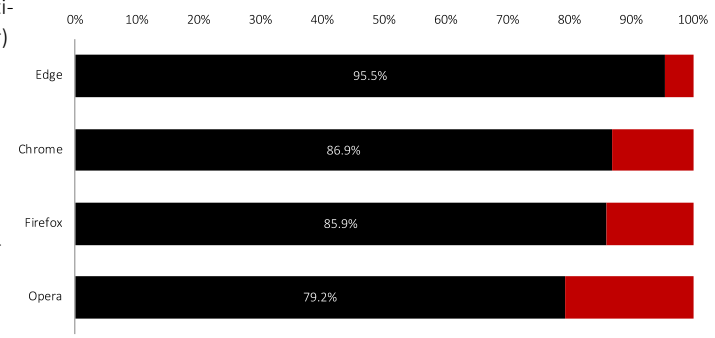
2. Quartal 2020 VERGLEICHENDER TESTBERICHT

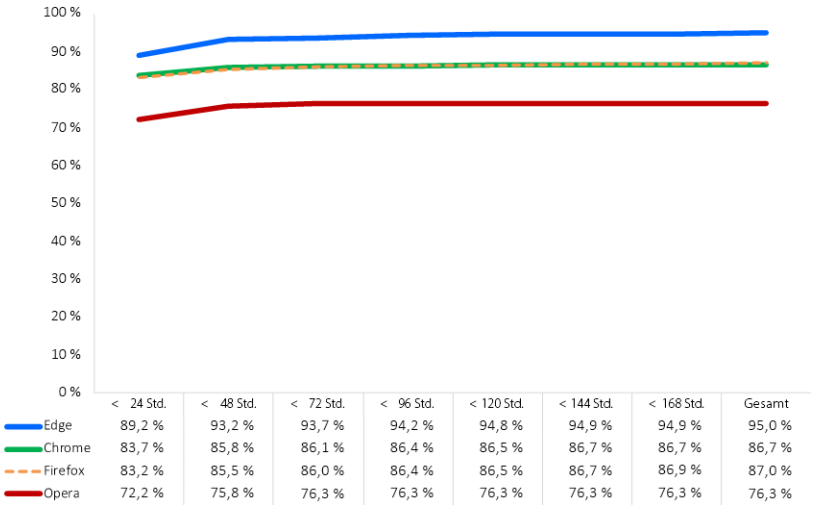
Übersicht

Im 2. Quartal 2020 führte NSS Labs einen unabhängigen Test von Anti-Phishing-Browsersoftware durch: 47.274 einzelne Tests (pro Browser) mit 2.443 einmaligen Phishing-URLs über einen Zeitraum von 18 Tagen. Microsoft Edge schützt sich mit dem Microsoft Defender SmartScreen vor Phishing, während Google Chrome und Mozilla Firefox die Google Safe Browsing API verwenden. Opera verwendet eine Kombination aus Blockierlisten von Drittanbietern.

Microsoft Edge blockierte 95,5 % der Phishing-URLs und bot somit den höchsten Schutz. Gleichzeitig überzeugte Microsoft Edge mit der höchsten Zero-Hour-Schutzrate (89,2 %). Google Chrome folgte direkt dahinter mit 86,9 % blockierten Phishing-URLs und Firefox kam mit 85,9 % auf den dritten Platz. Opera blockte gerade einmal 79,2 % der Phishing-URLs.



Zusammenfassung der Ergebnisse

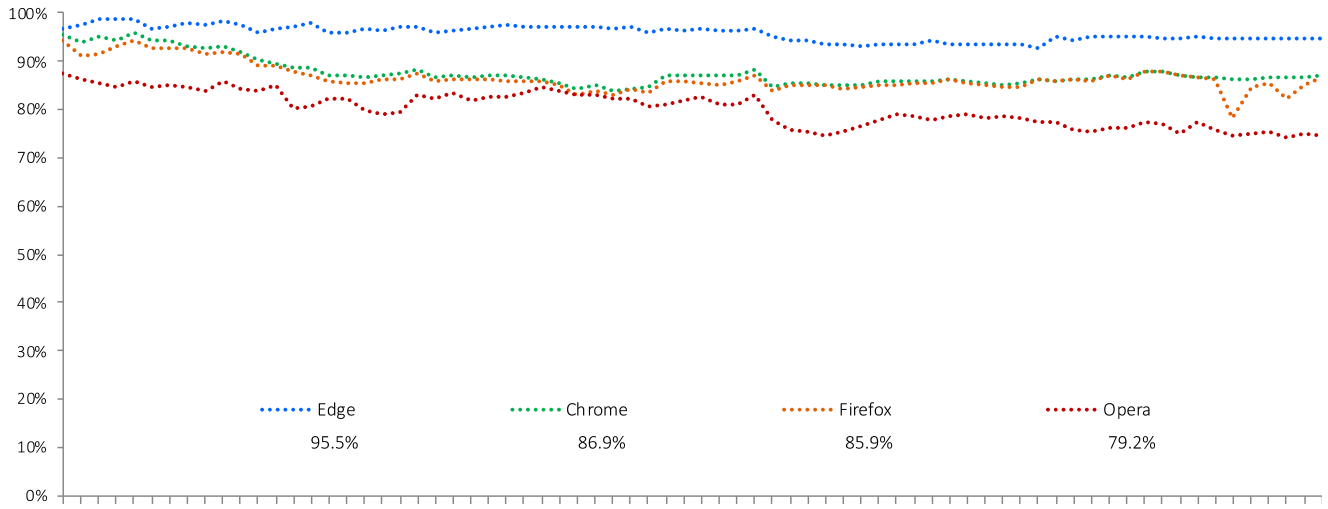


	< 24 Std.	< 48 Std.	< 72 Std.	< 96 Std.	< 120 Std.	< 144 Std.	< 168 Std.	Gesamt
Edge	89,2 %	93,2 %	93,7 %	94,2 %	94,8 %	94,9 %	94,9 %	95,0 %
Chrome	83,7 %	85,8 %	86,1 %	86,4 %	86,5 %	86,7 %	86,7 %	86,7 %
Firefox	83,2 %	85,5 %	86,0 %	86,4 %	86,5 %	86,7 %	86,9 %	87,0 %
Opera	72,2 %	75,8 %	76,3 %	76,3 %	76,3 %	76,3 %	76,3 %	76,3 %

URL-Reputationssysteme warnen Benutzer, dass eine URL eine bekannte Phishing-Website ist, und sorgen so dafür, dass Angreifern die nötige Zeit fehlt, um ihr Ziel zu erreichen. Benutzer besuchen jedoch eine große Anzahl an Websites und viele davon sind neu. URL-Reputationssysteme können nicht einfach alle neuen Seiten blockieren. Phishing-Angriffe ändern sich ständig und die Mehrzahl der Angriffe erfolgt in den ersten Stunden eines Angriffs.

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

Phishing-Schutz im Verlauf der Zeit



Während des Tests wurden täglich neue Phishing-URLs hinzugefügt. URLs, die nicht mehr erreichbar waren oder keine Phishing-Angriffe mehr ausführten, wurden entfernt. Jeder Datenpunkt stellt den Schutz zu einem bestimmten Zeitpunkt dar. Wurde die URL bereits früh blockiert, verbessert sich der Browser-Wert für einen konsistenten Schutz im Verlauf der Zeit. Konnte der Browser die URL nicht blockieren, verschlechterte sich der Wert.

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

Hintergrund

Phishing ist ein Social Engineering-Angriff, bei dem das Opfer überzeugt werden soll, dem Angreifer vertrauliche persönliche Daten zur Verfügung zu stellen. Einige Beispiele hierfür sind Kreditkartennummern, Sozialversicherungsnummern sowie Anmeldedaten und Passwörter für Bankkonten. E-Mail-Adressen, Instant Messages, SMS und Links auf Sozialen Netzwerken sind beliebte Ziele für Phishing-Angriffe. Die Startseite einer Phishing-Website dient häufig dazu heimlich still und leise den Computer des Besuchers zu infizieren und schädliche Software zu installieren (ein sogenannter Drive-By-Angriff).

Phishing-Angriffe stellen ein großes Risiko für Privatpersonen und Organisationen dar, denn Sie drohen damit, vertrauliche persönliche Daten oder Geschäftsdaten auszuspionieren und zu beschädigen. Die Anti-Phishing Working Group (APWG) meldete im ersten Quartal 2020 insgesamt 165.772 individuelle E-Mail-Phishing-Kampagnen.[1] Phishing-Angriffe werden immer komplexer und moderner. Sie sind dadurch noch schwerer aufzuspüren und zu verhindern.

Browser-Schutz gegen Phishing

Phishing-Schutz wird über eine Anwendung im Browser bereitgestellt, die die URL-Reputation von einem Reputationsserver in der Cloud abruft. Der Reputationsserver durchsucht das Internet auf Phishing-Websites, weist anschließend jeder URL einen Wert zu und fügt sie zur Blockierliste hinzu. Wenn ein Browser eine URL aufruft, fragt der Phishing-Schutz des Browsers (z. B. Safe Browsing, SmartScreen etc.) die Reputation der URL vom cloudbasierten Reputationsserver ab. Handelt es sich um eine schädliche Website, leitet der Browser den Benutzer zu einer Warnmeldung weiter, in der er auf die Schädlichkeit der Website hingewiesen wird. Einige Reputationssysteme bieten auch weitere interessante Inhalte zum Thema. Wird eine Website als „gut“ eingestuft, unternimmt der Browser nichts. Der Benutzer erfährt nicht, dass der Browser eine Sicherheitsprüfung durchgeführt hat.

Testaufbau – Phishing-URLs

Die Daten in diesem Bericht wurden über einen Zeitraum von 18 Tagen zwischen dem 21. April 2020 und dem 8. 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 URLs als auch Zugriff auf die Reputationssysteme in der Cloud hatten.

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

Gesamtanzahl der schädlichen URLs im Test

Insgesamt testeten wir 4.020 rohe, nicht validierte URLs mehrfach für jeden Browser. Daraus ergaben sich insgesamt 222.527 einzelne Tests, die über einen Zeitraum von 430 Stunden (alle 6 Stunden über einen Zeitraum von 18 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 2.443 individuelle und gültige Phishing-URLs in 189.096 einzelnen und gültigen Phishing-Tests (47.274 pro Browser) berücksichtigt. Dies führte zu einer Fehlerspanne von weniger als 2 % (<2 %) mit einer statistischen Sicherheit von 95 %.

Durchschnittliche Anzahl hinzugefügter schädlicher URLs pro Tag

Im Durchschnitt wurden pro Tag 136 neue validierte URLs zum Testset hinzugefügt. Aufgrund der Schwankungen der kriminellen Aktivitäten an einigen Tagen, wich auch diese Zahl an manchen Tagen ab.

Blockieren von Phishing-URLs

NSS hat die Fähigkeit von Browsern bewertet, schädliche URLs umgehend zu blockieren, sobald sie aufgespürt werden. Techniker wiederholten diese Tests alle sechs Stunden, um zu sehen, wie lange es dauert, bis ein Anbieter mit einer Schutzfunktion drauf reagiert, bzw., ob er überhaupt reagiert.

Microsoft Edge basiert auf Chromium und wurde am 15. Januar 2020 vorgestellt. Der Browser ist kompatibel mit allen unterstützten Versionen von Windows und macOS. Durch das Herunterladen des Browsers wird die veraltete Version von Microsoft Edge auf Windows 10 PCs ersetzt.

https://support.microsoft.com/de-de/help/4501095/download-the-new-microsoft-edge-based-on-chromium

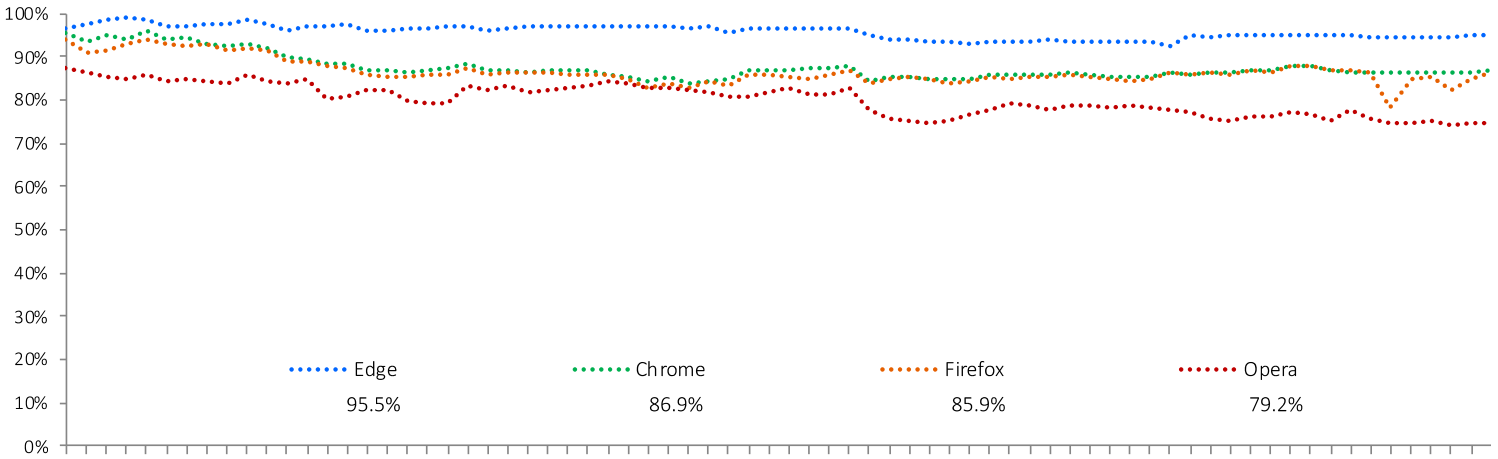
[1] APWG Phishing Activity Trends Report

Phishing-Blockierungsrate

Google Chrome und Mozilla Firefox verwenden die Google Safe Browsing API. 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,[2] PhishTank[3] und Metamask[4] sowie eine Malware-Blockierliste von Yandex.[5]
Die Möglichkeit, potenzielle Opfer vor potenziell schädlichen Websites zu warnen, bietet Browsern die einzigartige Chance, gegen Phishing und sonstige kriminelle Aktivitäten vorzugehen. Phishing-Websites sind sehr kurzlebig. Deshalb ist es umso wichtiger, sie schnell zu entdecken, zu validieren, zu klassifizieren und zum Reputationssystem hinzuzufügen. Dies erklärt die Korrelation zwischen der durchschnittlichen Zeit bis zu Blockierung und der Erkennungsrate. Es versteht sich von selbst, dass gute Reputationssysteme sowohl genau als auch schnell sein müssen, um eine möglichst hohe Erkennungsrate zu erzielen. Browser-Entwickler verstehen dieses Zusammenspiel. In den ersten 24 Stunden wird deutlich mehr Phishing blockiert als zu einem späteren Zeitpunkt.

Wir führten eine kontinuierliche Messung der individuellen Leistung der Browser beim Blockieren durch und zeichneten die allgemeine Blockierrate bei allen getesteten URLs auf. Die allgemeine Blockierrate eines Browsers ergibt sich aus der Anzahl der erfolgreichen Blockierungen, geteilt durch die Gesamtanzahl der Testfälle. Bei einer Testwiederholung alle 6 Stunden, wird eine URL, die 48 Stunden online ist, 8 Mal getestet. Ein Browser, der die URL beim 6. Testlauf (von maximal 8) blockiert, erzielt eine Blockierrate von 75 %.

Beständigkeit des Schutzes im Verlauf der Zeit



Während des Tests wurden täglich neue Phishing-URLs hinzugefügt. URLs, die nicht mehr erreichbar waren oder keine Phishing-Angriffe mehr ausführten, wurden entfernt. Jeder Datenpunkt stellt den Schutz zu einem bestimmten Zeitpunkt dar. Wurde die URL bereits früh blockiert, verbessert sich der Browser-Wert für einen konsistenten Schutz im Verlauf der Zeit. Konnte der Browser die URL nicht blockieren, verschlechterte sich der Wert.

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

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

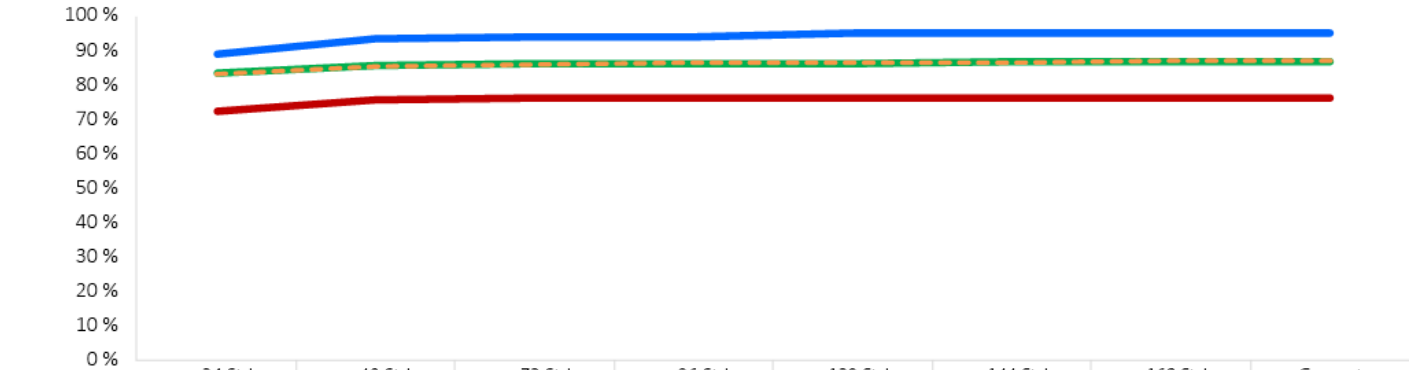
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

Balkendiagramm zum Phishing-Schutz

Der umgehende Schutz vor neuen Phishing-URLs ist das A und O. Phishing-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 eine Phishing-Website zu blockieren, nachdem die Bedrohung im Testzyklus aktiviert wurde. Über einen Zeitraum von 7 Tagen werden täglich kumulative Schutzraten berechnet, bis Bedrohungen blockiert werden.

Während des Tests überzeugte Microsoft Edge mit einer anfänglichen Phishing-Schutzrate von 89,2 %. Google Chrome und Mozilla Firefox erzielten eine anfängliche Schutzrate von 83,7 % bzw. 83,2 %. Die anfängliche Schutzrate von Opera lag bei 72,2 %. Nach dem 7-Tage-Test konnte bei allen Browsern ein verbesserter Schutz festgestellt werden. Microsoft Edge konnte eine Verbesserung von 5,7 % auf insgesamt 94,9 % verzeichnen. Mozilla Firefox erzielte eine Verbesserung von 3,7 % auf insgesamt 86,9 % und Google Chrome verbesserte sich um 3 % auf insgesamt 86,7 %. Opera konnte eine Verbesserung von 4,1 % auf insgesamt 76,3 % verzeichnen.



	< 24 Std.	< 48 Std.	< 72 Std.	< 96 Std.	< 120 Std.	< 144 Std.	< 168 Std.	Gesamt
Edge	89,2 %	93,2 %	93,7 %	94,2 %	94,8 %	94,9 %	94,9 %	95,0 %
Chrome	83,7 %	85,8 %	86,1 %	86,4 %	86,5 %	86,7 %	86,7 %	86,7 %
Firefox	83,2 %	85,5 %	86,0 %	86,4 %	86,5 %	86,7 %	86,9 %	87,0 %
Opera	72,2 %	75,8 %	76,3 %	76,3 %	76,3 %	76,3 %	76,3 %	76,3 %

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 – 84.0.502.0
- Mozilla Firefox: Version 75.0 – 76.0.1
- Opera: Version: 67.0.3575.137 – 68.0.3618.125

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