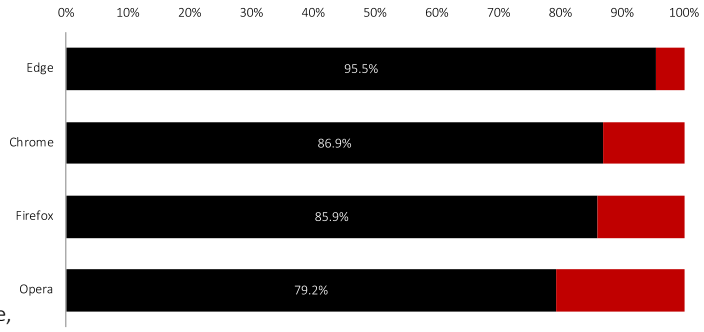
T2 2020 RAPPORT DE TEST COMPARATIF

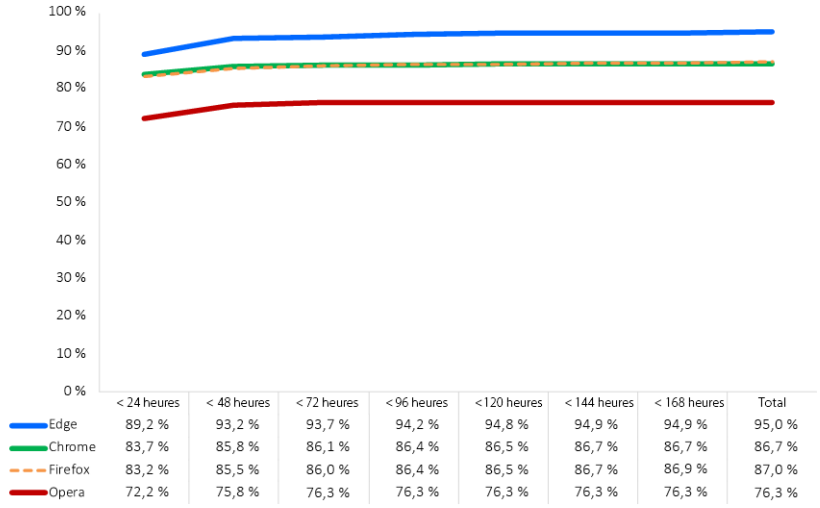
Vue d'ensemble

Au cours du deuxième trimestre 2020, NSS Labs a effectué un test indépendant de la protection contre l'hameçonnage proposée par les navigateurs web : il s'agit de 47 274 tests distincts (par navigateur web) utilisant 2 443 URL d'hameçonnage uniques sur une période de 18 jours. Pour se protéger de l'hameçonnage, Microsoft Edge utilise Microsoft Defender SmartScreen ; Google Chrome et Mozilla Firefox utilisent l'API Google Safe Browsing ; Opera utilise une combinaison de listes rouges de tiers.

Microsoft Edge a offert la meilleure protection, en bloquant 95,5 % des URL d'hameçonnage, tout en offrant le taux de protection zéro heure le plus élevé (89,2 %). Google Chrome a fourni la deuxième protection la plus élevée, bloquant 86,9 % de ces logiciels en moyenne, suivi de Mozilla Firefox, qui en a bloqué 85,9 %. Opera a bloqué 79,2 % des fichiers malveillants.



Résumé des résultats

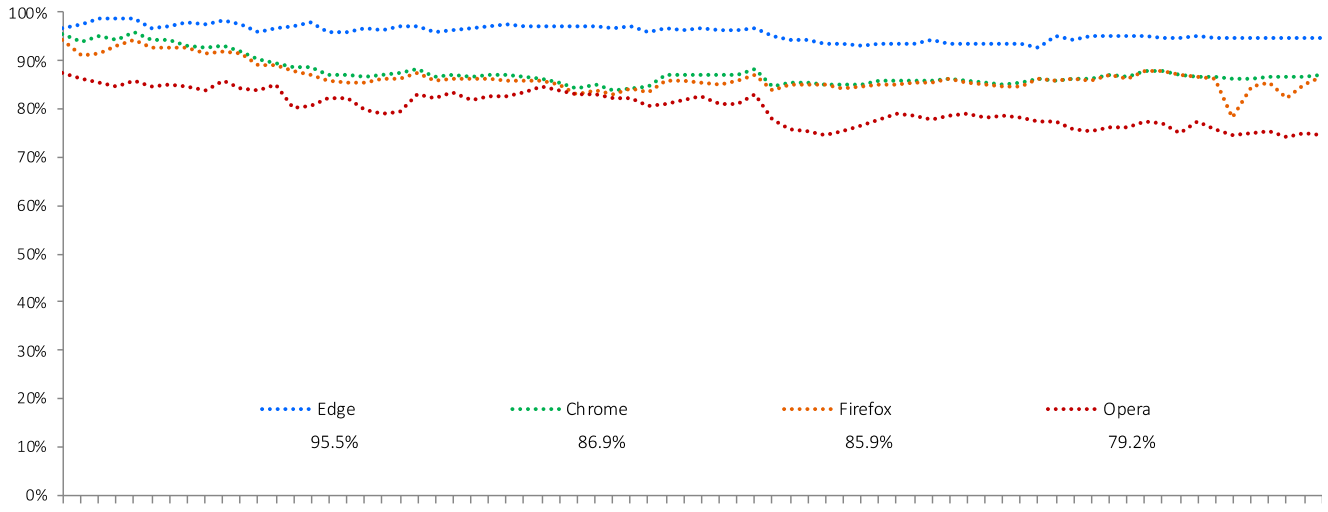


	< 24 heures	< 48 heures	< 72 heures	< 96 heures	< 120 heures	< 144 heures	< 168 heures	Total
Edge	89,2 %	93,2 %	93,7 %	94,2 %	94,8 %	94,9 %	94,9 %	95,0 %
Chrome	83,7 %	85,8 %	86,1 %	86,4 %	86,5 %	86,7 %	86,7 %	86,7 %
Firefox	83,2 %	85,5 %	86,0 %	86,4 %	86,5 %	86,7 %	86,9 %	87,0 %
Opera	72,2 %	75,8 %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

Les systèmes de réputation des URL réduisent le temps dont disposent les attaquants pour atteindre leurs objectifs en avertissant les utilisateurs qu'une URL est un site d'hameçonnage connu ou en les empêchant de l'ouvrir. Toutefois, comme les utilisateurs visitent de nombreux sites web, dont beaucoup sont nouveaux, les systèmes de réputation d'URL ne peuvent pas simplement bloquer toutes les nouvelles URL. Sachant cela, les campagnes d'hameçonnage des attaquants changent constamment, la plupart des nouvelles attaques se produisant dans les premières heures suivant le lancement d'une attaque.

NSS Labs a évalué la capacité des navigateurs à bloquer les URL malveillantes aussi rapidement que nous les avons trouvées sur Internet. Nous avons continué à les tester toutes les six heures afin de déterminer si le fournisseur ajoutait une protection et son temps de réaction.

Protection contre l'hameçonnage au fil du temps



Tout au long du test, de nouvelles URL d'hameçonnage ont été ajoutées tous les jours, et les URL qui n'étaient plus accessibles ou qui ne transmettaient plus d'attaques d'hameçonnage ont été supprimées. Chaque point de données représente une protection à un moment précis. Si l'URL était bloquée 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 l'URL, 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

L'hameçonnage est un type d'attaque d'ingénierie sociale qui tente de persuader une victime de fournir des informations personnelles sensibles au pirate. Les numéros de carte de crédit, les numéros de sécurité sociale, les informations de connexion et les mots de passe des comptes bancaires sont des exemples d'informations sensibles. Les e-mails, les messages instantanés, les SMS et les liens sur les sites de réseaux sociaux sont autant de vecteurs d'attaques d'hameçonnage. Souvent, la page d'accueil d'un site d'hameçonnage tente également d'exploiter silencieusement l'ordinateur d'un visiteur et d'installer un logiciel malveillant (appelé téléchargement furtif).

Les attaques d'hameçonnage présentent un risque important pour les personnes et les organisations en menaçant de compromettre ou d'acquérir des informations personnelles et professionnelles sensibles. Le groupe de travail anti-hameçonnage (Anti-Phishing Working Group, APWG) a fait état d'un total de 165 772 campagnes d'hameçonnage par e-mails uniques au cours du premier trimestre 2020.[1] Les attaques d'hameçonnage sont de plus en plus complexes et sophistiquées, ce qui les rend plus difficiles à détecter et à prévenir.

Protection des navigateurs web contre l'hameçonnage

La protection contre l'hameçonnage est assurée par une application dans le navigateur web qui demande la réputation d'une URL à un serveur de réputation sur le cloud. Le serveur de réputation parcourt Internet pour trouver des sites d'hameçonnage, puis attribue un score à chaque URL et l'ajoute à une liste noire. Ainsi, lorsqu'un navigateur web est invité à visiter une URL, la protection contre l'hameçonnage du navigateur (c'est-à-dire Safe Browsing, SmartScreen, etc.) demande la réputation de l'URL au serveur de réputation sur le cloud et si les résultats indiquent qu'un site web est « mauvais », le navigateur web redirige l'utilisateur vers un message d'avertissement qui explique que l'URL est malveillante. Certains systèmes de réputation comprennent également un contenu éducatif supplémentaire. À l'inverse, si le site web 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.

Composition du test – URL d'hameçonnage

Les données de ce rapport couvrent une période d'essai de 18 jours entre le 21 avril 2020 et le vendredi 8 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 URL d'hameçonnage, ainsi qu'aux services de réputation du navigateur sur le cloud.

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

Nombre total d'URL malveillantes testées

Au total, 4 020 URL brutes non validées ont été testées à plusieurs reprises avec chaque navigateur web, pour un total de 222 527 tests distincts effectués sans interruption pendant 430 heures (toutes les 6 heures pendant 18 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, 2 443 URL d'hameçonnage uniques et valides ont été incluses dans 189 096 tests distincts et valides (47 274 par navigateur web), ce qui donne une marge d'erreur inférieure à 2 % (<2 %) avec un niveau de confiance de 95 %.

Nombre moyen d'URL malveillantes ajoutées par jour

En moyenne, 136 nouvelles URL validées ont été ajoutées à la série de tests chaque jour ; les chiffres ont varié certains jours en fonction des fluctuations des niveaux d'activité criminelle.

Blocage des URL d'hameçonnage

Le NSS a évalué les capacités des navigateurs à bloquer les URL malveillantes aussi rapidement qu'elles étaient découvertes sur Internet. Les ingénieurs ont répété ces tests toutes les six heures afin de déterminer si le fournisseur ajoutait une protection et son temps de réaction.

Le nouveau Microsoft Edge est basé sur Chromium et a été publié le 15 janvier 2020. Il est compatible avec toutes les versions de Windows et de macOS prises en charge. Le téléchargement du navigateur remplacera l'ancienne version de Microsoft Edge sur les PC Windows 10.

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

[1] Rapport de l'APWG sur les tendances des activités d'hameçonnage

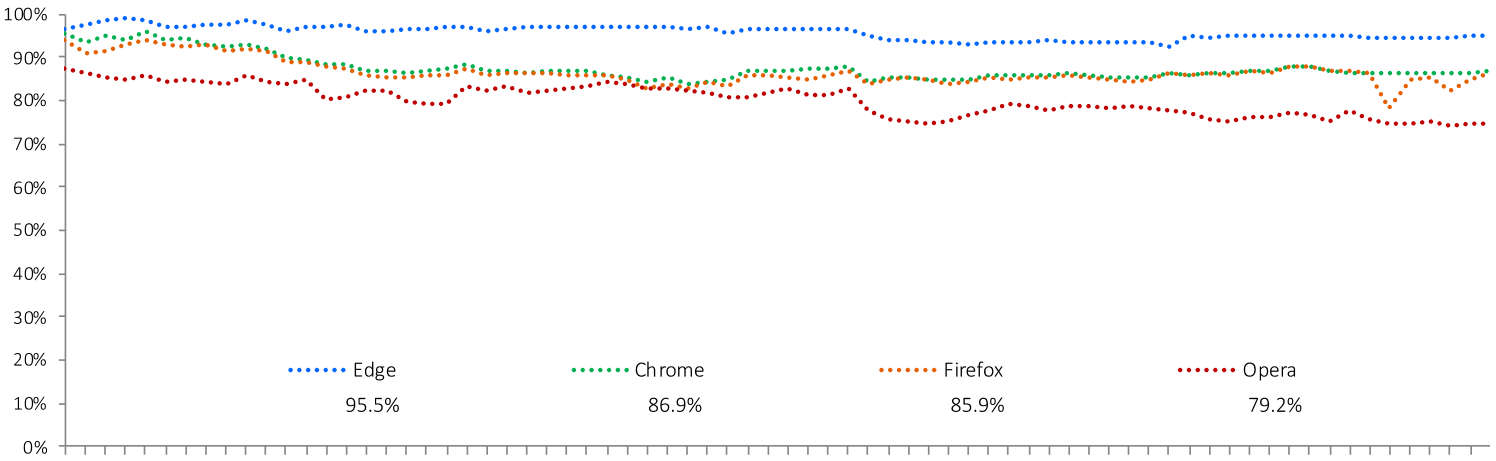
Taux de blocage de tentatives d'hameçonnage

Google Chrome et Mozilla Firefox utilisent l'API de navigation sécurisée de Google. 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,[2] PhishTank[3] et Metamask[4], ainsi qu'une liste noire des logiciels malveillants de Yandex.[5]

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 l'hameçonnage et d'autres activités criminelles. Comme les sites d'hameçonnage 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. Cela explique la corrélation entre la durée moyenne de blocage et le taux de capture. 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 sites d'hameçonnage sont bloqués dans les 24 premières heures suivant leur détection qu'après ce délai.

Les performances de blocage de chaque navigateur ont été mesurées en permanence et le taux de blocage global de toutes les URL testées par navigateur a été enregistré. Le taux de blocage global d'un navigateur est calculé ainsi : le nombre de blocs réussis divisé par le nombre total de cas testés. Par exemple, avec des tests effectués toutes les 6 heures, une URL qui était en ligne pendant 48 heures sera testée 8 fois. Un navigateur qui la bloque à 6 reprises (sur un maximum de 8) atteindra un taux de blocage de 75 %.

Cohérence de la protection dans le temps



Tout au long du test, de nouvelles URL d'hameçonnage ont été ajoutées tous les jours, et les URL qui n'étaient plus accessibles ou qui ne transmettaient plus d'URL d'hameçonnage ont été supprimées. Chaque point de données représente une protection à un moment précis. Si l'URL était bloquée 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 l'URL, le score diminuait.

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

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

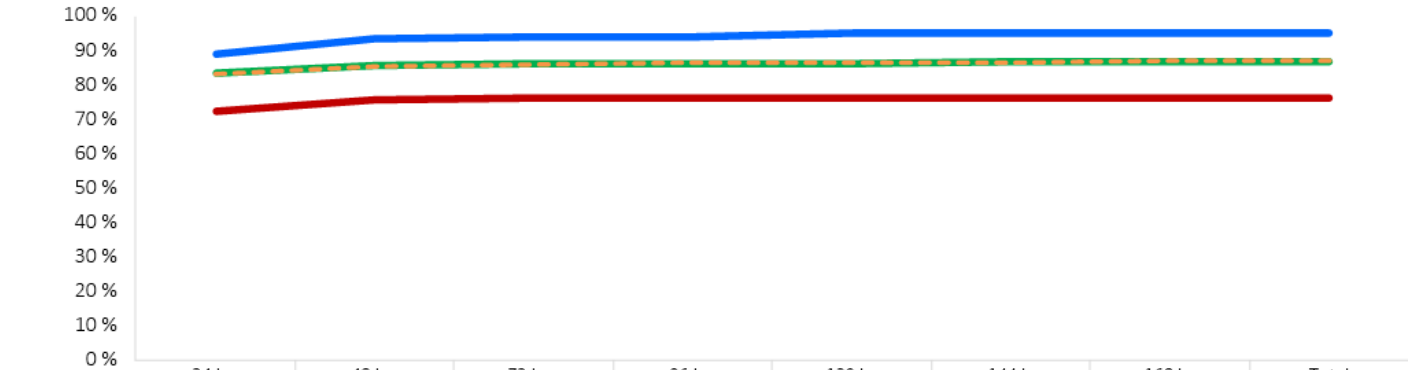
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

Histogramme de protection contre l'hameçonnage

Une protection immédiate contre les nouvelles URL d'hameçonnage est essentielle. Lorsque des sites d'hameçonnage sont découverts, ils sont supprimés, et 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 ci-dessous montre le temps que chaque navigateur a mis pour bloquer un site d'hameçonnage une fois la menace introduite 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.

Au cours du test, Microsoft Edge a démontré un taux de protection initial de 89,2 % contre les attaques d'hameçonnage. Google Chrome et Mozilla Firefox ont atteint un taux de protection initial de 83,7 % et 83,2 % respectivement. Le taux de protection initiale d'Opera était de 72,2 %. 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 5,7 % pour atteindre 94,9 %. Mozilla Firefox l'a augmenté de 3,7 % pour atteindre 86,9 % ; Google Chrome l'a augmenté de 3 % pour atteindre 86,7 %. Opera a augmenté de 4,1 % pour atteindre 76,3 %.



	< 24 heures	< 48 heures	< 72 heures	< 96 heures	< 120 heures	< 144 heures	< 168 heures	Total
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 %

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 – 84.0.502.0
- 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