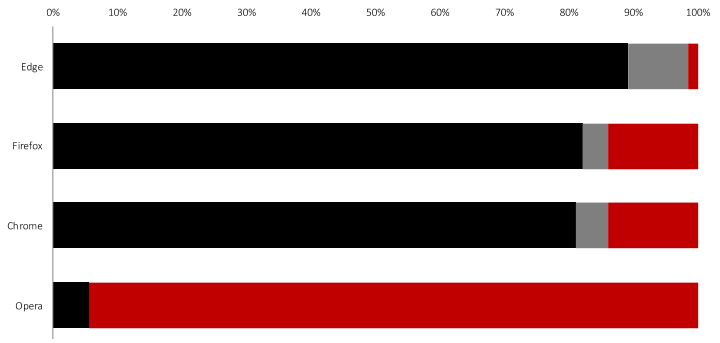
T2 2020 RAPPORT DE TEST COMPARATIF

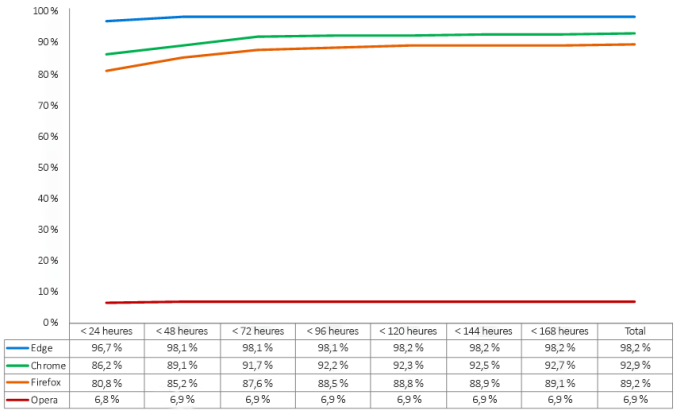
Vue d'ensemble

Au cours du deuxième trimestre 2020, NSS Labs a effectué un test indépendant de la protection contre les logiciels malveillants proposée par les navigateurs web : il s'agit de 32 267 tests distincts (par navigateur web) utilisant 1 065 échantillons uniques sur une période de 34 jours. Pour se protéger des logiciels malveillants, Microsoft Edge utilise Microsoft Defender SmartScreen ; Google Chrome et Mozilla Firefox utilisent l'API de navigation sécurisée de Google ; et Opera utilise Yandex.

Microsoft Edge a offert la meilleure protection, en bloquant 98,5 % des logiciels malveillants, tout en offrant le taux de protection zéro heure le plus élevé (96,7 %). Firefox a fourni la deuxième protection la plus élevée, bloquant 86,1 % de ces logiciels en moyenne, suivi de Google Chrome, qui en a bloqué 86,0 %. Opera a bloqué 5,6 % des fichiers malveillants.



Résumé des résultats

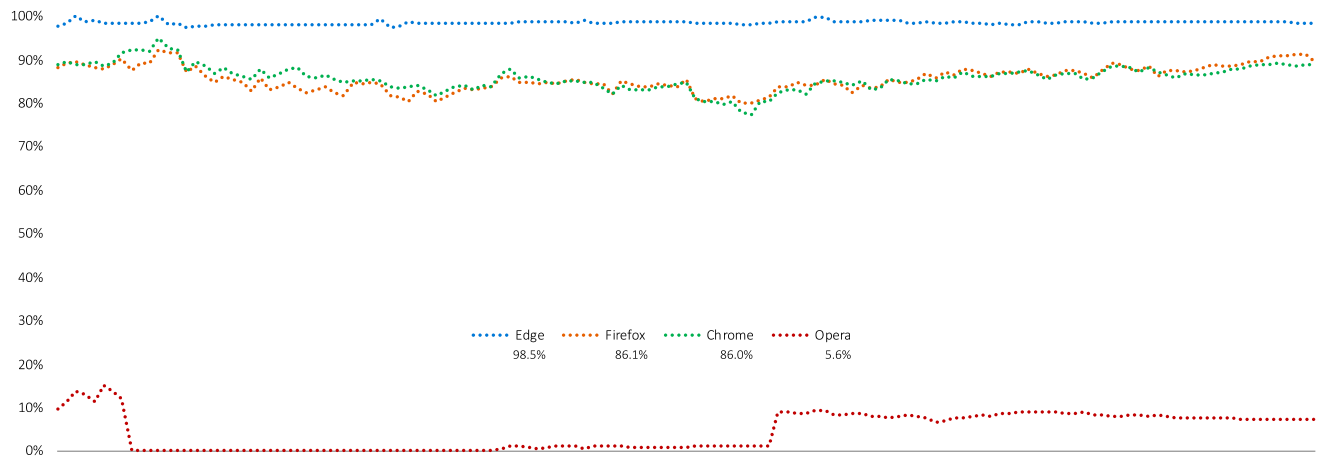


	< 24 heures	< 48 heures	< 72 heures	< 96 heures	< 120 heures	< 144 heures	< 168 heures	Total
Edge	96,7 %	98,1 %	98,1 %	98,1 %	98,2 %	98,2 %	98,2 %	98,2 %
Chrome	86,2 %	89,1 %	91,7 %	92,2 %	92,3 %	92,5 %	92,7 %	92,9 %
Firefox	80,8 %	85,2 %	87,6 %	88,5 %	88,8 %	88,9 %	89,1 %	89,2 %
Opera	6,8 %	6,9 %	6,9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

Les systèmes de réputation réduisent le temps dont disposent les attaquants pour atteindre leurs objectifs en prévenant les utilisateurs qu'une URL, un fichier ou une application présente un danger ou en les empêchant de les ouvrir. Cependant, les utilisateurs visitent constamment de nouveaux sites web, téléchargent des fichiers et installent des applications. Les systèmes de réputation ne peuvent pas simplement bloquer tout ce qui est nouveau. Sachant cela, les campagnes de logiciels malveillants des attaquants changent constamment et la majorité des attaques se produisent dans les premières heures suivant le lancement d'une campagne. C'est pourquoi une classification rapide et précise du contenu est la clé d'une protection efficace.

NSS Labs a évalué la capacité des navigateurs à bloquer les logiciels malveillants aussi rapidement que nous les avons trouvés sur Internet. Nous avons continué à tester les URL, les fichiers et les applications représentant une menace toutes les six heures afin de déterminer si le fournisseur ajoutait une protection et son temps de réaction.

Protection contre les logiciels malveillants au fil du temps



Tout au long du test, de nouveaux logiciels malveillants ont été constamment ajoutés. Les URL, les fichiers et les applications qui n'étaient plus accessibles ou qui hébergeaient des logiciels malveillants ont été supprimés. Chaque point de données est calculé à partir de mesures enregistrées à un moment précis. Si le logiciel malveillant était bloqué dès le début, le score du navigateur pour la cohérence de la protection dans le temps augmentait. Par contre, si le navigateur ne bloquait pas le logiciel malveillant, le score diminuait.

Les tests se basaient sur la méthodologie de test des navigateurs web v4.0 (disponible à l'adresse www.nsslabs.com).

Contexte

Les attaques de logiciels malveillants d'ingénierie sociale (SEM) utilisent une combinaison dynamique de médias sociaux, de comptes de messagerie détournés, de fausses notifications de problèmes informatiques et d'autres tromperies pour encourager les utilisateurs à télécharger des logiciels malveillants. Les cybercriminels utilisent des comptes de messagerie détournés pour profiter de la confiance implicite entre les contacts et tromper les victimes en leur faisant croire que les liens vers des fichiers malveillants sont dignes de confiance. Les comptes de médias sociaux détournés sont utilisés de la même manière que les comptes de messagerie détournés. Dans le cas des réseaux sociaux, cependant, le cercle s'élargit : les amis et même les amis des amis risquent d'être trompés.

Les tactiques d'ingénierie sociale peuvent utiliser des messages contextuels ; par exemple, informer les utilisateurs que des applications telles qu'Adobe Flash Player doivent être installées ou que leurs ordinateurs sont infectés ou nécessitent des mises à jour. Une fois le logiciel malveillant installé, les victimes sont vulnérables au vol d'identité, au piratage de leur compte bancaire et à d'autres conséquences potentiellement dévastatrices.

Protection des navigateurs web contre les logiciels malveillants

Pour se protéger des logiciels malveillants, les navigateurs utilisent des systèmes de réputation basés sur le cloud qui parcourent Internet à la recherche de sites web malveillants et classent ensuite le contenu en conséquence, soit en l'ajoutant à des listes autorisées ou à des listes rouges, soit en lui attribuant une note (selon l'approche du fournisseur).

Ces techniques de catégorisation peuvent être effectuées manuellement ou automatiquement. La deuxième composante fonctionnelle de la protection contre les logiciels malveillants consiste, pour le navigateur web, à demander aux systèmes de réputation basés sur le cloud des informations sur des URL, des fichiers ou des applications spécifiques, puis à mettre en garde contre le logiciel malveillant ou à le bloquer.

Si les résultats signalent la présence d'un logiciel malveillant, le navigateur web redirige l'utilisateur vers un message d'avertissement expliquant le caractère malveillant de l'URL, du fichier ou de l'application. Certains systèmes de réputation comprennent également un contenu éducatif supplémentaire. À l'inverse, si le contenu est jugé « bon », le navigateur web n'intervient pas et l'utilisateur ne sait pas qu'un contrôle de sécurité vient d'être effectué par le navigateur.

Google et Firefox utilisent l'API Google Safe Browsing à la fois pour la réputation des URL et pour bloquer ou avertir les utilisateurs du téléchargement de certains types de fichiers. Microsoft Edge utilise Microsoft Defender SmartScreen, y compris son service de réputation des applications, pour assurer une protection contre l'hameçonnage et les menaces de logiciels malveillants. Opera utilise une combinaison de listes rouges de Netcraft,[1] PhishTank[2] et Metamask[3], ainsi qu'une liste noire des logiciels malveillants de Yandex.[4]

De plus, Microsoft Defender SmartScreen a été intégré comme une fonctionnalité à l'échelle du système d'exploitation avec la mise à jour Windows 10 d'octobre 2017. La version du système d'exploitation de la protection SmartScreen est un filet de sécurité pour tous les navigateurs, clients de messagerie, USB et autres applications dans le cadre de la protection du système d'exploitation contre les logiciels malveillants. Les utilisateurs bénéficient donc de la protection des URL des navigateurs, de la protection des applications/fichiers des navigateurs, ainsi que de la protection du système d'exploitation.

Composition du test – Échantillons de logiciels malveillants

Les données de ce rapport couvrent une période d'essai de 34 jours entre le 21 avril 2020 et le 25 mai 2020. Tous les tests ont été effectués dans les installations d'essai du NSS à Austin, Texas. Pendant le test, les ingénieurs du NSS ont régulièrement contrôlé la connectivité pour s'assurer que les navigateurs testés pouvaient accéder aux logiciels malveillants, ainsi qu'aux services de réputation sur le cloud.

L'accent a été mis sur le caractère récent des logiciels. Ainsi, un plus grand nombre d'échantillons ont été évalués que ceux qui ont été finalement retenus dans le cadre de la série de tests résultants, puisque de nouveaux échantillons étaient constamment ajoutés au test et que les échantillons morts en étaient retirés.

Nombre total d'échantillons malveillants testés

Au total, 1 844 échantillons bruts non validés ont été testés à plusieurs reprises avec chaque navigateur web, pour un total de 182 676 tests distincts effectués sans interruption pendant 822 heures (toutes les 6 heures pendant 34 jours). Les ingénieurs du NSS ont retiré les échantillons qui ne répondaient pas aux critères de validation, y compris ceux qui étaient corrompus par des exploits (ne faisant pas partie de ce test). À la fin, 1 065 échantillons de logiciels malveillants uniques et valides ont été inclus dans 129 068 tests distincts et valides (32 267 par navigateur web), ce qui donne une marge d'erreur inférieure à 2 % (<2 %) avec un niveau de confiance de 95 %.

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

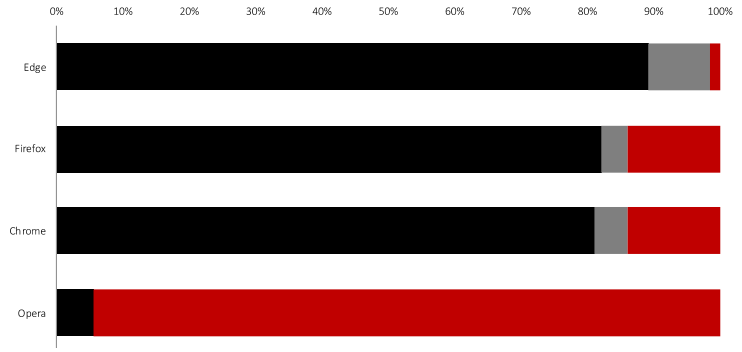
[2] http://www.phishtank.com/

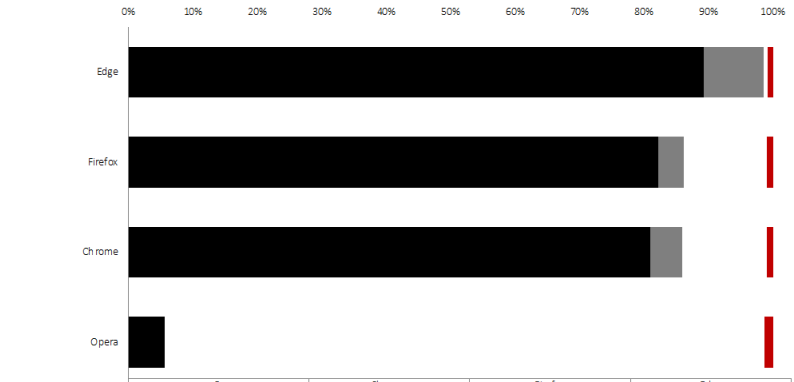
[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

Taux de blocage des logiciels malveillants

La possibilité d'avertir les victimes potentielles qu'elles sont sur le point de s'égarer sur un site web malveillant place les navigateurs web dans une position unique pour combattre les logiciels malveillants d'ingénierie sociale. Comme les sites malveillants ont une durée de vie courte, il est essentiel que le site soit découvert, validé, classé et ajouté au système de réputation le plus rapidement possible. Ainsi, un bon système de réputation doit être à la fois précis et rapide afin d'atteindre des taux de capture élevés. Les développeurs de navigateurs comprennent clairement cette relation, et un nombre nettement plus important de logiciels malveillants sont bloqués dans les 24 premières heures suivant leur détection qu'après ce délai.





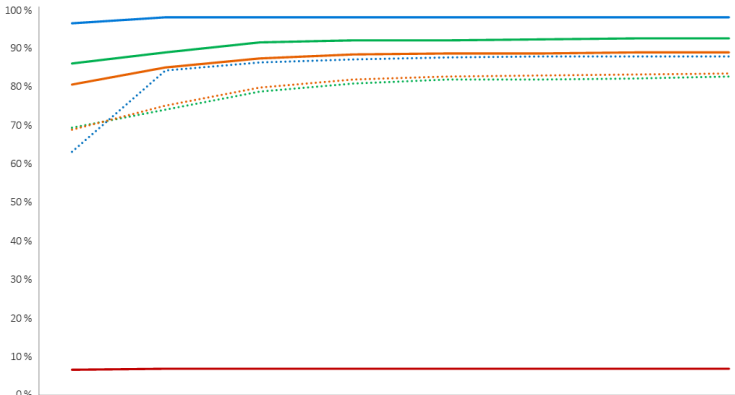
	Opera	Chrome	Firefox	Edge
Réputation d'URL	5,6%	80,9%	82,1%	89,2%
Réputation d'URL + réputation d'application	0,0%	5,0%	4,0%	9,3%
Réputation d'URL + réputation d'application + réputation du SE	93,1%	13,1%	13,0%	0,7%
Échec	1,4%	0,9%	0,9%	0,8%

La technologie de protection de base d'Edge est SmartScreen, qui offre une protection contre les attaques par URL au moyen d'un service intégré de réplication d'URL sur le cloud, ainsi qu'une réputation d'application pour le blocage des fichiers malveillants. SmartScreen avec la réputation de l'application a bloqué 98,5 % pour Edge. Mozilla Firefox et Google Chrome utilisent l'API Safe Browsing. Firefox a bloqué 86,1 des fichiers malveillants. Google Chrome bloqué à 86,0 % des fichiers malveillants. Opera, qui utilise une combinaison de listes rouges provenant de plusieurs sources, a bloqué 5,6 % des fichiers malveillants.

De plus, Microsoft Defender SmartScreen a bloqué 93,1 % supplémentaires pour Opera, 13,1 % pour Chrome, 13,0 % pour Firefox et 0,7 % de fichiers malveillants pour Edge lorsque nous avons tenté de les exécuter.

Histogramme de protection contre les logiciels malveillants

Une protection immédiate contre les nouveaux logiciels malveillants est essentielle. Lorsque les sites qui hébergent des logiciels malveillants sont découverts, ils sont supprimés, souvent dans un délai relativement court. Les produits qui n'ajoutent pas de protection en temps utile peuvent avoir une action trop tardive pour contrer une menace. L'histogramme montre le temps que chaque navigateur a mis pour bloquer les logiciels malveillants une fois l'échantillon introduit dans le cycle de test. Dans la fenêtre de sept jours, les taux de protection cumulés sont calculés chaque jour jusqu'à ce que les menaces soient bloquées.



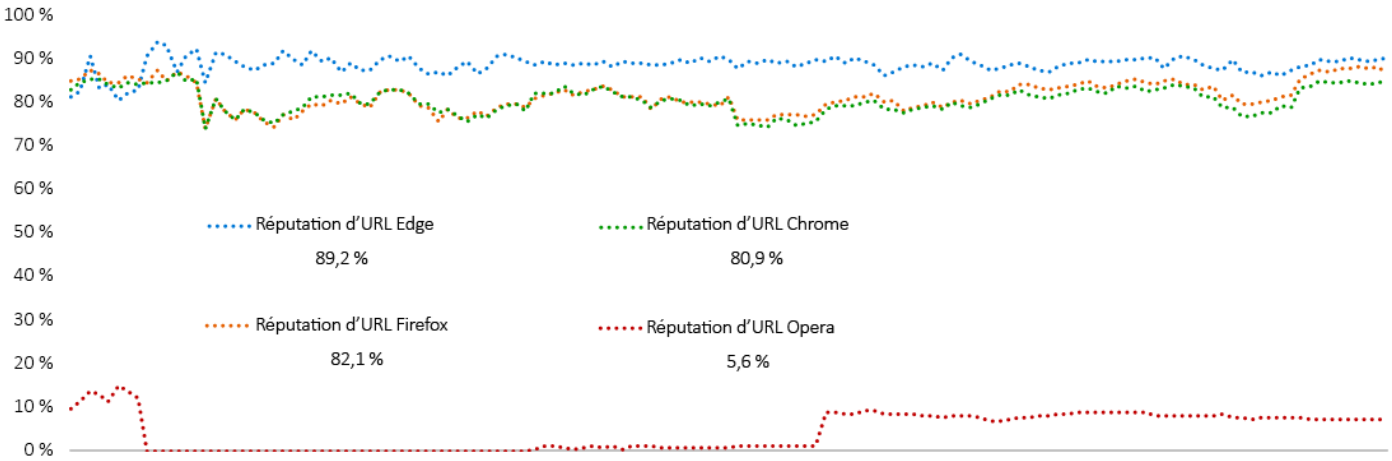
	< 24 heures	< 48 heures	< 72 heures	< 96 heures	< 120 heures	< 144 heures	< 168 heures	Total
Edge avec réputation d'application	96,7 %	98,1 %	98,1 %	98,1 %	98,2 %	98,2 %	98,2 %	98,2 %
Edge avec réputation d'URL	63,4 %	84,5 %	86,5 %	87,3 %	87,8 %	88,1 %	88,1 %	88,1 %
Chrome avec réputation d'application	86,2 %	89,1 %	91,7 %	92,2 %	92,3 %	92,5 %	92,7 %	92,9 %
Chrome avec réputation d'URL	69,7 %	74,4 %	79,0 %	81,0 %	82,0 %	82,2 %	82,4 %	82,7 %
Firefox avec réputation d'application	80,8 %	85,2 %	87,6 %	88,5 %	88,8 %	88,9 %	89,1 %	89,2 %
Firefox avec réputation d'URL	69,1 %	75,3 %	80,0 %	82,1 %	82,9 %	83,0 %	83,4 %	83,6 %
Opera avec réputation d'URL	6,8 %	6,9 %	6,9 %	6,9 %	6,9 %	6,9 %	6,9 %	6,9 %

Au cours du test, Microsoft Edge a démontré un taux de protection initial de 96,7 % contre les logiciels malveillants. Google Chrome et Mozilla Firefox ont atteint un taux de protection initial de 86,2 % et 80,8 % respectivement. Le taux de protection initiale d'Opera était de 6,8 %. À la fin du septième jour de test, tous les navigateurs web ont vu leur taux de protection augmenter. Microsoft Edge l'a augmenté de 4,5 % pour atteindre 98,2 %. Google Chrome l'a augmenté de 6,7 % pour atteindre 92,9 % ; Mozilla Firefox l'a augmenté de 8,4 % pour atteindre 89,2 % ; Opera l'a augmenté de 0,1 % pour atteindre 6,9 %.

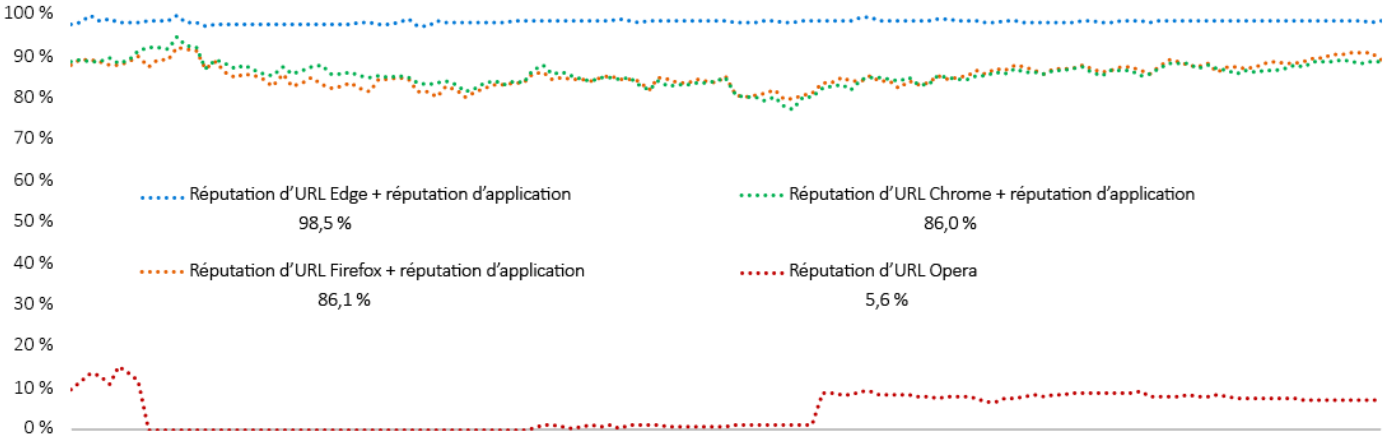
Cohérence de la protection dans le temps

Tout au long du test, de nouveaux logiciels malveillants ont été constamment ajoutés. Les URL, les fichiers et les applications qui n'étaient plus accessibles ou qui hébergeaient des logiciels malveillants ont été supprimés. Chaque point de données est calculé à partir de mesures enregistrées à un moment précis. Si le logiciel malveillant était bloqué dès le début, le score du navigateur pour la cohérence de la protection dans le temps augmentait. Par contre, si le navigateur ne bloquait pas le logiciel malveillant, le score diminuait.

Les tests ont révélé trois niveaux de protection : La réputation de l'URL, la réputation de l'application dans le navigateur et la réputation de l'application du système d'exploitation. La réputation de l'URL offrait une protection raisonnablement bonne.



La protection est renforcée par la réputation de l'application.



La réputation du système d'exploitation offrait une protection supplémentaire. Idéalement, le navigateur web bloquera les logiciels malveillants afin qu'ils n'atteignent jamais le système d'exploitation. Cependant, les tests ont montré que la réputation du système d'exploitation était très efficace.

Environnement de test

- BaitNET™ (propriété de NSS Labs)
- Microsoft Windows 10 Pro 64 bits (version 1909 build : 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (version 4.19.0-kali5-amd64 du noyau)
- 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

Produits testés

- 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

Auteurs

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Méthodologie de test

La méthodologie de test de la sécurité des navigateurs web (WBS) v4.0 de NSS Labs est disponible à l'adresse www.nsslabs.com.

Coordonnées

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com