsoft Windows 10 Pro (Version 1909 Build: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (Kernel-Version 4.19.0-kali5-amd64)
- VMware vCenter (Version 6.7u2 Build 6.7.0.30000)
- VMware vSphere (Version 6.7.0.20000)
- VMware ESXi (Version 6.7u3 Build 14320388)
- VMware Tools 10.3.5
- Wireshark Version 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

Getestete Produkte

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

Dieser Bericht ist vertraulich und ausdrücklich auf die Nutzung durch lizenzierte Kunden von NSS Labs eingeschränkt.

Autoren

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Testmethodik

NSS Labs Web Browser Security (WBS) Test Methodology Version 4.0, verfügbar unter www.nsslabs.com.

Kontaktinformationen

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com

Diese und dazugehörige Dokumente sind hier verfügbar: www.nsslabs.com. Bitte wenden Sie sich an NSS Labs, um eine lizenzierte Kopie zu erhalten oder Missbrauch zu melden.

© 2020 NSS Labs, Inc. Alle Rechte vorbehalten. Dieses Dokument oder Teile davon dürfen nicht vervielfältigt, kopiert/gescannt, auf einem Abfragesystem gespeichert, per E-Mail versendet oder anderweitig freigegeben oder übertragen werden, sofern keine ausdrückliche schriftliche Genehmigung von NSS Labs, Inc. („Uns“ oder „Wir“) vorliegt.

Bitte lesen Sie diesen Haftungsausschluss, da er wichtige und bindende Informationen enthält. Sollten Sie diesen Bedingungen nicht zustimmen, bitten wir Sie, nicht weiterzulesen, sondern den Bericht umgehend an uns zurückzugeben. „Sie“ oder „Ihre“ bezieht sich auf die Person, die auf diesen Bericht zugreift, sowie auf alle Personen/Einrichtungen für die diese Person den Bericht entgegen nimmt.

1. Änderungen für Informationen in diesem Bericht sind vorbehalten. Wir sind nicht verpflichtet, diese Informationen zu aktualisieren.

2. Wir gehen von der Richtigkeit und Zuverlässigkeit der Daten zum Zeitpunkt der Veröffentlichung aus. Eine Garantie wird jedoch ausgeschlossen. Sie verwenden diesen Bericht auf eigenes Risiko. Wir sind nicht für Schäden, Verluste oder Kosten jedweder Natur verantwortlich, die sich durch Fehler oder Auslassungen in diesem Bericht ergeben könnten.

3. WIR ÜBERNEHMEN KEINE GARANTIE, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND. SÄMTLICHE IMPLIZIERTEN GARANTIEN, EINSCHLIESSLICH IMPLIZIERTE ZUSICHERUNGEN DER GEBRAUCHSTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SOWIE IMPLIZIERTE GARANTIEN DES NICHTVERSTOSSES WERDEN HIERMIT FÜR NICHTIG ERKLÄRT UND AUSGESCHLOSSEN WIR HAFTEN IN KEINEM FALL FÜR DIREKTE, RESULTIERENDE, ZUFÄLLIGE, STRAF-, EXEMPLARISCHE ODER INDIREKTE SCHÄDEN ODER SCHADENERSATZANSPRÜCHE, GEWINNVERLUSTE, DATENVERLUSTE, VERLUSTE VON COMPUTER-PROGRAMMEN ODER SONSTIGEN VERMÖGENSWERTEN, AUCH WENN ÜBER DIE MÖGLICHKEITEN SOLCHER SCHÄDEN INFORMIERT WURDE.

4. Dieser Bericht stellt keine Werbung, Empfehlung oder Garantie für eines der getesteten Produkte (Hardware oder Software) oder für Hardware und/oder Software, die für die Tests der Produkte verwendet wurde, dar. Die Tests stellen keinerlei Garantie dar, dass die Produkte fehler- oder schadensfrei sind, dass die Produkte Ihren Erwartungen, Anforderungen, Bedürfnissen oder Spezifikationen entsprechen oder sie fehlerfrei funktionieren.

5. Dieser Bericht stellt keine Werbung, Unterstützung, Partnerschaft oder Verifizierung mit einer der erwähnten Organisationen dar.

6. Alle Markenzeichen, Dienstleistungszeichen und Markennamen in diesem Bericht sind Eigentum ihrer jeweiligen Inhaber.