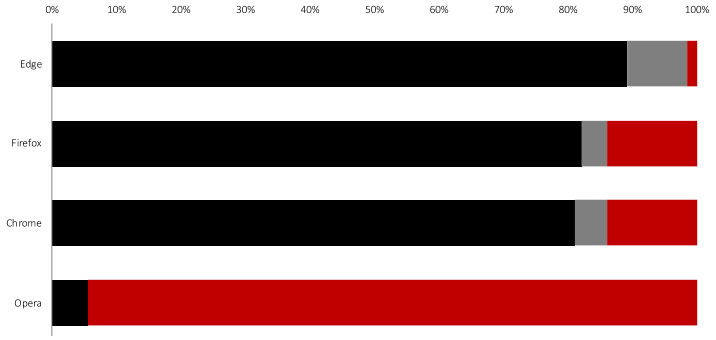
2ο τρίμηνο 2020 ΣΥΓΚΡΙΤΙΚΗ ΑΝΑΦΟΡΑ ΔΟΚΙΜΩΝ

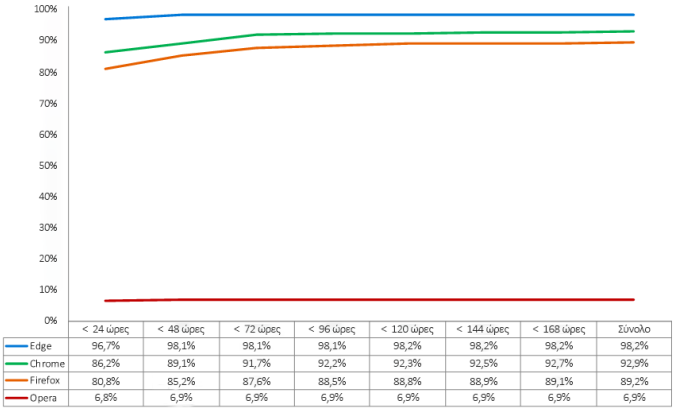
Επισκόπηση

Κατά τη διάρκεια του 2ου τριμήνου του 2020, η NSS Labs διεξήγαγε μια ανεξάρτητη δοκιμή αναφορικά με την προστασία από κακόβουλο λογισμικό που προσφέρεται από τα προγράμματα περιήγησης Web: 32.267 μεμονωμένες δοκιμές (ανά πρόγραμμα περιήγησης) χρησιμοποιώντας 1.065 μοναδικά δείγματα για 34 ημέρες. Για την προστασία έναντι κακόβουλου λογισμικού ο Microsoft Edge χρησιμοποιεί το Microsoft Defender SmartScreen. Το Google Chrome και το Mozilla Firefox χρησιμοποιούν το Google Safe Browsing API. Το Opera χρησιμοποιεί τη Yandex.

Ο Microsoft Edge προσέφερε τη μεγαλύτερη προστασία, αποκλείοντας το 98,5% των κακόβουλων λογισμικών, παρέχοντας παράλληλα το υψηλότερο ποσοστό αυτόματου αποκλεισμού (96,7%). Το Firefox παρείχε τη δεύτερη μεγαλύτερη προστασία, αποκλείοντας κατά μέσο όρο το 86,1%, ενώ ακολουθούσε το Google Chrome με 86,0%. Το Opera απέκλεισε το 5,6%.



Σύνοψη των αποτελεσμάτων

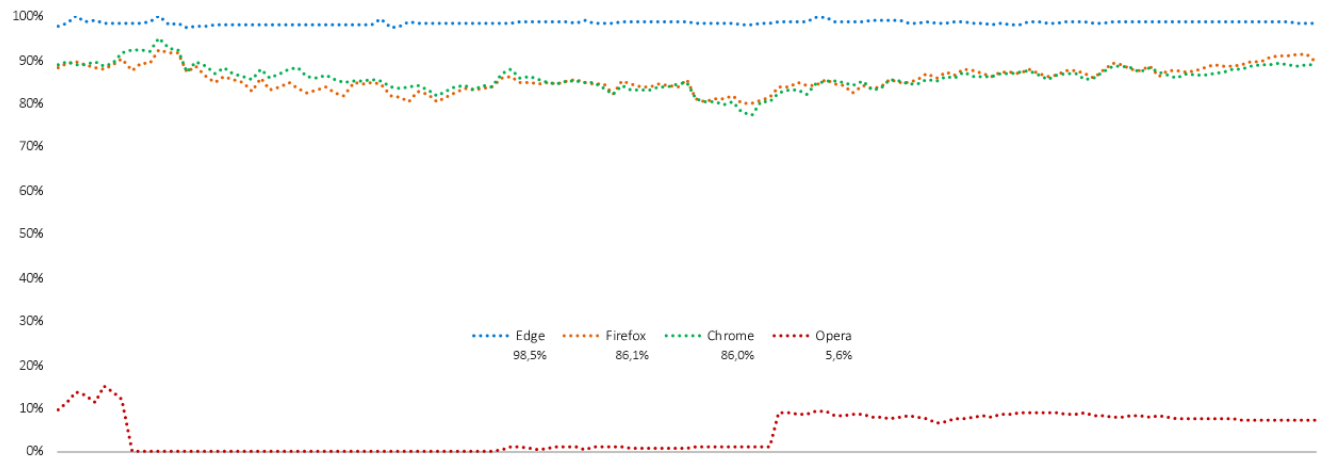


	< 24 ώρες	< 48 ώρες	< 72 ώρες	< 96 ώρες	< 120 ώρες	< 144 ώρες	< 168 ώρες	Σύνολο
Edge	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Chrome	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Firefox	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Opera	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Τα συστήματα διαχείρισης φήμης μειώνουν τον χρόνο που χρειάζονται οι εισβολείς για να επιτύχουν τους στόχους τους αποτρέποντας ή προειδοποιώντας τους χρήστες ότι μια διεύθυνση URL, ένα αρχείο ή μια εφαρμογή είναι επιβλαβής. Ωστόσο, οι χρήστες επισκέπτονται διαρκώς νέες τοποθεσίες Web, κατεβάζουν αρχεία και εγκαθιστούν εφαρμογές. Τα συστήματα διαχείρισης φήμης δεν μπορούν απλώς να αποκλείσουν οτιδήποτε καινούριο. Γνωρίζοντάς το αυτό, οι εκστρατείες κακόβουλου λογισμικού των εισβολέων αλλάζουν διαρκώς, με το μεγαλύτερο μέρος όλων των επιθέσεων να λαμβάνουν χώρα τις πρώτες ώρες μετά την κυκλοφορία μιας εκστρατείας. Συνεπώς, η ακριβής και γρήγορη ταξινόμηση του περιεχομένου είναι το κλειδί για μια επιτυχή προστασία.

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

Προστασία από κακόβουλο λογισμικό με την πάροδο του χρόνου



Καθ' όλη τη διάρκεια της δοκιμής, προσθέτονταν συνεχώς νέα κακόβουλα λογισμικά. Οι διευθύνσεις URL, τα αρχεία και οι εφαρμογές που δεν ήταν πλέον προσβάσιμες ή φιλοξενούσαν κακόβουλο λογισμικό αφαιρέθηκαν. Κάθε σημείο δεδομένων υπολογίζεται από τις μετρήσεις που καταγράφονται σε μια συγκεκριμένη χρονική στιγμή. Σε περίπτωση που ένα κακόβουλο λογισμικό αποκλειστεί σε πρώιμο στάδιο, η βαθμολογία του προγράμματος περιήγησης αναφορικά με τη συνοχή της προστασίας με την πάροδο του χρόνου θα αυξηθεί. Ειδάλλως, εάν το πρόγραμμα περιήγησης δεν αποκλείσει το κακόβουλο λογισμικό, η βαθμολογία θα μειωθεί.

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

Γενικές πληροφορίες

Οι επιθέσεις κακόβουλων λογισμικών κοινωνικής μηχανικής (SEM) χρησιμοποιούν έναν δυναμικό συνδυασμό μέσων κοινωνικής δικτύωσης, λογαριασμών ηλεκτρονικού ταχυδρομείου που έχουν υποκλαπεί, ψευδών ειδοποιήσεων για τυχόν προβλήματα στον υπολογιστή και άλλες απάτες με σκοπό να ενθαρρύνουν τους χρήστες να κατεβάσουν ένα κακόβουλο λογισμικό. Οι δράστες του ηλεκτρονικού εγκλήματος χρησιμοποιούν λογαριασμούς ηλεκτρονικού ταχυδρομείου που έχουν υποκλαπεί για να εκμεταλλευτούν την εμπιστοσύνη μεταξύ των επαφών και να εξαπατήσουν τα θύματα ώστε να πιστέψουν ότι οι σύνδεσμοι με κακόβουλα αρχεία είναι αξιόπιστοι. Οι λογαριασμοί των μέσων κοινωνικής δικτύωσης που έχουν υποκλαπεί χρησιμοποιούνται με τον ίδιο τρόπο με τους λογαριασμούς ηλεκτρονικού ταχυδρομείου που έχουν υποκλαπεί. Εντούτοις, στην περίπτωση των μέσων κοινωνικής δικτύωσης, ο κύκλος γίνεται ευρύτερος: φίλοι ή ακόμη φίλοι φίλων υπόκεινται στον κίνδυνο της εξαπάτησης.

Οι μέθοδοι κοινωνικής μηχανικής ενδέχεται να περιλαμβάνουν αναδυόμενα μηνύματα, συμβουλεύοντας, για παράδειγμα, τους χρήστες ότι πρέπει να εγκαταστήσουν εφαρμογές όπως το Adobe Flash Player ή ότι ο υπολογιστής τους είτε είναι μολυσμένος είτε απαιτεί κάποια ενημέρωση. Μόλις εγκατασταθεί το κακόβουλο λογισμικό, τα θύματα είναι πλέον ευάλωτα σε υποκλοπή της ταυτότητάς τους, σε έκθεση των τραπεζικών λογαριασμών και άλλες δυνητικά καταστροφικές συνέπειες.

Προστασία προγραμμάτων περιήγησης Web από κακόβουλο λογισμικό

Για την προστασία από κακόβουλο λογισμικό, τα προγράμματα περιήγησης χρησιμοποιούν συστήματα διαχείρισης φήμης βασισμένα στο cloud που σαρώνουν το Internet για κακόβουλες τοποθεσίες Web και κατόπιν κατηγοριοποιούν ανάλογα το περιεχόμενο, είτε προσθέτοντάς το σε λίστες αποκλεισμού είτε σε λίστες αποδοχής, είτε προσδίδοντας μια βαθμολογία (ανάλογα με την προσέγγιση του προμηθευτή).

Αυτές οι τεχνικές κατηγοριοποίησης μπορούν να εκτελεστούν χειροκίνητα ή αυτόματα. Το δεύτερο λειτουργικό στοιχείο προστασίας από κακόβουλο λογισμικό περιλαμβάνει το πρόγραμμα περιήγησης Web το οποίο απαιτεί πληροφορίες φήμης από τα συστήματα διαχείρισης φήμης που βασίζονται στο cloud σχετικά με συγκεκριμένες διευθύνσεις URL, αρχεία ή εφαρμογές και στη συνέχεια προειδοποιεί για το κακόβουλο λογισμικό ή το αποκλείει.

Εάν τα αποτελέσματα υποδεικνύουν ότι υπάρχει κακόβουλο λογισμικό, τότε το πρόγραμμα περιήγησης Web ανακατευθύνει τον χρήστη σε ένα προειδοποιητικό μήνυμα που εξηγεί ότι η διεύθυνση URL, το αρχείο ή η εφαρμογή είναι κακόβουλη. Ορισμένοι μηχανισμοί φήμης περιλαμβάνουν επιπλέον ένα πρόσθετο εκπαιδευτικό περιεχόμενο. Αντίθετα, εάν το περιεχόμενο χαρακτηριστεί "καλό", το πρόγραμμα περιήγησης Web δεν αναλαμβάνει δράση και ο χρήστης δεν ενημερώνεται ότι μόλις πραγματοποιήθηκε έλεγχος ασφαλείας από το πρόγραμμα περιήγησης.

Το Google και το Firefox χρησιμοποιούν το Google Safe Browsing API τόσο για τη διαχείριση φήμης των διευθύνσεων URL όσο και για τον αποκλεισμό ή την προειδοποίηση των χρηστών σχετικά με τη λήψη συγκεκριμένων τύπων αρχείων. 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,[1] PhishTank,[2] και Metamask[3], καθώς και λίστα αποκλεισμού κακόβουλου λογισμικού από τη Yandex.[4]

Επιπλέον, το Microsoft Defender SmartScreen ενσωματώθηκε ως χαρακτηριστικό ολόκληρου του λειτουργικού συστήματος με την ενημέρωση των Windows 10 τον Οκτωβρίου 2017. Η έκδοση του λειτουργικού συστήματος της προστασίας SmartScreen αποτελεί μηχανισμό ασφαλείας για όλα τα προγράμματα περιήγησης, τα προγράμματα-πελάτες ηλεκτρονικής αλληλογραφίας, τα USB και άλλες εφαρμογές, ως μέρος προστασίας του λειτουργικού συστήματος από κακόβουλα λογισμικά.. Επομένως, οι χρήστες επωφελούνται από την προστασία των διευθύνσεων URL του προγράμματος περιήγησης, την προστασία των εφαρμογών/ αρχείων του προγράμματος περιήγησης, καθώς και την προστασία του λειτουργικού συστήματος.

Σύνθεση δοκιμής – Δείγματα κακόβουλου λογισμικού

Τα δεδομένα της παρούσας αναφοράς καλύπτουν μια περίοδο δοκιμής 34 ημερών μεταξύ της 21ης Απριλίου 2020 και της 25ης Μαΐου 2020. Όλες οι δοκιμές διεξήχθησαν στις εγκαταστάσεις δοκιμών της NSS στο Όστιν του Τέξας. Κατά τη διάρκεια της δοκιμής, οι μηχανικοί της NSS παρακολουθούσαν τακτικά τη συνδεσιμότητα για να διασφαλίσουν ότι τα υπό δοκιμή προγράμματα περιήγησης θα έχουν πρόσβαση σε κακόβουλα λογισμικά, καθώς και στις υπηρεσίες διαχείρισης φήμης στο cloud.

Δόθηκε έμφαση στην ενεργητικότητα, επομένως αξιολογήθηκε μεγαλύτερος αριθμός δειγμάτων από ό, τι εντέλει προσμετρήθηκε ως μέρος των συνολικών αποτελεσμάτων των δοκιμών, καθώς νέα δείγματα προσθέτονταν συνεχώς στη δοκιμή και "νεκρά" δείγματα αφαιρούνταν.

Συνολικός αριθμός κακόβουλων δειγμάτων στη δοκιμή

Συνολικά 1.844 ακατέργαστα, μη επικυρωμένα δείγματα ελέγχθηκαν πολλάκις με κάθε πρόγραμμα περιήγησης Web σε συνολικά 182.676 μεμονωμένες δοκιμές που διεξήχθησαν χωρίς διακοπή για 822 ώρες (ανά 6 ώρες για 34 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, 1.065 μοναδικά, έγκυρα δείγματα κακόβουλου λογισμικού συμπεριλήφθηκαν στις 129.068 μεμονωμένες, έγκυρες δοκιμές κακόβουλου λογισμικού (32.267 ανά πρόγραμμα περιήγησης), παρέχοντας ένα περιθώριο σφάλματος μικρότερο από 2 τοις εκατό (<2%) με επίπεδο εμπιστοσύνης 95%.

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

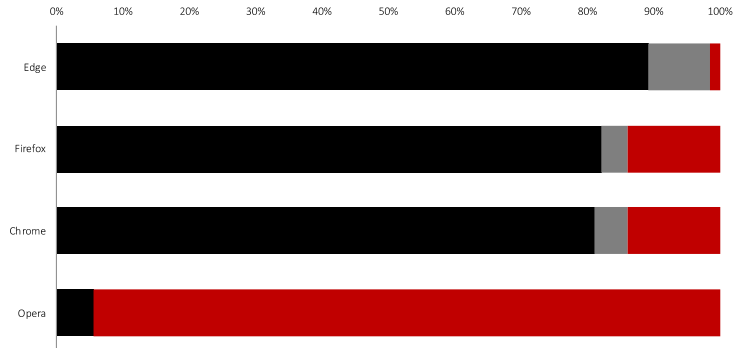
[2] http://www.phishtank.com/

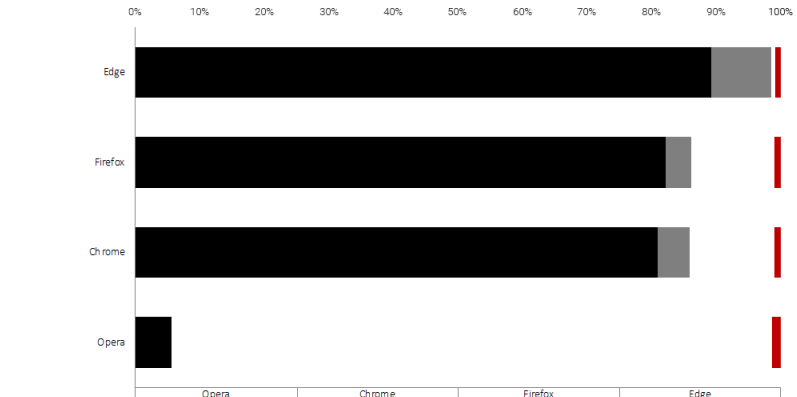
[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

Ποσοστό αποκλεισμού κακόβουλων λογισμικών

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 της κοινωνικής μηχανικής των κακόβουλων λογισμικών. Δεδομένου ότι οι τοποθεσίες Web κακόβουλων λογισμικών έχουν μικρή διάρκεια ζωής, είναι ουσιώδες να εντοπίζονται, να επικυρώνονται, να ταξινομούνται και να προστίθενται στο σύστημα διαχείρισης φήμης το συντομότερο δυνατό. Ως εκ τούτου, 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 τα περισσότερα κακόβουλα λογισμικά αποκλείονται τις πρώτες 24 ώρες της ανίχνευσής τους, παρά μετέπειτα.





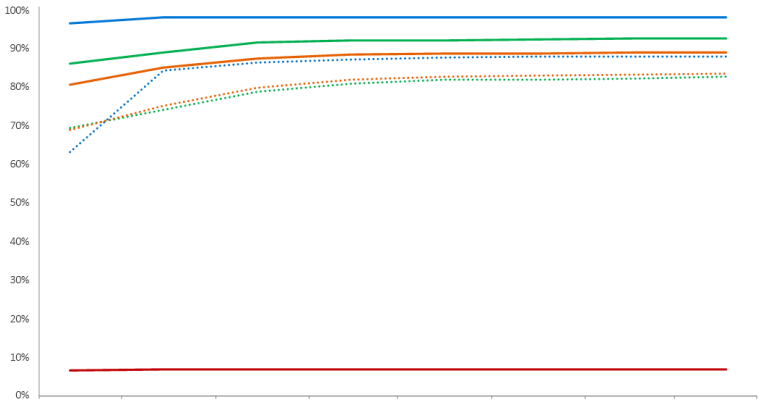
	Opera	Chrome	Firefox	Edge
Φήμη URL	5,6%	80,9%	82,1%	89,2%
Φήμη URL και εφαρμογής	0,0%	5,0%	4,0%	9,3%
Φήμη URL, εφαρμογής και λειτουργικού συστήματος	93,1%	13,1%	13,0%	0,7%
Δεν εντοπίστηκαν	1,4%	0,9%	0,9%	0,8%

Η κύρια τεχνολογία προστασίας του Edge είναι το SmartScreen που προστατεύει από επιθέσεις βάσει διευθύνσεων URL μέσω μιας ολοκληρωμένης υπηρεσίας διαχείρισης φήμης διευθύνσεων URL που βασίζεται στο cloud, καθώς και μιας εφαρμογής διαχείρισης φήμης για αποκλεισμό κακόβουλων αρχείων. Το SmartScreen με την εφαρμογή διαχείρισης φήμης απέκλεισε το 98,5% για τον Edge. Το Mozilla Firefox και το Google Chrome χρησιμοποιούν το Safe Browsing API. Το Firefox απέκλεισε το 86,1%. Το Google Chrome απέκλεισε το 86,0%. Το Opera που χρησιμοποιεί έναν συνδυασμό προγραμμάτων αποκλεισμού διαφόρων πηγών απέκλεισε το 5,6%.

Επιπλέον, το Microsoft Defender SmartScreen απέκλεισε ένα επιπρόσθετο 93,1% για το Opera, 13,1% για το Chrome, 13,0% για το Firefox και 0,7% κακόβουλα αρχεία για τον Edge, όταν επιχειρήσαμε να τα εκτελέσουμε.

Ιστόγραμμα προστασίας κακόβουλου λογισμικού

Η άμεση προστασία έναντι νέων κακόβουλων λογισμικών είναι καθοριστικής σημασίας. Όταν ανιχνεύονται τοποθεσίες Web που φιλοξενούν κακόβουλα λογισμικά, 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 ιστόγραμμα απεικονίζει τον χρόνο που χρειάζεται κάθε πρόγραμμα περιήγησης για να αποκλείσει ένα κακόβουλο λογισμικό μετά την εισαγωγή του δείγματος στον κύκλο δοκιμών. Εντός διαστήματος επτά ημερών, τα αθροιστικά ποσοστά προστασίας υπολογίζονται ανά μέρα έως ότου αποκλειστούν οι απειλές.



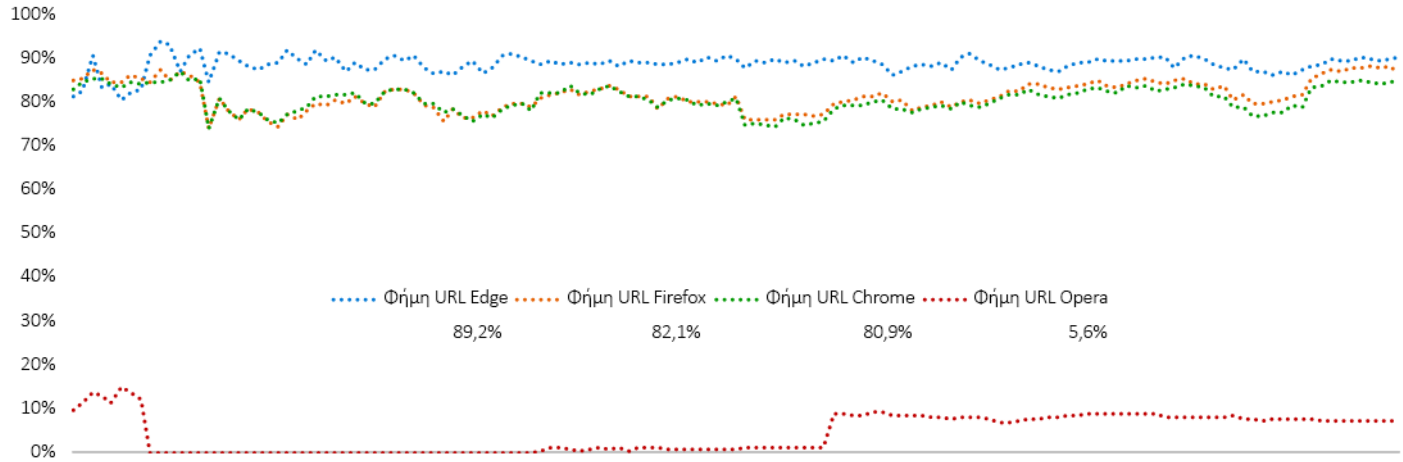
	< 24 ώρες	< 48 ώρες	< 72 ώρες	< 96 ώρες	< 120 ώρες	< 144 ώρες	< 168 ώρες	Σύνολο
Φήμη Edge με εφαρμογή	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Φήμη Edge με URL	63,4%	84,5%	86,5%	87,3%	87,8%	88,1%	88,1%	88,1%
Φήμη Chrome με εφαρμογή	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Φήμη Chrome με URL	69,7%	74,4%	79,0%	81,0%	82,0%	82,2%	82,4%	82,7%
Φήμη Firefox με εφαρμογή	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Φήμη Firefox με URL	69,1%	75,3%	80,0%	82,1%	82,9%	83,0%	83,4%	83,6%
Φήμη Opera με URL	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Κατά τη διάρκεια της δοκιμής, ο Microsoft Edge επέδειξε αρχικό ποσοστό προστασίας της τάξης του 96,7% έναντι κακόβουλων λογισμικών. Το Google Chrome και το Mozilla Firefox πέτυχαν αρχικό ποσοστό προστασίας 86,2% και 80,8% αντίστοιχα. Το αρχικό ποσοστό προστασίας του Opera ανήλθε στο 6,8%. Κατά το τέλος της έβδομης ημέρας των δοκιμών, όλα τα προγράμματα περιήγησης Web παρουσίασαν αύξηση της προστασίας. Η προστασία του Microsoft Edge αυξήθηκε κατά 4,5% σε ποσοστό 98,2%. Η προστασία του Google Chrome αυξήθηκε κατά 6,7% σε ποσοστό 92,9%, ενώ του Mozilla Firefox αυξήθηκε κατά 8,4% σε ποσοστό 89,2%. Η προστασία του Opera αυξήθηκε κατά 0,1% σε ποσοστό 6,9%.

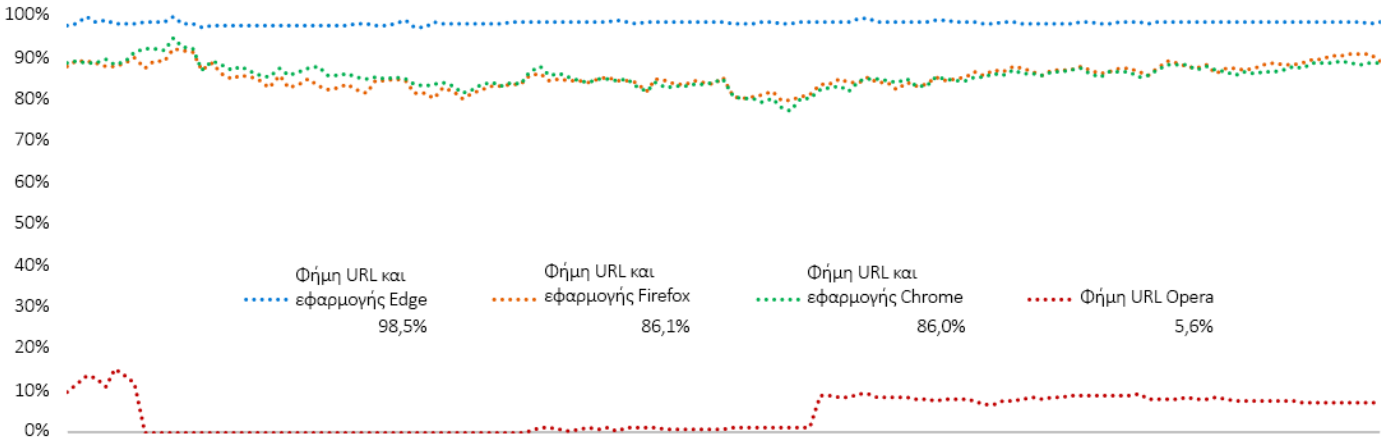
Συνοχή προστασίας με την πάροδο του χρόνου

Καθ' όλη τη διάρκεια της δοκιμής, προσθέτονταν συνεχώς νέα κακόβουλα λογισμικά. Οι διευθύνσεις URL, τα αρχεία και οι εφαρμογές που δεν ήταν πλέον προσβάσιμες ή φιλοξενούσαν κακόβουλο λογισμικό αφαιρέθηκαν. Κάθε σημείο δεδομένων υπολογίζεται από τις μετρήσεις που καταγράφονται σε μια συγκεκριμένη χρονική στιγμή. Σε περίπτωση που ένα κακόβουλο λογισμικό αποκλειστεί σε πρώιμο στάδιο, η βαθμολογία του προγράμματος περιήγησης αναφορικά με τη συνοχή της προστασίας με την πάροδο του χρόνου θα αυξηθεί. Ειδάλλως, εάν το πρόγραμμα περιήγησης δεν αποκλείσει το κακόβουλο λογισμικό, η βαθμολογία θα μειωθεί.

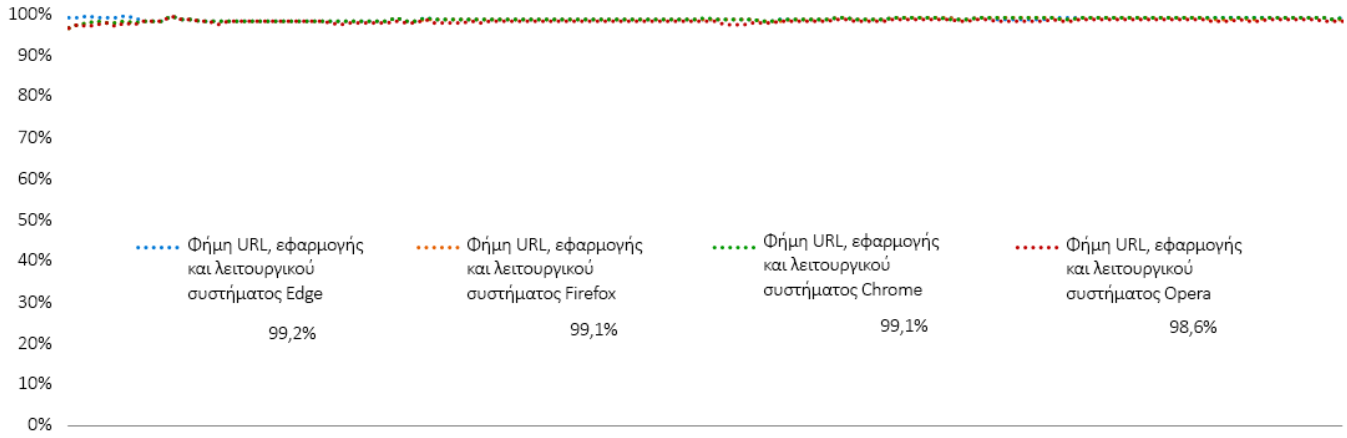
Η δοκιμή αποκάλυψε τρία επίπεδα προστασίας: διαχείριση φήμης διεύθυνσης URL, διαχείριση φήμης εφαρμογής εντός του προγράμματος περιήγησης και διαχείριση φήμης εφαρμογής λειτουργικού συστήματος. Η διαχείριση φήμης διεύθυνσης URL προσέφερε μια ευλόγως καλή προστασία.



Η κλιμάκωση της διαχείρισης φήμης εφαρμογών σε επίπεδα αύξησε την προστασία.



Η διαχείριση φήμης του λειτουργικού συστήματος πρόσφερε πρόσθετη προστασία. Ιδανικά, το πρόγραμμα περιήγησης Web θα αποκλείσει τα κακόβουλα λογισμικά, ώστε να μην εισβάλουν ποτέ στο λειτουργικό σύστημα. Ωστόσο, οι δοκιμές έδειξαν ότι η διαχείριση φήμης του λειτουργικού συστήματος ήταν αρκετά αποτελεσματική.



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 – 84.0.516.1
- Mozilla Firefox: Έκδοση 75.0 – 76.0.1
- Opera: Έκδοση: 67.0.3575.137 – 68.0.3618.125

Συντάκτες

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