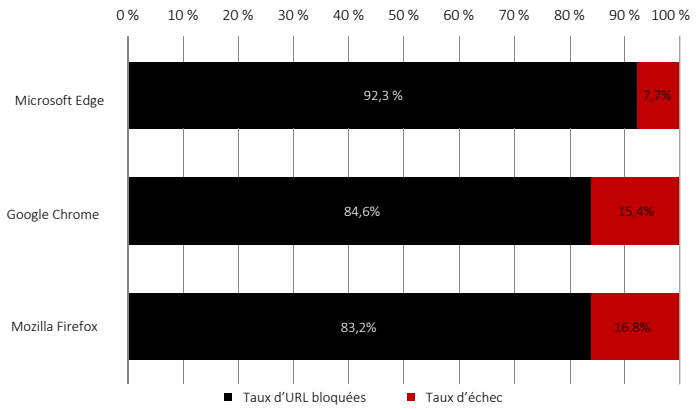
T2 2021 Navigateurs web vs attaques d'hameçonnage

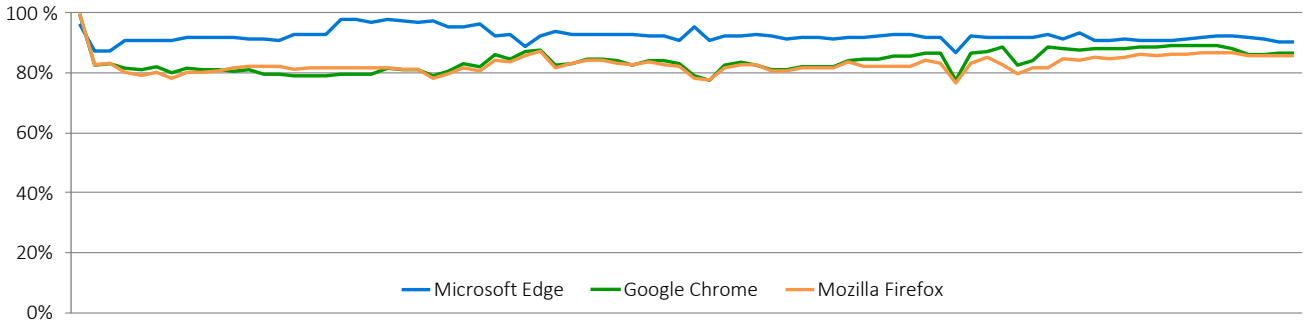
Présenta

Au cours du deuxième trimestre 2021, CyberRatings.org a effectué, de façon indépendante, un test de la protection contre les attaques d'hameçonnage proposée par les navigateurs web. 80 tests discrets ont été effectués sur une période de 20 jours. Pour assurer une protection contre les attaques d'hameçonnage, Microsoft Edge utilise Microsoft Defender SmartScreen, alors que Google Chrome et Mozilla Firefox utilisent l'API Google Safe Browsing.
Microsoft Edge a bloqué 92,3 % des URL d'hameçonnage, soit le taux de protection le plus élevé, et s'est également retrouvé en première position à l'heure H0, avec un taux de 93,5 %. Google Chrome a fourni la deuxième protection la plus élevée, bloquant en moyenne 84,6 % des programmes malveillants, suivi par Mozilla Firefox à 83,2 %.



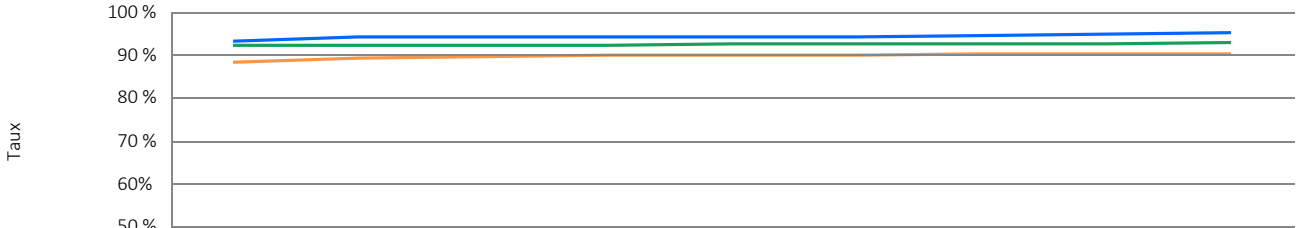
Les systèmes de réputation d'URL réduisent le temps dont disposent les cybercriminels pour atteindre leurs objectifs, en empêchant l'accès à une URL d'hameçonnage connue et en avertissant les utilisateurs de cette menace. Cependant, dans la mesure où les utilisateurs visitent un large éventail de sites web, dont beaucoup sont récents, les systèmes de réputation d'URL ne peuvent pas bloquer toutes les nouvelles URL. Conscients de cela, les cybercriminels renouvellent constamment leurs campagnes d'hameçonnage, la majorité des attaques se produisant durant les premières heures suivant leur lancement.

Protection contre l'hameçonnage sur la durée



Tout au long du test, de nouvelles URL d'hameçonnage ont été ajoutées quotidiennement, et les URL qui n'étaient plus accessibles ou qui n'étaient plus à l'origine d'attaques d'hameçonnage ont été supprimées. Chaque point de données représente le taux de protection à un moment précis. Si une URL est bloquée dès le début, le score de régularité de la protection du navigateur s'améliore au fil du temps. De la même façon, si le navigateur ne bloque pas l'URL, son score diminue.

Taux d'URL bloquées au fil du temps



	H0	J1	J2	J3	J4	J5	J6	J7	Total
Microsoft Edge	93,5 %	94,4%	94,5%	94,5%	94,5%	94,7%	94,9%	95,1%	95,4%
Google Chrome	92,4 %	92,6%	92,7%	92,7%	92,8%	92,8%	92,8%	92,9%	93,2%
Mozilla Firefox	88,7 %	89,7%	90,0%	90,4%	90,4%	90,4%	90,5%	90,6%	90,6%

Résumé des

Nous avons évalué la capacité de chaque navigateur à bloquer les URL malveillantes dès leur repérage sur Internet. Ces tests ont été effectués toutes les six heures afin de déterminer le temps nécessaire à un navigateur pour ajouter une protection. L'illustration ci-dessus indique le temps nécessaire à chaque navigateur pour bloquer un site d'hameçonnage une fois la menace intégrée au cycle de test.

Attaques d'hameçonnage

L'hameçonnage est un type d'attaque par ingénierie sociale qui consiste à inciter la victime à fournir des informations personnelles sensibles au cybercriminel. Des informations sensibles sont, par exemple, les numéros de carte de crédit, les numéros de sécurité sociale et les identifiants et mots de passe liés à des comptes bancaires. Les e-mails, les messages instantanés, les SMS et les liens sur les réseaux sociaux sont autant de moyens utilisés pour réaliser des attaques d'hameçonnage. La page d'arrivée d'un site d'hameçonnage cherche souvent à accéder furtivement à l'ordinateur d'un visiteur et à y installer un programme malveillant (téléchargement furtif).

Permettant de compromettre ou de récupérer des informations sensibles personnelles ou liées à une entreprise, ces attaques d'hameçonnage présentent un risque important pour les individus et les entreprises. Le groupe de travail antihameçonnage (Anti-Phishing Working Group, APWG) a signalé un total de 396 688 campagnes d'hameçonnage par e-mail distinctes au T4 2020[1].

Protection des navigateurs web contre l'hameçonnage

La protection contre l'hameçonnage est assurée par une application au sein d'un navigateur web, qui interroge un service cloud concernant la réputation d'une URL, celui-ci scannant Internet à la recherche de sites d'hameçonnage et les ajoutant ensuite à une liste d'URL bloquées. Ainsi, lorsqu'un navigateur web tente d'accéder à une URL, la protection contre l'hameçonnage du navigateur (soit Safe Browsing, SmartScreen, etc.) redirige l'utilisateur vers un message d'avertissement expliquant que l'URL est malveillante. Certains systèmes de réputation incluent également des contenus pédagogiques. À l'inverse, si un site web est jugé « fiable », le navigateur web n'effectue aucune action.

Google et Mozilla utilisent l'API Google Safe Browsing pour vérifier la réputation des URL, mais également pour alerter les utilisateurs concernant le téléchargement de certains types de fichiers. Microsoft Defender SmartScreen, la technologie de protection intégrée à Microsoft Edge, fournit une protection contre les attaques reposant sur les URL, via un service cloud intégré de réputation d'URL et d'applications destiné au blocage de fichiers malveillants.

Nombre moyen d'URL malveillantes ajoutées chaque jour

En moyenne, 50 nouvelles URL malveillantes validées ont été ajoutées, chaque jour, à la série de tests. Les chiffres variaient en fonction de l'évolution du taux d'activités frauduleuses.

Environnement de test

- Microsoft Windows 10 Professionnel, 21H1

Nombre total d'URL malveillantes testées

Chacune des 26 976 URL brutes non validées a été testée plusieurs fois sur chaque navigateur web durant 80 cycles de test, effectués sans interruption pendant 480 heures (toutes les 6 heures pendant 20 jours). Nos ingénieurs ont retiré les échantillons qui ne répondaient pas aux critères de validation, y compris ceux comprenant un code malveillant exploitant une faille de sécurité (ce qui n'était pas l'objet de ce test). Enfin, 996 URL d'hameçonnage distinctes et validées ont été incluses à l'ensemble de 61 605 tests d'hameçonnage discrets et valides (20 535 tests par navigateur web), avec une marge d'erreur de 3,1 % (3,1 %) et un niveau de confiance de 95 %.

Déroulement du test (URL d'hameçonnage)

Les données de ce rapport couvrent une période de test de vingt (20) jours, du 11 au 31 mai 2021. Pendant le test, nos ingénieurs ont vérifié régulièrement la connectivité afin de s'assurer que les navigateurs testés pouvaient accéder aux URL d'hameçonnage ainsi qu'à leurs services cloud de réputation.

La priorité était le renouvellement constant. En permanence, de nouvelles URL étaient ajoutées, et les URL inactives retirées.

Évaluation des résultats

Nous avons évalué la capacité de chaque navigateur à bloquer les URL malveillantes dès leur repérage sur Internet. Les ingénieurs ont répété ces tests toutes les six heures afin de déterminer le temps nécessaire à un navigateur pour ajouter une protection, le cas échéant.

Les performances de chaque navigateur ont été mesurées en continu et l'on a enregistré le taux global d'URL bloquées pour l'ensemble des URL testées sur le navigateur. Le taux global d'URL bloquées de chaque navigateur a été calculé en divisant le nombre de blocages par le nombre total de tests. Par exemple, pour des tests effectués toutes les 6 heures, une URL en ligne pendant 48 heures est testée huit (8) fois. Un navigateur qui la bloque 6 fois (sur un maximum de 8 tests) atteint un taux de 75 %.

Produits testés

- 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

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

Auteurs :

Thomas Skybakmoen, Vikram Phatak

Méthodologie utilisée

La méthodologie CyberRatings relative aux tests de sécurité sur les navigateurs web (v1.0) est disponible sur www.cyberratings.org.

Coordonnées

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

info@cyberratings.org
www.cyberratings.org