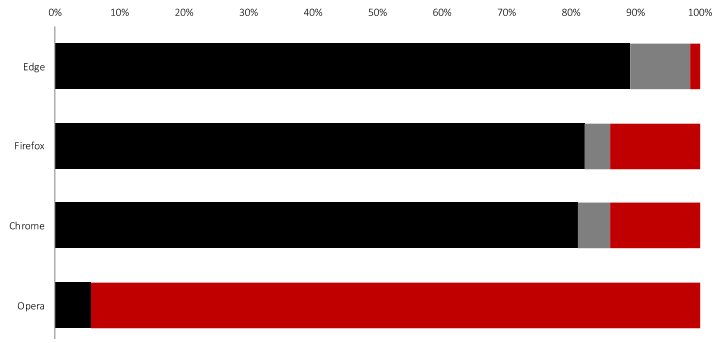
2020 második negyedéve JELENTÉS AZ ÖSSZEHASONLÍTÓ TESZTRŐL

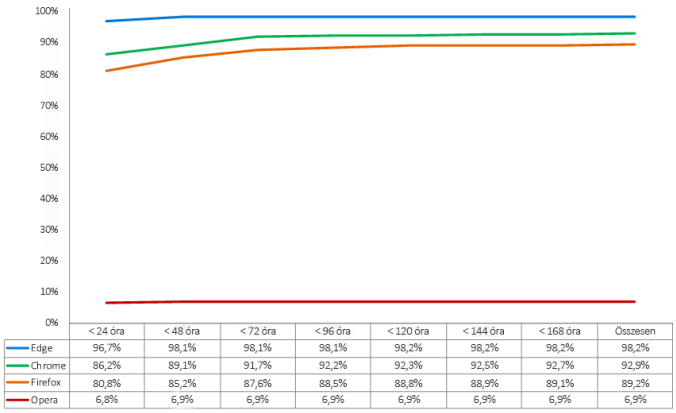
Áttekintés

2020 második negyedévében az NSS Labs független tesztelésnek vetette alá a böngészők által a rosszindulatú programok ellen kínált védelmet: 32267 különálló tesztet végzett (böngészőnként) 1065 különböző minta használatával 34 napon keresztül. A rosszindulatú programok elleni védekezéshez a Microsoft Edge a Microsoft Defender SmartScreen szoftvert, a Google Chrome és a Mozilla Firefox a Google Safe Browsing API-t, az Opera pedig a Yandex keresőrendszert használja.

A Microsoft Edge nyújtotta a legnagyobb védelmet, a rosszindulatú programok 98,5%-át blokkolta, emellett a legmagasabb azonnali védelmi arányt (96,7%) biztosította. A Firefox nyújtotta a második legnagyobb védelmet, átlagosan 86,1%-ot blokkolt, ezt követte a Google Chrome 86,0%-os blokkolással. Az Opera blokkolási aránya 5,6% volt.



Az eredmények összefoglalása

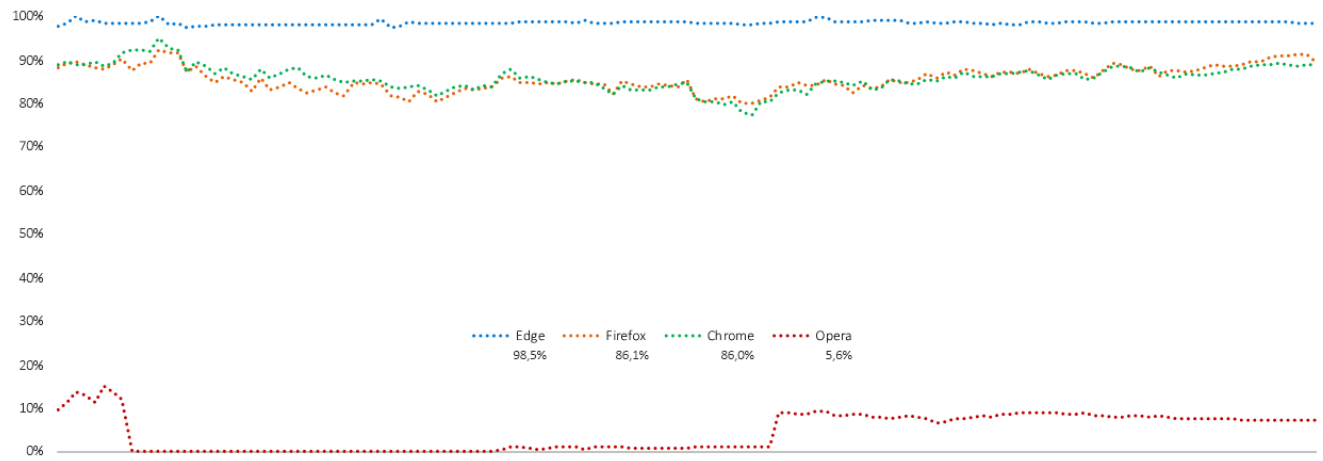


	< 24 óra	< 48 óra	< 72 óra	< 96 óra	< 120 óra	< 144 óra	< 168 óra	Összesen
Edge	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Chrome	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Firefox	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Opera	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

A besorolási rendszerek úgy rövidítik le azt az időt, amely alatt a támadók elérhetik a céljukat, hogy figyelmeztetik a felhasználókat, hogy egy URL, egy fájl vagy alkalmazás veszélyes, illetve blokkolják azokat. A felhasználók azonban folyamatosan új webhelyeket látogatnak, fájlokat töltenek le és alkalmazásokat telepítenek. A besorolási rendszerek nem blokkolhatnak egyszerűen mindent, ami új. Ennek ismeretében a támadók folyamatosan változtatják a rosszindulatú programokkal végrehajtott kampányokat, és az összes támadás többsége a kampány elindításának első néhány órájában történik. Ezért a tartalom gyors és pontos osztályozása kulcsfontosságú a sikeres védelemhez.

Az NSS Labs azt mérte fel, hogy a böngészők milyen mértékben képesek blokkolni a rosszindulatú programokat, amint azokat megtaláljuk az interneten. A rosszindulatú URL-eket, fájlokat és alkalmazásokat határónként teszteltük, hogy megállapítsuk, mennyi időbe telik a gyártóknak a védelem biztosítása, ha egyáltalán alkalmaznak védelmet.

A rosszindulatú programok elleni védelem időbeli alakulása



A teszt során folyamatosan bővítettük az új rosszindulatú programok körét. A már nem elérhető vagy rosszindulatú programot tartalmazó URL-eket, fájlokat és alkalmazásokat eltávolítottuk. Minden adatpont kiszámítása egy meghatározott időpillanatban rögzített mérések alapján történt. Ha a rosszindulatú program blokkolása korán megtörtént, nő a böngésző pontszáma a védelem időbeli konzisztenciájának terén. Ha a böngésző nem blokkolta a rosszindulatú programot, akkor a pontszám csökken.

A tesztelés a Web Browser Test Methodology 4.0 verzión alapult (lásd: www.nsslabs.com).

Háttér

A megtévesztésen alapuló csalást alkalmazó rosszindulatú programokkal (social engineered malware, SEM) végrehajtott támadások a közösségi média, az ellopott e-mail-fiókok, a számítógép problémáira figyelmeztető hamis értesítések és egyéb megtévesztések dinamikus kombinációjával veszik rá a felhasználókat a rosszindulatú programok letöltésére. A kiberbűnözők ellopott e-mail-fiókokkal használják ki a partnerek közötti megbízható kapcsolatot, és az áldozatokat megtévesztve azt a látszatot keltik, hogy a rosszindulatú fájlokra mutató hivatkozások megbízhatóak. Az ellopott közösségi médiabeli fiókokat ugyanúgy használják fel, ahogy az ellopott e-mail-fiókokat. A közösségi hálózatok esetében azonban a kör szélesebb: fennáll a barátok, és akár a barátok barátainak megtévesztési veszélye.

A megtévesztésen alapuló csalások egyik taktikája az előugró üzenetek használata, amelyek például olyan alkalmazások telepítését javasolják a felhasználóknak, mint az Adobe Flash Player, vagy a számítógépre telepítendő alkalmazásokra és frissítésekre vagy a számítógépük fertőzöttségére figyelmeztetnek. A rosszindulatú program telepítése után az áldozatoknál személyiséglopások, bankszámla-feltörések és egyéb kétségbeejtő következmények fordulhatnak elő.

A böngészők által a rosszindulatú programok ellen nyújtott védelem

A rosszindulatú programok elleni védekezéshez a böngészők felhőalapú besorolási rendszereket használnak, amelyek rosszindulatú webhelyeket keresnek az interneten, majd a tartalmukat megfelelően kategorizálva tiltólistára vagy engedélyezési listára helyezik azokat, vagy pontszámot rendelnek hozzájuk (a gyártó által alkalmazott megoldástól függően).

Ezek a kategorizálási technikák végrehajthatók manuálisan vagy automatikusan. A rosszindulatú programok elleni védelem másik funkcionális összetevője a böngésző által végrehajtott információkérés: a böngésző lekéri az URL-címek, a fájlok vagy az alkalmazások besorolási információt a felhőalapú besorolási rendszerekből, majd figyelmeztetést jelenít meg vagy blokkolja a rosszindulatú programot.

Ha az eredmények rosszindulatú program jelenlétét jelzik, a böngésző átirányítja a felhasználót egy figyelmeztető üzenetre, amely tájékoztatja a felhasználót, hogy az URL, a fájl vagy az alkalmazás rosszindulatú. Néhány besorolási rendszer magyarázó jellegű tartalmat is biztosít. Ha azonban a tartalom „jónak” lett minősítve, a böngésző nem hajt végre semmilyen műveletet, és felhasználó nem fog tudni arról, hogy a böngésző biztonsági ellenőrzést hajtott végre.

A Google és a Firefox a Google Safe Browsing API-t használja az URL-besoroláshoz, valamint a blokkoláshoz, illetve a bizonyos típusú fájlok letöltésekor megjelenített figyelmeztetéshez. A Microsoft Edge a Microsoft Defender SmartScreen szoftvert használja, beleértve az alkalmazásbesorolási szolgáltatást, hogy védelmet nyújtson az adathalászat és a rosszindulatú programok fenyegetései ellen. Az Opera a Netcraft,[1] a PhishTank[2] és a Metamask[3] tiltólistáinak kombinációját használja, valamint a Yandex rosszindulatú programokra vonatkozó tiltólistáját.[4]

Ezenkívül a Microsoft Defender SmartScreen be lett építve az operációs rendszer szolgáltatásaként a Windows 10 2017. októberi frissítésébe. A SmartScreen-védelmet biztosító operációs rendszer védőhálónak tekinthető minden böngésző, e-mail-kliens, USB és egyéb alkalmazás számára a rosszindulatú programok rendszerszintű elleni védelem részeként. Biztosítja a felhasználók számára a böngészőben az URL-ek védelmét, az alkalmazások és a fájlok védelmét, valamint az operációs rendszer védelmét.

A teszt összetétele – a rosszindulatú programok mintái

Az ebben a jelentésben található adatok egy 34 napos időszakra vonatkoznak, 2020. április 21. és 2020. május 25. között. A tesztelés az NSS tesztlaborjában történt, a texasi Austinban. A teszt során az NSS mérnökei rutinszerűen figyelték a csatlakozásokat annak biztosításához, hogy a tesztelt böngésző hozzáférhessen a rosszindulatú programhoz, valamint a felhőbeli besorolási rendszerhez is.

A hangsúly a frissességen volt, ezért számos mintát értékeltek ki, majd tartottak meg a tesztkészlet részeként, a tesztet folyamatosan bővítették új mintákkal, és eltávolították a működésképtelenné vált mintákat.

A tesztelt rosszindulatú minták száma

Összesen 1844 nyers, nem érvényesített mintát teszteltek többször minden böngészőben, összesen 182676 különálló tesztet hajtottak végre megszakítás nélkül 822 órán keresztül (6 óránként 34 napon keresztül). Az NSS mérnökei eltávolították azokat a mintákat, amelyek nem feleltek meg az érvényesítési feltételeknek, beleértve a biztonsági rések által érintetteket (ez nem volt része a tesztnek). Végül 1065 különböző, érvényes rosszindulatú minta szerepelt 129068 különálló, érvényes tesztben (böngészőnként 32267), ami 2 százaléknál kisebb (<2%) hibahatárt eredményezett 95%-os megbízhatósági szinttel.

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

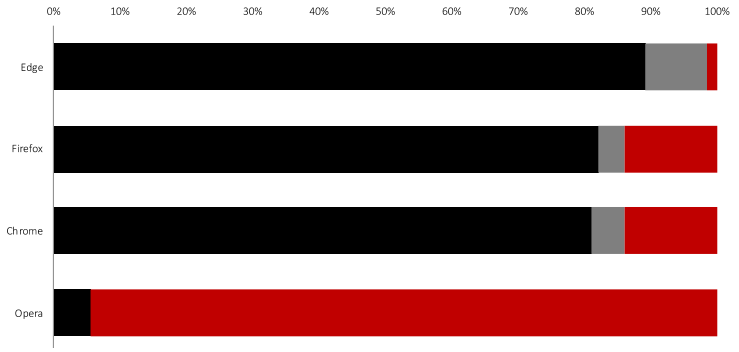
[2] http://www.phishtank.com/

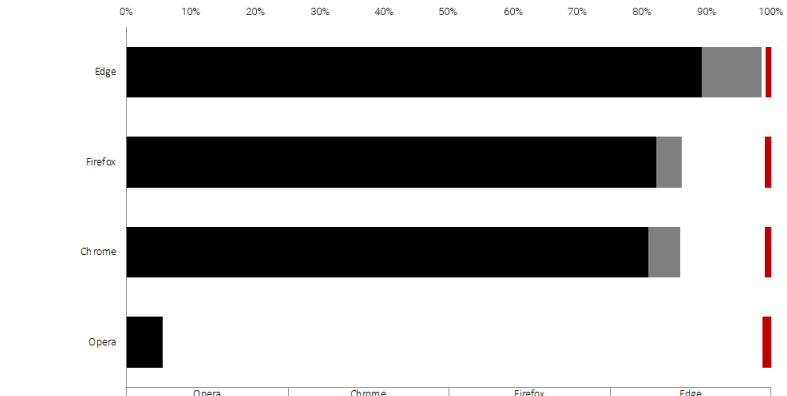
[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

A rosszindulatú programok blokkolási aránya

Az a képesség, hogy figyelmeztetni tudják a potenciális áldozatokat a rosszindulatú webhelyek felkeresésekor, kivételes helyzetbe emeli a böngészőket a megtévesztésen alapuló rosszindulatú programok elleni küzdelemben. Mivel a rosszindulatú programok webhelyei rövid élettartamúak, lényeges, hogy a webhely felderítése, ellenőrzése, besorolása és a besorolási rendszerbe való felvétele a lehető leggyorsabban történjen. Ebből következően a jó besorolási rendszernek pontosnak és gyorsnak kell lennie, hogy magas elfogási arányt tudjon nyújtani. A böngészők fejlesztői tökéletesen értik ezt az összefüggést, és lényegesen több rosszindulatú programot sikerül blokkolni az észlelés utáni első 24 órában, mint azután.





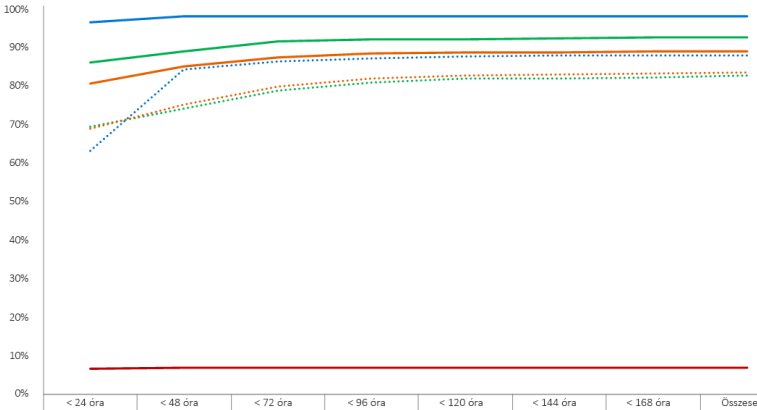
	Opera	Chrome	Firefox	Edge
URL-besorolás	5,6%	80,9%	82,1%	89,2%
URL + alk. besorolás	0,0%	5,0%	4,0%	9,3%
URL + alk. + op. r. besorolás	93,1%	13,1%	13,0%	0,7%
Kimaradt	1,4%	0,9%	0,9%	0,8%

Az Edge alapvető védelmi technológiája a SmartScreen, amely URL-alapú védelmet biztosít a támadások ellen egy integrált, felhőalapú URL-besorolási szolgáltatáson keresztül, valamint alkalmazásbesorolást a rosszindulatú fájlok blokkolásához. Az alkalmazásbesorolást használó SmartScreen blokkolási aránya 98,5% volt az Edge esetében. A Mozilla Firefox és a Google Chrome a Safe Browsing API-t használja. A Firefox blokkolási aránya 86,1% volt. A Google Chrome blokkolási aránya 86,0% volt. A több forrásból származó tiltólisták kombinációját használó Opera esetében 5,6%-os volt a blokkolás.

Ezenkívül a Microsoft Defender SmartScreen a rosszindulatú fájlokból további 93,1%-ot blokkolt az Opera esetében, 13,1%-ot a Chrome esetében, 13,0%-ot a Firefox esetében és 0,7%-ot az Edge esetében, amikor megpróbáltuk végrehajtani ezeket a fájlokat.

A rosszindulatú programok elleni védelem hisztogramja

A rosszindulatú programok elleni azonnali védelem kritikus fontosságú. A rosszindulatú programokat tartalmazó webhelyeket a felderítésük után általában viszonylag rövid időn belül lekapcsolják. Az olyan termékek esetében, amelyek nem alkalmazzák időben a védelmet, már késő lehet a fenyegetések elleni intézkedések végrehajtása. A hisztogram azt mutatja, milyen hosszú ideig tartott az egyes böngészőkben a rosszindulatú programok blokkolása, miután a minta bekerült a tesztciklusba. A hétnapos időablakon belül összesített védelmi arányokat számítottunk minden nap, amíg meg nem történt a fenyegetések blokkolása.



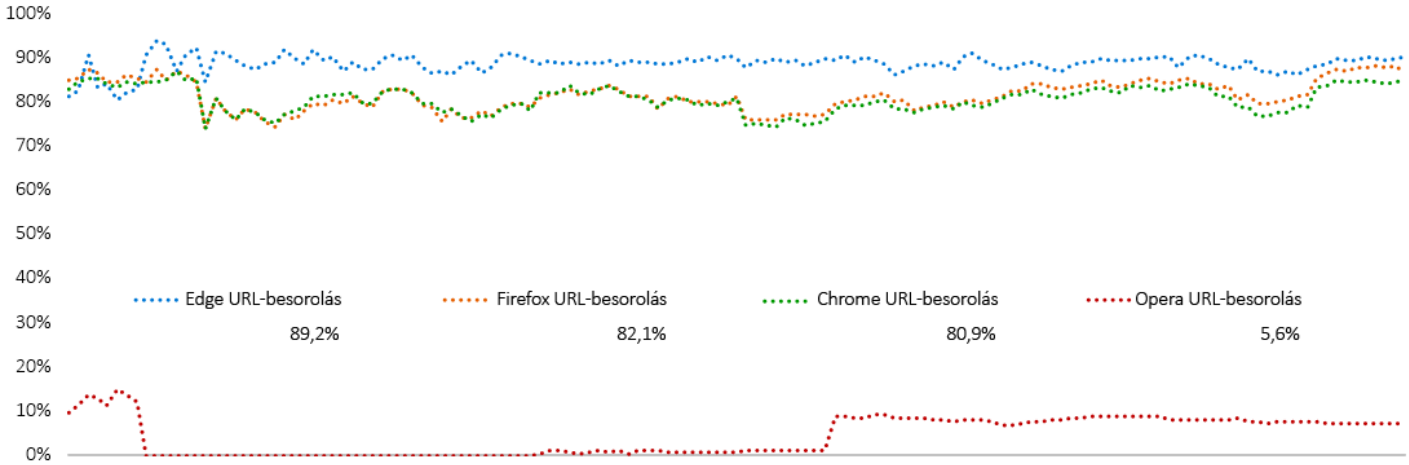
	< 24 óra	< 48 óra	< 72 óra	< 96 óra	< 120 óra	< 144 óra	< 168 óra	Összesen
Edge alkalmazásbesorolással	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Edge URL-besorolással	63,4%	84,5%	86,5%	87,3%	87,8%	88,1%	88,1%	88,1%
Chrome alkalmazásbesorolással	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Chrome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

A teszt során a Microsoft Edge 96,7%-os kezdeti védelmi arányt mutatott a rosszindulatú programok ellen. A Google Chrome és a Mozilla Firefox kezdeti védelmi aránya 86,2%, illetve 80,8% volt. Az Opera kezdeti védelmi aránya 6,8% volt. A tesztelés hetedik napjának végén mindegyik böngészőnél javulás volt tapasztalható. A Microsoft Edge 4,5%-os javulással 98,2%-ot ért el. A Google Chrome esetében 6,7% javulással 92,9%-ra növekedett a védelem, a Mozilla Firefox esetében 8,4%-os javulással 89,2%-ra, az Opera esetében pedig 0,1%-os javulással 6,9%-ra.

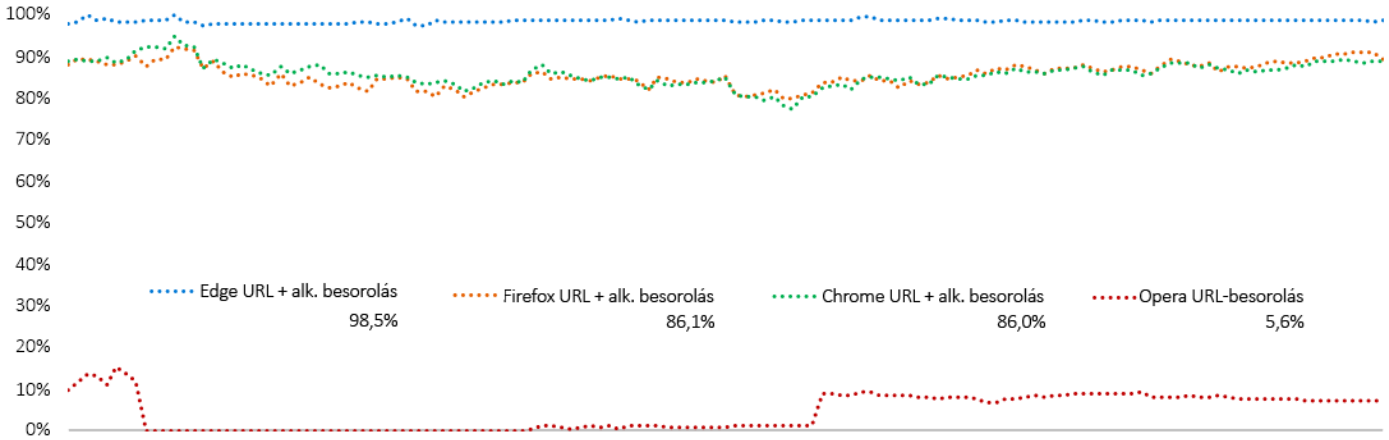
A védelem konzisztenciájának időbeli alakulása

A teszt során folyamatosan bővítettük az új rosszindulatú programok körét. A már nem elérhető vagy rosszindulatú programot tartalmazó URL-eket, fájlokat és alkalmazásokat eltávolítottuk. Minden adatpont kiszámítása egy meghatározott időpillanatban rögzített mérések alapján történt. Ha a rosszindulatú program blokkolása korán megtörtént, nő a böngésző pontszáma a védelem időbeli konzisztenciájának terén. Ha a böngésző nem blokkolta a rosszindulatú programot, akkor a pontszám csökken.

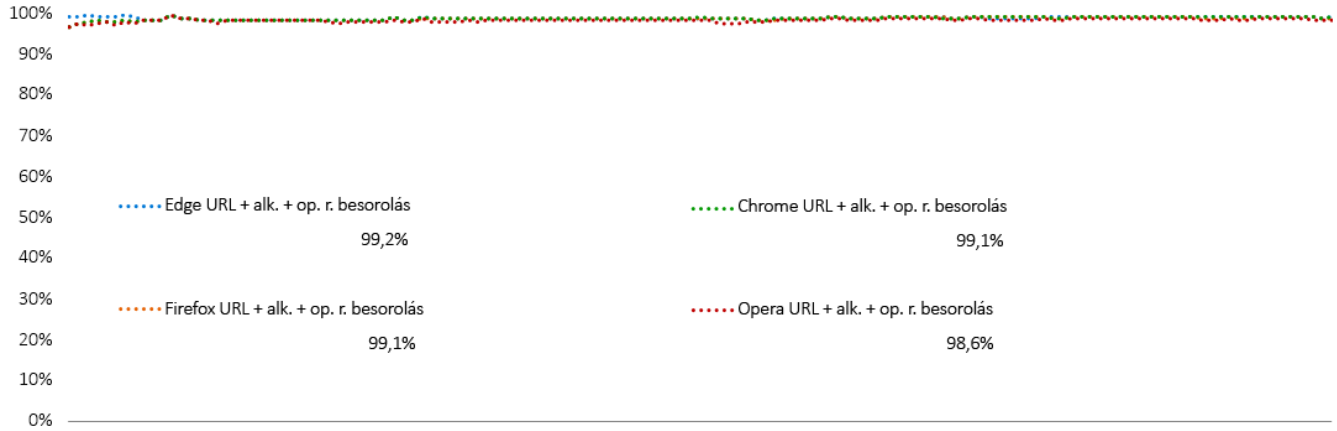
A tesztelés a védelem három rétegét fedte fel: URL-besorolás, alkalmazásbesorolás a böngészőben, valamint az operációs rendszer alkalmazásbesorolása. Az URL-besorolás megfelelően jó védelmet nyújtott.



Az alkalmazásbesorolás rétege megerősítette a védelmet.



Az operációs rendszer általi besorolás még tovább fokozta a védelmet. Ideális esetben a böngésző blokkolja a rosszindulatú programokat, így azok soha nem jutnak el az operációs rendszerig. A tesztelés azonban kimutatta, hogy az operációs rendszer általi besorolás nagyon hatékony volt.



Tesztkörnyezet

- BaitNET™ (NSS Labs saját szoftvere)
- 64 bites Microsoft Windows 10 Pro (verzió: 1909, build: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (kernel kiadása: 4.19.0-kali5-amd64)
- VMware vCenter (verzió: 6.7u2, build: 6.7.0.30000)
- VMware vSphere (verzió: 6.7.0.20000)
- VMware ESXi (verzió: 6.7u3, build 14320388)
- VMware Tools 10.3.5
- Wireshark 2.6.3-as verzió
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (283-as build)
- GNU Wget 1.19.4
- Curl 7.58.0

Tesztelt termékek

- Google Chrome: 81.0.4044.113-as verziótól 81.0.4044.138-as verzióig
- Microsoft Edge: 83.0.478.10-s verziótól 84.0.516.1-es verzióig
- Mozilla Firefox: 75.0-s verziótól 76.0.1-es verzióig
- Opera: Verzió: 67.0.3575.137-től 68.0.3618.125-ig

Szerzők

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Tesztelési módszer

Az NSS Labs Web Browser Security (WBS) Test Methodology v4.0 a következő webhelyen érhető el: www.nsslabs.com.

Elérhetőségi adatok

NSS Labs, Inc.

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746

info@nsslabs.com

www.nsslabs.com