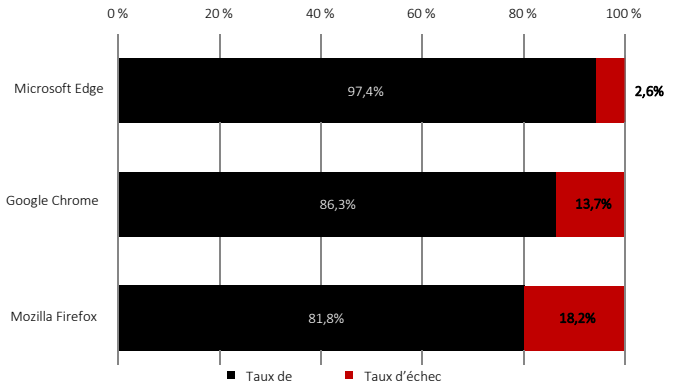
T2 2021 Navigateurs web vs programmes malveillants

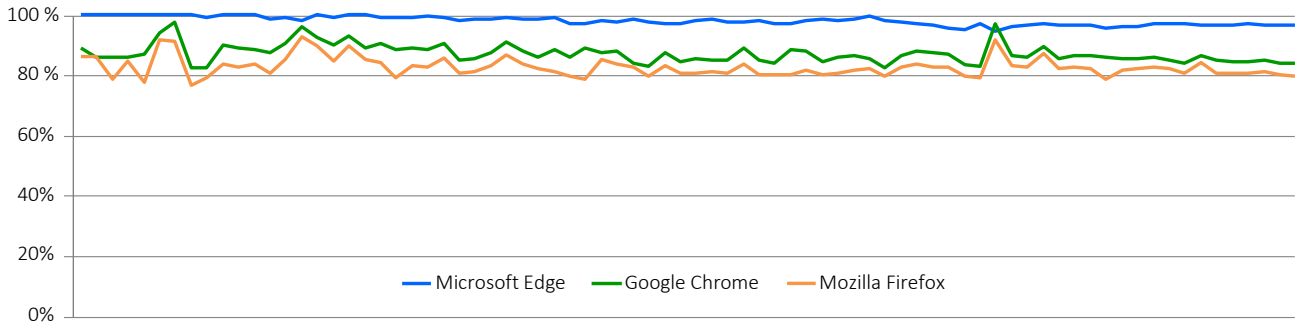
Présenta

Au cours du deuxième trimestre 2021, CyberRatings.org a effectué, de façon indépendante, un test de la protection contre les programmes malveillants proposée par les navigateurs web. 80 tests discrets ont été effectués sur une période de 20 jours. Pour assurer une protection contre les programmes malveillants, Microsoft Edge utilise Microsoft Defender SmartScreen, alors que Google Chrome et Mozilla Firefox utilisent l'API Google Safe Browsing. Microsoft Edge a bloqué 97,4 % des programmes malveillants, soit le taux de protection le plus élevé, et s'est également retrouvé en première position à l'heure H0, avec un taux de 97,7 %. Google Chrome a fourni la deuxième protection la plus élevée, bloquant en moyenne 86,3 % des programmes malveillants, suivi par Mozilla Firefox à 81,8 %.



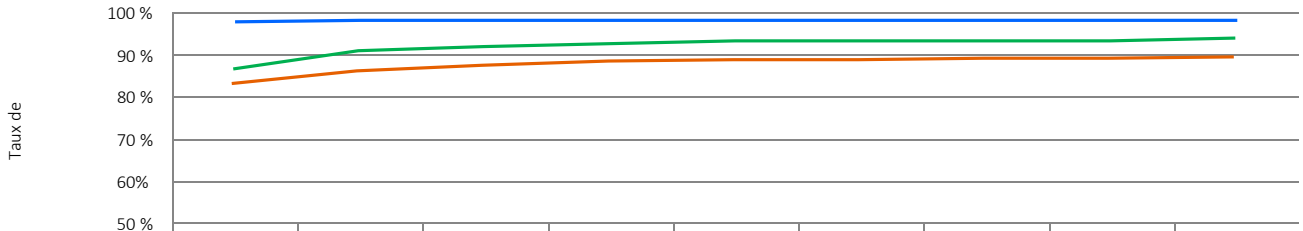
La capacité à avertir les potentielles victimes qu'elles sont sur le point d'accéder à un site web malveillant confère aux navigateurs web une position centrale dans la lutte contre les programmes malveillants. Les sites web incitant les utilisateurs (par ingénierie sociale) à télécharger des programmes malveillants ont une durée de vie réduite. Il est donc essentiel que le site soit identifié et ajouté au système de réputation, et ce, le plus rapidement possible. Un tel système doit être à la fois précis et rapide pour atteindre des taux de réussite élevés.

Protection contre les programmes malveillants sur la durée



Tout au long du test, de nouveaux programmes malveillants ont été continuellement ajoutés. Les URL qui n'étaient plus accessibles ou n'hébergeaient plus de programmes malveillants ont été supprimées. Chaque point de données est calculé à partir de mesures enregistrées à un moment précis. Si le programme malveillant est bloqué dès le début, le score de protection du navigateur s'améliore au fil du temps. De la même façon, si le navigateur ne bloque pas le programme malveillant, son score diminue.

Taux de programmes malveillants bloqués au fil du temps



	H0	J1	J2	J3	J4	J5	J6	J7	Total
Microsoft Edge	97,7 %	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%
Google Chrome	86,4 %	90,6%	91,7%	92,5%	92,9%	93,1%	93,1%	93,1%	93,6%
Mozilla Firefox	82,8 %	85,9%	87,1%	88,0%	88,3%	88,4%	88,6%	88,7%	89,1%

Résumé des

L'illustration ci-dessus indique le temps nécessaire à chaque navigateur pour bloquer le programme malveillant une fois l'échantillon intégré au cycle de test. 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 programmes malveillants. Google Chrome et Mozilla Firefox 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, ou encore bloquer ces derniers.

Attaques de programmes malveillants

Les attaques via des programmes malveillants d'ingénierie sociale utilisent des procédés visant à duper les utilisateurs afin de les inciter à télécharger des programmes malveillants. Le piratage de comptes de messagerie et de réseaux sociaux permet de tirer parti de la confiance implicite entre les contacts et de faire croire aux victimes que les liens vers des fichiers malveillants sont fiables. D'autres techniques consistent à afficher des messages contextuels informant les utilisateurs que des applications (comme Adobe Flash Player) doivent être installées, ou encore indiquant que l'ordinateur est infecté ou nécessite une mise à jour.

Une fois le programme malveillant installé, les victimes sont vulnérables face au vol d'identifiants, à l'usurpation d'identité, à l'utilisation frauduleuse de leur compte bancaire, etc.

Protection des navigateurs web contre les programmes malveillants

Afin d'assurer une protection contre les programmes malveillants, les systèmes cloud de réputation scannent Internet à la recherche de sites web malveillants, puis trient le contenu en conséquence. Les navigateurs web interrogent ensuite les systèmes cloud de réputation concernant des URL, des fichiers ou des applications spécifiques. Si les résultats indiquent la présence d'un programme malveillant, le navigateur web affiche un message d'avertissement expliquant qu'une URL, un fichier ou une application est de nature malveillante. Certains systèmes de réputation incluent également des contenus pédagogiques.

Google Chrome et Mozilla Firefox utilisent l'API Google Safe Browsing pour vérifier la réputation des URL et des applications afin de bloquer les fichiers malveillants. Microsoft Edge utilise Microsoft Defender SmartScreen, qui fournit une protection contre les attaques via un service cloud de réputation d'URL et d'applications visant à bloquer les fichiers malveillants.

Nombre moyen d'échantillons de programmes malveillants ajoutés chaque jour

En moyenne, 49 nouveaux échantillons de programmes malveillants validés ont été ajoutés, chaque jour, à la série de tests. Les chiffres variaient en fonction de l'évolution du nombre d'activités frauduleuses.

Nombre total d'échantillons malveillants testés

Chacun des 18 621 échantillons bruts non validés a été testé plusieurs fois sur chaque navigateur web durant 78 cycles de test, effectués sans interruption pendant 468 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, 950 échantillons de programmes malveillants distincts et validés ont été inclus à l'ensemble de 48 672 tests discrets et valides de programmes malveillants (16 224 tests par navigateur web), avec une marge d'erreur de moins de 3,2 % (< 3,2 %) et un niveau de confiance de 95 %.

Déroulement des tests et échantillons de programmes malveillants

Les données de ce rapport couvrent une période de test de vingt (20) jours, du 11 au 31 mai 2021. Pendant le test, les ingénieurs de CyberRatings vérifiaient régulièrement la connectivité afin de s'assurer que les navigateurs testés pouvaient accéder aux programmes malveillants ainsi qu'aux services cloud de réputation.

La priorité était le renouvellement constant. En permanence, de nouveaux échantillons étaient ajoutés, et les échantillons inactifs retirés.

Évaluation des résultats

Nous avons évalué la capacité de chaque navigateur à bloquer les programmes malveillants 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 de programmes bloqués pour l'ensemble des échantillons de programmes malveillants testés sur le navigateur. Le taux global de programmes bloqués 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, un échantillon de programme malveillant en ligne pendant 48 heures est testé huit (8) fois. Un navigateur qui le bloque 6 fois (sur un maximum de 8 tests) atteint un taux de 75 %.

Environnement de test

- Microsoft Windows 10 Professionnel, 21H1

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

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