

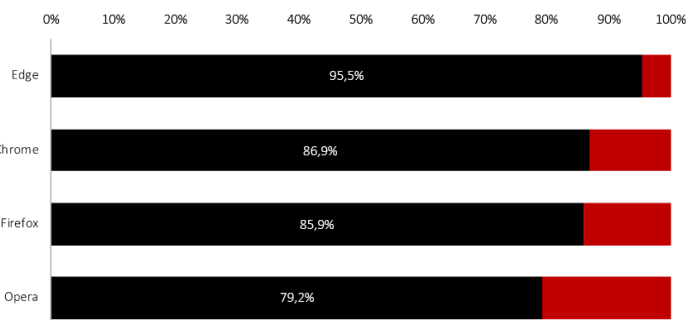
2ο τρίμηνο 2020

ΣΥΓΚΡΙΤΙΚΗ ΑΝΑΦΟΡΑ ΔΟΚΙΜΩΝ

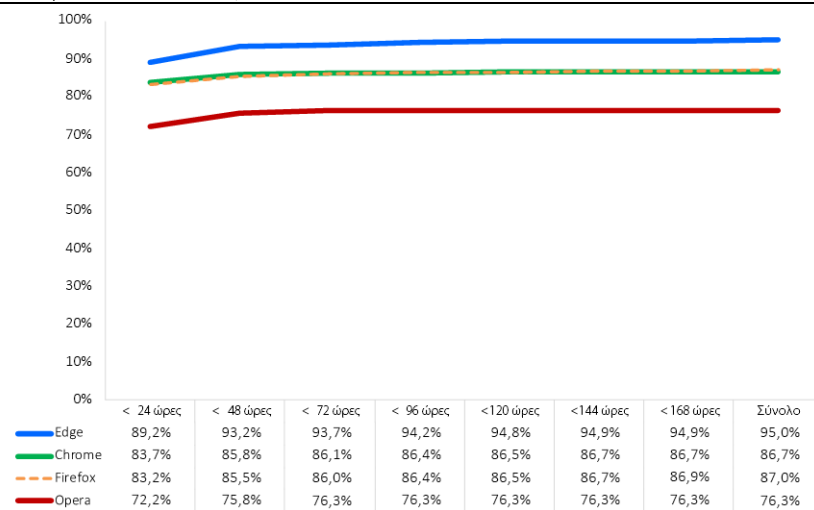
Επισκόπηση

Κατά τη διάρκεια του 2ου τριμήνου του 2020, η NSS Labs διεξήγαγε μια ανεξάρτητη δοκιμή αναφορικά με την προστασία από το ηλεκτρονικό "ψάρεμα" που προσφέρεται από τα προγράμματα περιήγησης Web: 47.274 μεμονωμένες δοκιμές (ανά πρόγραμμα περιήγησης) χρησιμοποιώντας 2.443 μοναδικά URL ηλεκτρονικού "ψαρέματος" για 18 ημέρες. Για την προστασία έναντι του ηλεκτρονικού "ψαρέματος" ο Microsoft Edge χρησιμοποιεί το Microsoft Defender SmartScreen. Το Google Chrome και το Mozilla Firefox χρησιμοποιούν το Google Safe Browsing API. Το Opera χρησιμοποιεί έναν συνδυασμό τρίτων προγραμμάτων αποκλεισμού.

Ο Microsoft Edge προσέφερε τη μεγαλύτερη προστασία, αποκλείοντας το 95,5% των URL ηλεκτρονικού "ψαρέματος", παρέχοντας παράλληλα το υψηλότερο ποσοστό αυτόματου αποκλεισμού (89,2%). Το Google Chrome παρείχε τη δεύτερη μεγαλύτερη προστασία, αποκλείοντας κατά μέσο όρο το 86,9%, ενώ ακολούθησε το Mozilla Firefox με 85,9%. Το Opera απέκλεισε το 79,2%.



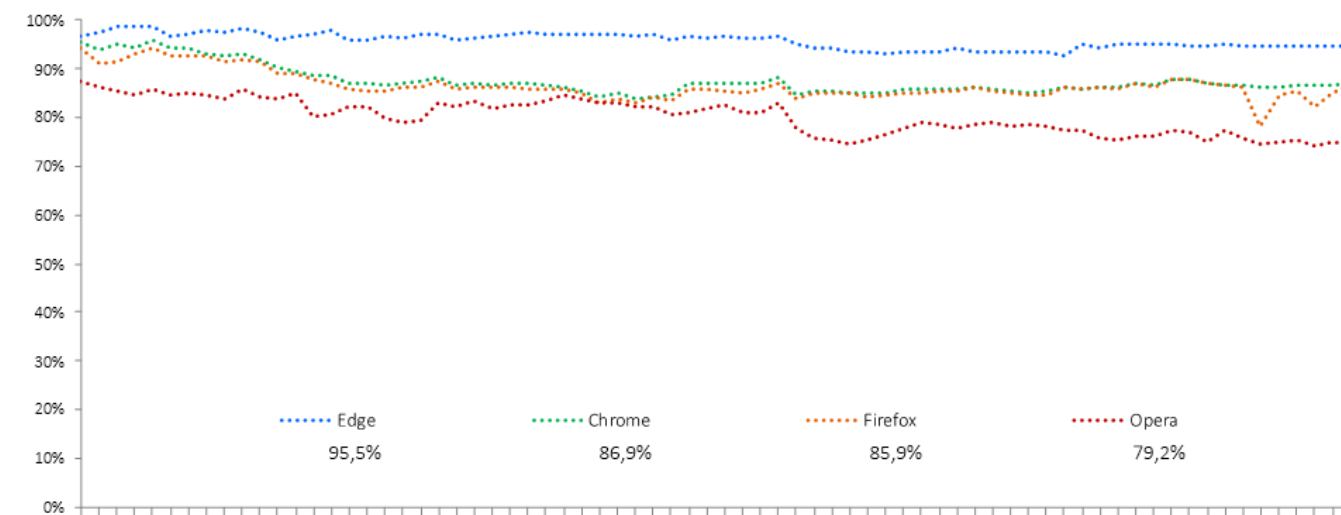
Σύνοψη των αποτελεσμάτων



Τα συστήματα διαχείρισης φήμης διευθύνσεων URL μειώνουν τον χρόνο που διαθέτουν οι εισβολείς για να επιτύχουν τους στόχους τους αποτρέποντας/προειδοποιώντας τους χρήστες ότι μια διεύθυνση URL είναι μια γνωστή ιστοσελίδα ηλεκτρονικού "ψαρέματος". Ωστόσο, δεδομένου ότι οι χρήστες επισκέπτονται ένα ευρύ φάσμα τοποθεσιών Web, πολλές από τις οποίες είναι καινούριες, τα συστήματα διαχείρισης φήμης των διευθύνσεων URL δεν μπορούν απλώς να αποκλείσουν όλες τις νέες διευθύνσεις URL. Γνωρίζοντας αυτό, οι εκστρατείες ηλεκτρονικού "ψαρέματος" των εισβολέων αλλάζουν διαρκώς, με το μεγαλύτερο μέρος των νέων επιθέσεων να λαμβάνουν χώρα τις πρώτες ώρες μετά την έναρξη μιας εκστρατείας.

Η NSS Labs αξιολόγησε την ικανότητα των προγραμμάτων περιήγησης να αποκλείουν κακόβουλα URL με την ίδια ταχύτητα που τα εντοπίζουμε στο Internet. Συνεχίσαμε τις δοκιμές ανά έξι ώρες για να προσδιορίσουμε τον χρόν που χρειάστηκε ένας προμηθευτής για να προσθέσει την προστασία, εάν εντέλει την πρόσθεσε.

Προστασία κατά του ηλεκτρονικού "ψαρέματος" με την πάροδο του χρόνου



Καθ' όλη τη διάρκεια της δοκιμής, νέες διευθύνσεις URL ηλεκτρονικού "ψαρέματος" προσθέτονταν καθημερινά και αφαιρούνταν διευθύνσεις URL που είτε δεν ήταν πλέον προσβάσιμες είτε δεν επέφεραν πλέον επιθέσεις ηλεκτρονικού "ψαρέματος". Κάθε σημείο δεδομένων αναπαριστά την προστασία σε μια συγκεκριμένη χρονική στιγμή. Σε περίπτωση που μια διεύθυνση URL αποκλειστεί σε πρώιμο στάδιο, η βαθμολογία του προγράμματος περιήγησης αναφορικά με τη συνοχή της προστασίας με την πάροδο του χρόνου θα αυξηθεί. Ειδικά, εάν το πρόγραμμα περιήγησης δεν αποκλείσει τη διεύθυνση URL, η βαθμολογία θα μειωθεί.

Η δοκιμή βασίστηκε στη μεθοδολογία Web Browser Test Methodology v4.0 (διαθέσιμη στη διεύθυνση www.nsslabs.com).

Η παρούσα αναφορά είναι εμπιστευτική και περιορίζεται ρητά σε εξουσιοδοτημένους πελάτες της NSS Labs.

Γενικές πληροφορίες

Το ηλεκτρονικό "ψάρεμα" είναι ένας τύπος επίθεσης κοινωνικής μηχανικής που επιχειρεί να πείσει το θύμα να παράσχει ευαίσθητες προσωπικές πληροφορίες στον εισβολέα. Τέτοια παραδείγματα ευαίσθητων πληροφοριών είναι αριθμοί πιστωτικών καρτών, αριθμοί κοινωνικής ασφάλισης, στοιχεία σύνδεσης και κωδικοί πρόσβασης τραπεζικών λογαριασμών. Το ηλεκτρονικό ταχυδρομείο, τα άμεσα μηνύματα, τα μηνύματα SMS και οι σύνδεσμοι σε τοποθεσίες κοινωνικής δικτύωσης είναι όλοι φορείς επιθέσεων ηλεκτρονικού "ψαρέματος". Συχνά, η σελίδα προορισμού μιας τοποθεσίας Web ηλεκτρονικού "ψαρέματος" επιχειρεί επίσης να εκμεταλλευτεί σιωπηλά τον υπολογιστή ενός επισκέπτη και να εγκαταστήσει ένα κακόβουλο λογισμικό (κοινώς drive-by exploit).

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" ενέχουν σημαντικό κίνδυνο τόσο για τα άτομα όσο και για τους οργανισμούς, καθώς απειλούν να διαρρεύσουν ή να αποκτήσουν ευαίσθητες προσωπικές και εταιρικές πληροφορίες. Η Ομάδα εργασίας για την καταπολέμηση του ηλεκτρονικού "ψαρέματος" (APWG) κατέγραψε συνολικά 165.772 μεμονωμένες εκστρατείες email ηλεκτρονικού "ψαρέματος" το πρώτο τρίμηνο του 2020.¹ Οι επιθέσεις ηλεκτρονικού "ψαρέματος" γίνονται ολοένα πιο σύνθετες και περίπλοκες, καθιστώντας δυσκολότερη την ανίχνευση καθώς και την πρόληψη τους.

Προστασία προγραμμάτων περιήγησης Web από το ηλεκτρονικό "ψάρεμα"

Η προστασία ηλεκτρονικού "ψαρέματος" παρέχεται από μια εφαρμογή εντός του προγράμματος περιήγησης Web που ζητά τη φήμη μιας διεύθυνσης URL από έναν διακομιστή φήμης στο cloud. Ο διακομιστής φήμης σαρώνει το Διαδίκτυο για να εντοπίσει τοποθεσίες Web ηλεκτρονικού "ψαρέματος" και κατόπιν προσδίδει σε κάθε διεύθυνση URL μια βαθμολογία και την προσθέτει στη λίστα αποκλεισμού. Με αυτόν τον τρόπο, όταν ένα πρόγραμμα περιήγησης Web έχει την οδηγία να επισκεφτεί μια διεύθυνση URL, η προστασία ηλεκτρονικού "ψαρέματος" του προγράμματος περιήγησης (π.χ. Safe Browsing, SmartScreen κ.λπ.) ζητά τη φήμη της διεύθυνσης URL από το διακομιστή φήμης στο cloud και, εφόσον τα αποτελέσματα δείξουν ότι μια τοποθεσία Web είναι "κακή", το πρόγραμμα περιήγησης Web θα ανακατευθύνει τον χρήστη σε ένα προειδοποιητικό μήνυμα που θα εξηγήσει ότι η διεύθυνση URL είναι κακόβουλη. Ορισμένοι μηχανισμοί φήμης περιλαμβάνουν επιπλέον ένα πρόσθετο εκπαιδευτικό περιεχόμενο. Αντίθετα, εάν μια τοποθεσία Web κριθεί "καλή", το πρόγραμμα περιήγησης Web δεν αναλαμβάνει δράση και ο χρήστης δεν ενημερώνεται ότι μόλις πραγματοποιήθηκε έλεγχος ασφαλείας από το πρόγραμμα περιήγησης.

Σύνθεση δοκιμής - Διευθύνσεις URL ηλεκτρονικού "ψαρέματος"

Τα δεδομένα της παρούσας αναφοράς καλύπτουν μια περίοδο δοκιμής 18 ημερών μεταξύ της 21ης Απριλίου 2020 και της 8ης Μαΐου 2020. Όλες οι δοκιμές διεξήχθησαν στις εγκαταστάσεις δοκιμών της NSS στο Όστιν του Τέξας. Κατά τη διάρκεια της δοκιμής, οι μηχανικοί του NSS παρακολουθούσαν τακτικά τη συνδεσιμότητα για να διασφαλίσουν ότι τα υπό δοκιμή προγράμματα περιήγησης έχουν πρόσβαση στις διευθύνσεις URL ηλεκτρονικού "ψαρέματος" καθώς και στις υπηρεσίες φήμης για προγράμματα περιήγησης στο cloud.

Δόθηκε έμφαση στην ενεργητικότητα, επομένως αξιολογήθηκε μεγαλύτερος αριθμός τοποθεσιών Web από ό,τι εντέλει προσμετρήθηκε ως μέρος των συνολικών αποτελεσμάτων των δοκιμών, καθώς νέες διευθύνσεις URL προσθέτονταν συνεχώς στη δοκιμή και "νεκροί" ιστότοποι αφαιρούνταν.

Συνολικός αριθμός κακόβουλων διευθύνσεων URL στη δοκιμή

Συνολικά 4.020 ακατέργαστες, μη επικυρωμένες διευθύνσεις URL ελέγχθηκαν πολλάκις με κάθε πρόγραμμα περιήγησης Web σε συνολικά 222.527 μεμονωμένες δοκιμές που διεξήχθησαν χωρίς διακοπή για 430 ώρες (ανά 6 ώρες για 18 ημέρες). Οι μηχανικοί της NSS αφαίρεσαν δείγματα που δεν πληρούσαν τις προϋποθέσεις επικύρωσης, συμπεριλαμβανομένων εκείνων που αλλοιώθηκαν από εκμεταλλεύσεις (δεν αποτελούν μέρος της δοκιμής). Εντέλει, 2.443 μοναδικά, έγκυρα URL ηλεκτρονικού "ψαρέματος" συμπεριλήφθηκαν στις 189.096 μεμονωμένες, έγκυρες δοκιμές ηλεκτρονικού "ψαρέματος" (47.274 ανά πρόγραμμα περιήγησης), παρέχοντας ένα περιθώριο σφάλματος μικρότερο από 2 τοις εκατό (<2%) με επίπεδο εμπιστοσύνης 95%.

Μέσος αριθμός κακόβουλων διευθύνσεων URL που προσθέτονταν ανά ημέρα

Κατά μέσο όρο, 136 νέες επικυρωμένες διευθύνσεις URL προσθέτονταν στο σύνολο δοκιμών ανά ημέρα. Οι αριθμοί ποικίλουν σε ορισμένες ημέρες καθώς τα επίπεδα εγκληματικής δραστηριότητας παρουσίαζαν διακυμάνσεις.

Αποκλεισμός διευθύνσεων URL ηλεκτρονικού "ψαρέματος"

Η NSS Labs αξιολόγησε τις ικανότητες των προγραμμάτων περιήγησης να αποκλείουν κακόβουλα URL με την ίδια ταχύτητα που τα εντοπίζουμε στο Internet. Οι μηχανικοί επαναλάμβαναν τις δοκιμές ανά έξι ώρες για να προσδιορίσουν τον χρόνο που χρειάστηκε ένας προμηθευτής για να προσθέσει την προστασία, εάν εντέλει την πρόσθεσε.

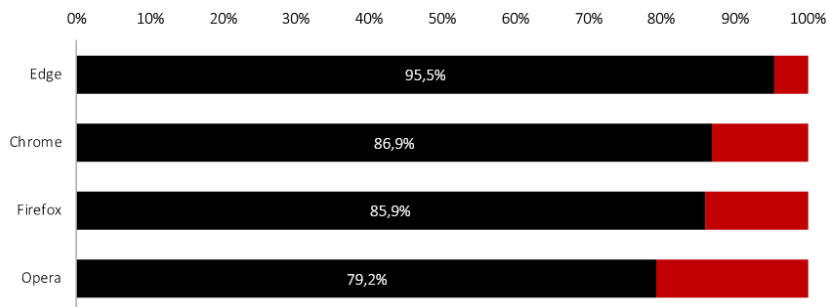
Ο νέος Microsoft Edge βασίζεται στο Chromium και κυκλοφόρησε στις 15 Ιανουαρίου 2020. Είναι συμβατός με όλες τις υποστηριζόμενες εκδόσεις των Windows και macOS. Η λήψη του προγράμματος περιήγησης θα αντικαταστήσει την παλιά έκδοση του Microsoft Edge σε υπολογιστές με Windows 10.

<https://support.microsoft.com/el-gr/help/4501095/download-the-new-microsoft-edge-based-on-chromium>

¹ Αναφορά τάσεων δραστηριότητας ηλεκτρονικού "ψαρέματος" της APWG

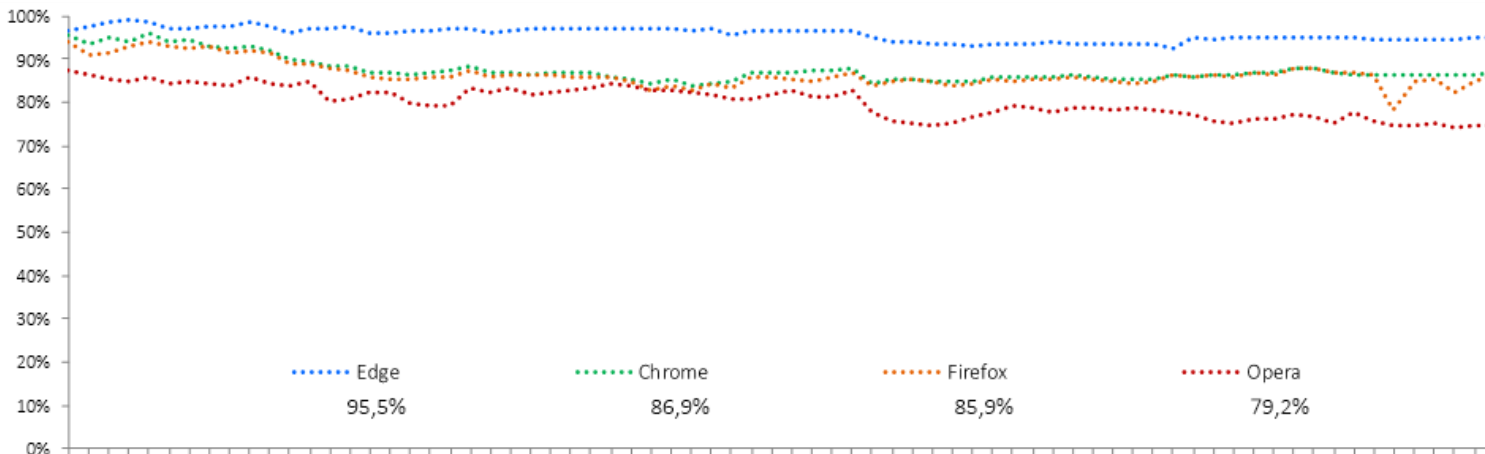
Ποσοστό αποκλεισμού ηλεκτρονικού "ψαρέματος"

Το Google Chrome και το Mozilla Firefox χρησιμοποιούν το Safe Browsing API της Google. Ο Microsoft Edge χρησιμοποιεί το Microsoft Defender SmartScreen, συμπεριλαμβανομένης της υπηρεσίας διαχείρισης φήμης εφαρμογών για την παροχή προστασίας από απειλές ηλεκτρονικού "ψαρέματος" και κακόβουλων λογισμικών. Το Opera χρησιμοποιεί έναν συνδυασμό προγραμμάτων αποκλεισμού από τις εταιρείες Netcraft,² PhishTank³ και Metamask⁴, καθώς και λίστα αποκλεισμού κακόβουλου λογισμικού από τη Yandex.⁵ Η δυνατότητα προειδοποίησης των πιθανών θυμάτων ότι πρόκειται να μεταφερθούν σε μια κακόβουλη τοποθεσία Web τοποθετεί τα προγράμματα περιήγησης Web σε καίρια θέση για την καταπολέμηση του ηλεκτρονικού "ψαρέματος" και άλλων εγκληματικών δραστηριοτήτων. Δεδομένου ότι οι τοποθεσίες Web ηλεκτρονικού "ψαρέματος" έχουν μικρή διάρκεια ζωής, είναι ουσιώδες η τοποθεσία Web να εντοπιστεί, να επικυρωθεί, να ταξινομηθεί και να προστεθεί στο σύστημα διαχείρισης φήμης το συντομότερο δυνατό. Το γεγονός αυτό εξηγεί τη συσχέτιση μεταξύ του μέσου χρόνου αποκλεισμού και του ποσοστού ανίχνευσης. Ένα καλό σύστημα διαχείρισης φήμης πρέπει να είναι όχι μόνο ακριβές αλλά και γρήγορο, ώστε να επιτευχθούν υψηλά ποσοστά ανίχνευσης. Οι προγραμματιστές προγραμμάτων περιήγησης κατανοούν πλήρως αυτή τη σχέση και ουσιαστικά οι περισσότερες τοποθεσίες ηλεκτρονικού "ψαρέματος" αποκλείονται τις πρώτες 24 ώρες της ανίχνευσής τους, παρά μετέπειτα.



Η επιμέρους απόδοση αποκλεισμού κάθε προγράμματος περιήγησης μετρήθηκε συνεχόμενα και το συνολικό ποσοστό αποκλεισμού όλων των διευθύνσεων URL που ελέγχθηκαν από το πρόγραμμα περιήγησης καταγράφηκε. Το συνολικό ποσοστό αποκλεισμού ενός προγράμματος περιήγησης υπολογίζεται από τον αριθμό των επιτυχημένων αποκλεισμών διαιρεμένο με τον συνολικό αριθμό των δοκιμών. Για παράδειγμα, σε δοκιμές που διεξάγονται ανά 6 ώρες, μια διεύθυνση URL που ήταν online για 48 ώρες θα ελεγχθεί 8 φορές. Ένα πρόγραμμα περιήγησης που αποκλείει 6 δοκιμές (μέγιστος αριθμός δοκιμών 8) θα επιτύχει ποσοστό αποκλεισμού 75%.

Συνοχή προστασίας με την πάροδο του χρόνου



Καθ' όλη τη διάρκεια της δοκιμής, νέες διευθύνσεις URL ηλεκτρονικού "ψαρέματος" προσθέτονταν καθημερινά, ενώ αφαιρούνταν διευθύνσεις URL που είτε δεν ήταν πλέον προσβάσιμες είτε δεν επέφεραν πλέον διευθύνσεις URL ηλεκτρονικού "ψαρέματος". Κάθε σημείο δεδομένων αναπαριστά την προστασία σε μια συγκεκριμένη χρονική στιγμή. Σε περίπτωση που μια διεύθυνση URL αποκλειστεί σε πρώιμο στάδιο, η βαθμολογία του προγράμματος περιήγησης αναφορικά με τη συνοχή της προστασίας με την πάροδο του χρόνου θα αυξηθεί. Ειδικά, εάν το πρόγραμμα περιήγησης δεν αποκλείσει τη διεύθυνση URL, η βαθμολογία θα μειωθεί.

² <http://www.netcraft.com/>

³ <http://www.phishtank.com/>

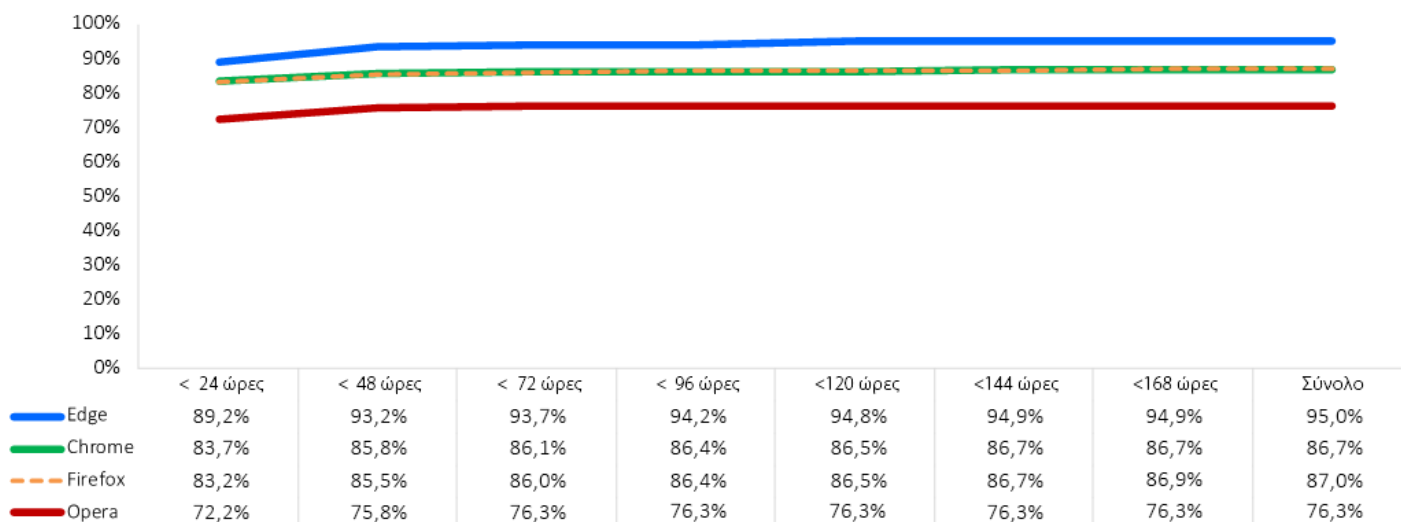
⁴ <https://github.com/metamask/eth-phishing-detect>

⁵ <https://yandex.com>

Ιστογράμμα προστασίας ηλεκτρονικού "ψαρέματος"

Η άμεση προστασία έναντι νέων διευθύνσεων URL ηλεκτρονικού "ψαρέματος" είναι καθοριστικής σημασίας. Όταν ανιχνεύονται τοποθεσίες Web ηλεκτρονικού "ψαρέματος", αυτές καταργούνται και συνήθως αυτό λαμβάνει χώρα εντός σχετικά μικρού χρονικού διαστήματος. Τα προϊόντα που αποτυγχάνουν να προσθέσουν έγκαιρη προστασία ενδέχεται να καθυστερήσουν στην αντιμετώπιση μιας απειλής. Το παρακάτω ιστογράμμα απεικονίζει τον χρόνο που χρειάστηκε κάθε πρόγραμμα περιήγησης για να αποκλείσει μια τοποθεσία Web ηλεκτρονικού "ψαρέματος" μετά την εισβολή της απειλής στον κύκλο δοκιμών. Εντός διαστήματος επτά ημερών, τα αθροιστικά ποσοστά προστασίας υπολογίζονται ανά μέρα έως ότου αποκλειστούν οι απειλές.

Κατά τη διάρκεια της δοκιμής, ο Microsoft Edge επέδειξε αρχικό ποσοστό προστασίας της τάξης του 89,2% έναντι επιθέσεων ηλεκτρονικού "ψαρέματος". Το Google Chrome και το Mozilla Firefox πέτυχαν αρχικό ποσοστό προστασίας 83,7% και 83,2% αντίστοιχα. Το αρχικό ποσοστό προστασίας του Opera ανήλθε στο 72,2%. Κατά το τέλος της εβδομής ημέρας των δοκιμών, όλα τα προγράμματα περιήγησης Web παρουσίασαν αύξηση της προστασίας. Η προστασία του Microsoft Edge αυξήθηκε κατά 5,7% σε ποσοστό 94,9%. Η προστασία του Mozilla Firefox αυξήθηκε κατά 3,7% σε ποσοστό 86,9%, ενώ του Google Chrome αυξήθηκε κατά 3% σε ποσοστό 86,7%. Η προστασία του Opera αυξήθηκε κατά 4,1% σε 76,3%.



Περιβάλλον δοκιμής

- BaitNET™ (Ιδιοκτησία της NSS Labs)
- 64 bit Microsoft Windows 10 Pro (έκδοση 1909 Δόμηση: 18363,592)
- Ubuntu 18.04.3 LTS
- Kali (έκδοση Kernel 4.19.0-kali5-amd64)
- VMware vCenter (έκδοση 6.7u2 Δόμηση 6.7.0.30000)
- VMware vSphere (έκδοση 6.7.0.20000)
- VMware ESXi (έκδοση 6.7u3 Δόμηση 14320388)
- VMware Tools 10.3.5
- Wireshark έκδοση 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (Δόμηση 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Προϊόντα δοκιμής

- Google Chrome: Έκδοση 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge: Έκδοση 83.0.478.10 – 84.0.502.0
- Mozilla Firefox: Έκδοση 75.0 – 76.0.1
- Opera: Έκδοση: 67.0.3575.137 – 68.0.3618.125

ΣΥΝΤΑΚΤΕΣ

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Μεθοδολογία δοκιμής

Η μεθοδολογία Web Browser Security (WBS) Test Methodology v4.0 της NSS Labs είναι διαθέσιμη στη διεύθυνση www.nsslabs.com.

Στοιχεία επικοινωνίας

NSS Labs, Inc.

3711 South Mopac Expressway

Building 1, Suite 400

Austin, TX 78746

info@nsslabs.com

www.nsslabs.com

Το παρόν καθώς και λοιπά συναφή έγγραφα είναι διαθέσιμα στη διεύθυνση: www.nsslabs.com. Για να λάβετε ένα εξουσιοδοτημένο αντίγραφο ή να αναφέρετε κάποια κατάχρηση, παρακαλείστε να επικοινωνήσετε με την NSS Labs.

© 2020 NSS Labs, Inc. Με την επιφύλαξη κάθε νόμιμου δικαιώματος. Δεν δύναται κανένα μέρος της παρούσας δημοσίευσης να αναπαραχθεί, αντιγραφεί/σarroωθεί, αποθηκευτεί σε σύστημα επανάκτησης, αποσταλεί μέσω ηλεκτρονικού ταχυδρομείου ή ειδικά να διαδοθεί ή να μεταδοθεί χωρίς τη ρητή γραπτή συγκατάθεση της NSS Labs, Inc. ("εμάς" ή "εμείς").

Παρακαλείστε να διαβάσετε τη δήλωση αποποίησης ευθύνης σε αυτό το πλαίσιο, καθώς εμπεριέχει σημαντικές δεσμευτικές προς εσάς πληροφορίες. Σε περίπτωση που δεν συμφωνείτε με αυτούς τους όρους, δεν πρέπει να συνεχίσετε την ανάγνωση της υπόλοιπης αναφοράς, αλλά να μας επιστρέψετε την αναφορά αμέσως. "Εσείς" ή "εσάς" σημαίνει το άτομο που έχει πρόσβαση σε αυτήν την αναφορά και οποιαδήποτε οντότητα εκ μέρους της οποίας το άτομο απέκτησε αυτήν την αναφορά.

1. Οι πληροφορίες της παρούσας αναφοράς υπόκεινται σε δικές μας αλλαγές άνευ προειδοποίησης και αποποιούμεστε οποιαδήποτε υποχρέωση ενημέρωσης.
2. Οι πληροφορίες της παρούσας αναφοράς θεωρούνται ακριβείς και αξιόπιστες κατά τη στιγμή της δημοσίευσής τους, αλλά δεν είναι εγγυημένες. Η χρήση και πίστη σε αυτή την αναφορά αποτελεί δική σας ευθύνη. Δεν φέρουμε καμία ευθύνη για τυχόν ζημιές, απώλειες ή έξοδα οποιασδήποτε φύσης που προκύπτουν από οποιοδήποτε λάθος ή παράλειψη αυτής της αναφοράς.
3. ΔΕΝ ΠΑΡΕΧΟΝΤΑΙ ΕΓΓΥΗΣΕΙΣ, ΡΗΤΕΣ Ή ΣΙΩΠΗΡΕΣ. ΟΛΕΣ ΟΙ ΣΙΩΠΗΡΕΣ ΕΓΓΥΗΣΕΙΣ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΤΩΝ ΣΙΩΠΗΡΩΝ ΕΓΓΥΗΣΕΩΝ ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ, ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΚΟΠΟ ΚΑΙ ΜΗ ΠΑΡΑΒΙΑΣΗΣ ΑΠΟΠΟΙΟΥΝΤΑΙ ΔΙΑ ΤΟΥ ΠΑΡΟΝΤΟΣ ΚΑΙ ΑΠΟΚΛΕΙΟΝΤΑΙ ΑΠΟ ΕΜΑΣ. ΣΕ ΚΑΜΙΑ ΠΕΡΙΠΤΩΣΗ ΔΕΝ ΦΕΡΟΥΜΕ ΕΥΘΥΝΗ ΓΙΑ ΤΥΧΟΝ ΑΜΕΣΕΣ, ΕΠΑΚΟΛΟΥΘΕΣ, ΤΥΧΑΙΕΣ, ΣΩΦΡΟΝΙΣΤΙΚΕΣ, ΥΠΟΔΕΙΓΜΑΤΙΚΕΣ Ή ΕΜΜΕΣΕΣ ΖΗΜΙΕΣ Ή ΓΙΑ ΤΥΧΟΝ ΑΠΩΛΕΙΑ ΚΕΡΔΟΥΣ, ΕΞΟΔΩΝ, ΔΕΔΟΜΕΝΩΝ, ΠΡΟΓΡΑΜΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ Ή ΑΛΛΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ, ΑΚΟΜΗ ΚΑΙ ΑΝ ΥΠΑΡΞΕΙ ΕΝΗΜΕΡΩΣΗ ΠΕΡΙ ΑΥΤΩΝ.
4. Αυτή η αναφορά δεν αποτελεί επικύρωση, σύσταση ή εγγύηση οποιουδήποτε προϊόντος δοκιμής (υλικό ή λογισμικό) ή του υλικού ή/και λογισμικού που χρησιμοποιήθηκε στις δοκιμές των προϊόντων. Η δοκιμή δεν εγγυάται ότι δεν υπάρχουν σφάλματα ή ελαττώματα στα προϊόντα ή ότι τα προϊόντα ανταποκρίνονται στις προσδοκίες, τις απαιτήσεις, τις ανάγκες ή τις προδιαγραφές σας είτε ότι θα λειτουργούν χωρίς διακοπή.
5. Αυτή η αναφορά δεν συνεπάγεται καμία επικύρωση, χορηγία, συνεργασία ή επαλήθευση από ή με οποιονδήποτε οργανισμό αναφέρεται στην παρούσα αναφορά.
6. Όλες οι εμπορικές επωνυμίες, σήματα υπηρεσιών και εμπορικές ονομασίες που χρησιμοποιούνται στην παρούσα αναφορά αποτελούν τις εμπορικές επωνυμίες, τα σήματα υπηρεσίας και τις εμπορικές ονομασίες των αντίστοιχων κατόχων τους.