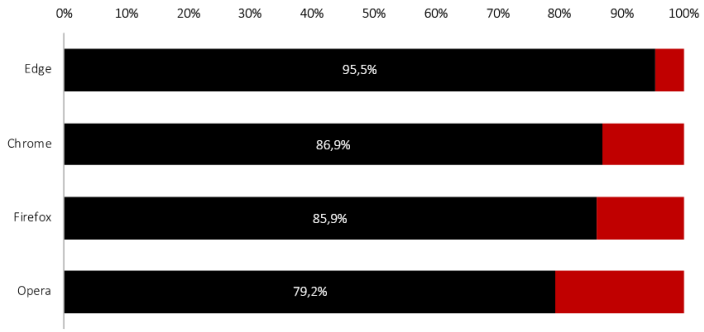
2020 második negyedéve JELENTÉS AZ ÖSSZEHASONLÍTÓ TESZTRŐL

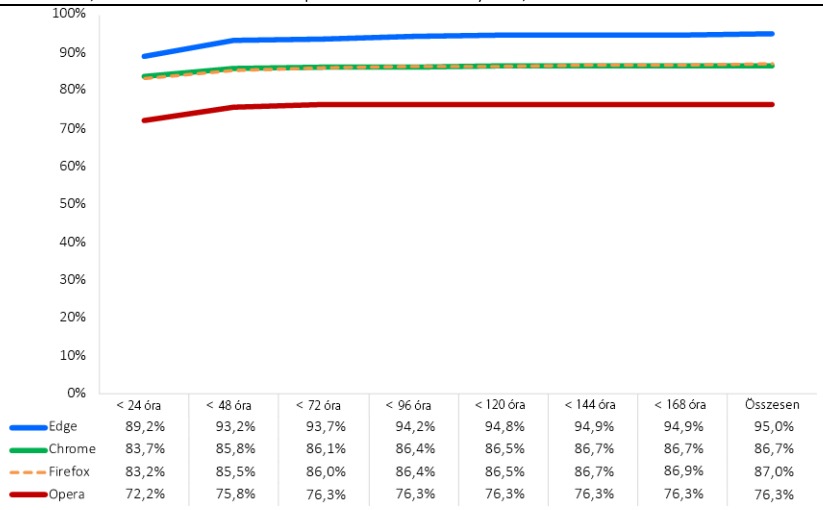
Áttekintés

2020 második negyedévében az NSS Labs független tesztelésnek vetette alá a böngészők által az adathalászat ellen kínált védelmet: 47274 különálló tesztet végzett (böngészőnként) 2443 különböző adathalászati URL használatával 18 napon keresztül. Az adathalászat 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 harmadik felek tiltólistáinak kombinációját használja.

A Microsoft Edge nyújtotta a legnagyobb védelmet, az adathalászati URL-ek 95,5%-át blokkolta, emellett a legmagasabb azonnali védelmi arányt (89,2%) biztosította. A Google Chrome nyújtotta a második legnagyobb védelmet, átlagosan 86,9%-ot blokkolt, ezt követte a Mozilla Firefox 85,9%-os blokkolással. Az Opera blokkolási aránya 79,2% volt.



Az eredmények összefoglalása

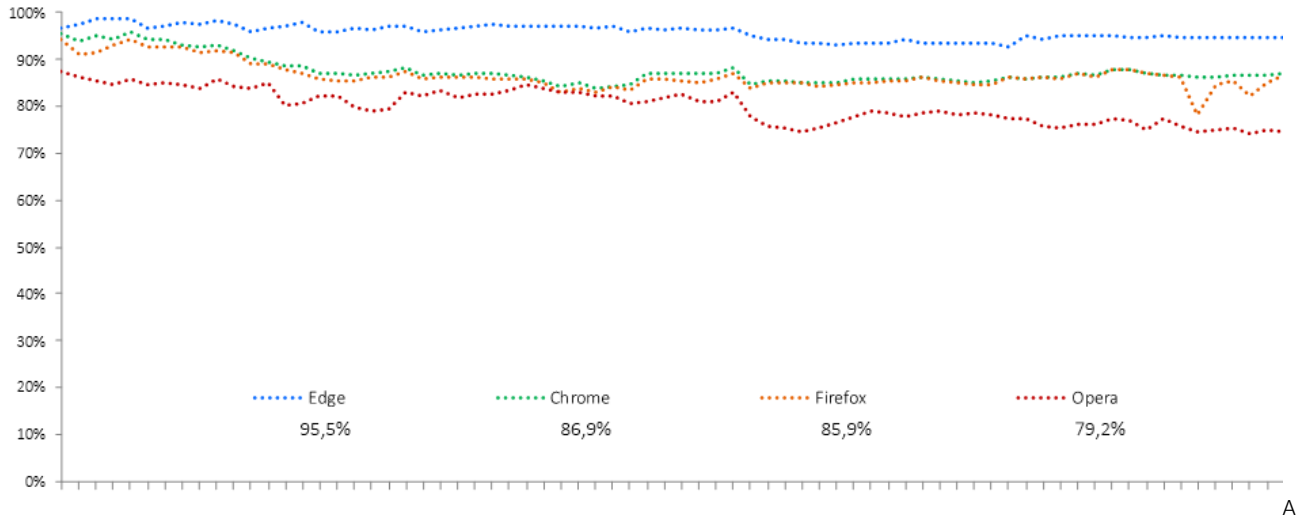


	< 24 óra	< 48 óra	< 72 óra	< 96 óra	< 120 óra	< 144 óra	< 168 óra	Összesen
Edge	89,2%	93,2%	93,7%	94,2%	94,8%	94,9%	94,9%	95,0%
Chrome	83,7%	85,8%	86,1%	86,4%	86,5%	86,7%	86,7%	86,7%
Firefox	83,2%	85,5%	86,0%	86,4%	86,5%	86,7%	86,9%	87,0%
Opera	72,2%	75,8%	76,3%	76,3%	76,3%	76,3%	76,3%	76,3%

Az URL-besorolási rendszerek úgy rövidítik le azt az időt, amely alatt a támadók elérhetik a céljukat, hogy figyelmeztetik a felhasználókat, hogy az adott URL egy ismert adathalászati célú webhely. Mivel azonban a felhasználók számos különböző webhelyet keresnek fel, amelyek között sok új is van, az URL-besorolási rendszerek nem blokkolhatják egyszerűen az összes új URL-t. Ennek ismeretében a támadók folyamatosan változtatják az adathalászati célú kampányokat, és az összes támadás többsége a kampány elindításának első néhány órájában történik.

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

Az adathalászat elleni védelem időbeli alakulása



A teszt során naponta adtunk hozzá új adathalászati URL-eket, és a már nem elérhető vagy az adathalászati támadásokat már nem indító URL-eket eltávolítottuk. Minden adatpont egy meghatározott időpillanatban rögzített védelmet jelent. Ha az URL blokkolása korán megtörtént, nő a böngésző pontszáma a védelem időbeli konzisztenciájának terén. Ha a böngésző nem blokkolta az URL-t, akkor a pontszám csökken.

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

Háttér

Az adathalászat a megtévesztésen alapuló támadások olyan típusa, amely megpróbálja rávenni az áldozatot arra, hogy megadja a bizalmas személyes adatait a támadónak. Az ilyen bizalmas adatok közé tartoznak például a bankkártyaszámok, a társadalombiztosítási azonosítók, a bankszámlák bejelentkezési adatai és jelszavai. Az e-mailek, az azonnali üzenetek, az SMS-ek és a közösségi hálózatok webhelyein található hivatkozások mind célpontok lehetnek az adathalászati célú támadásoknál. Az adathalászati célú webhelyek kezdőoldala gyakran megkísérli a háttérben kiaknázni a látogatók számítógépeinek biztonsági réseit, és megpróbál rosszindulatú szoftvert telepíteni (ez az ún. „drive-by exploit”).

Az adathalászati célú támadások komoly kockázatot jelentenek a személyekre és a szervezetekre, és fenyegetéssel próbálják megszerezni a bizalmas személyes és vállalati adatokat. Az Anti-Phishing Working Group (APWG) összesen 165772 különböző e-mailes adathalászati kampányról tett jelentést 2020 első negyedévében.[1] Az adathalászati támadások egyre komplexebbek és bonyolultabbak, ami megnehezíti az észlelésüket és a megakadályozásukat.

A böngészők által az adathalászat ellen nyújtott védelem

Az adathalászat elleni védelmet egy alkalmazás biztosítja a böngészőn belül, amely lekéri az URL-ek besorolását a felhőben található besorolási kiszolgálóról. A besorolási kiszolgáló adathalászati célú webhelyeket keres az interneten, majd pontszámot rendel minden ilyen URL-hez, és tiltólistára helyezi azokat. Így amikor a felhasználó a böngészőben felkeres egy URL-t, a böngésző adathalászat elleni védelme (például a Safe Browsing, a SmartScreen stb.) lekéri az URL besorolását a felhőalapú besorolási kiszolgálóról, és ha az eredmény az, hogy a webhely „rossz”, akkor a böngésző átirányítja a felhasználót egy figyelmeztető üzenetre, amely tájékoztatja arról, hogy az URL rosszindulatú. Néhány besorolási rendszer magyarázó jellegű tartalmat is biztosít. Ha azonban egy webhely „jónak” lett minősítve, a böngésző nem hajt végre semmilyen műveletet, és felhasználó nem fog tudni arról, hogy a böngésző biztonsági ellenőrzést hajtott végre.

A teszt összetétele – adathalászati URL-ek

Az ebben a jelentésben található adatok egy 18 napos időszakra vonatkoznak, 2020. április 21. és 2020. május 8., péntek között. A tesztelés az NSS tesztlaborjában történt, a texasi Austinban. A teszt során a NSS mérnökei rutinszerűen figyelték a csatlakozásokat annak biztosításához, hogy a tesztelt böngésző hozzáférhessen az adathalászati URL-ekhez, valamint a felhőbeli besorolási rendszerhez is.

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

A tesztelt rosszindulatú URL-ek száma

Összesen 4020 nyers, nem érvényesített URL-t teszteltek többször minden böngészőben, összesen 222527 különálló tesztet hajtottak végre megszakítás nélkül 430 órán keresztül (6 óránként 18 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 2443 különböző, érvényes adathalászati URL szerepelt 189096 különálló, érvényes tesztben (böngészőnként 47274), ami 2 százaléknál kisebb (<2%) hibahatárt eredményezett 95%-os megbízhatósági szinttel.

A naponta hozzáadott rosszindulatú URL-ek száma

Átlagosan 136 új, ellenőrzött URL volt hozzáadva a tesztkészlethez naponta. Bizonyos napokon más volt a szám, mivel változó volt a rosszindulatú tevékenységek szintje.

Az adathalászati URL-ek blokkolása

Az NSS azt mérte fel, hogy a böngészők milyen mértékben képesek blokkolni a rosszindulatú URL-eket, amint azokat megtaláljuk az interneten. A mérnökök határónként ismételték ezeket a teszteket, hogy megállapítsák, mennyi időbe telik a gyártóknak a védelem biztosítása, ha egyáltalán alkalmaznak védelmet.

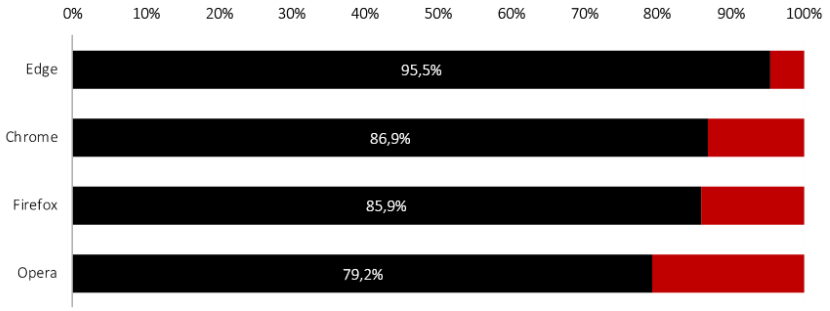
A Chromium-alapú új Microsoft Edge 2020. január 15-én jelent meg. Kompatibilis a Windows összes támogatott verziójával és a macOS rendszerrel. A böngésző letöltésével lecserélhető a Microsoft Edge korábbi verziója a Windows 10-es számítógépeken.

https://support.microsoft.com/hu-hu/help/4501095/download-the-new-microsoft-edge-based-on-chromium

[1] APWG-jelentés az adathalászati tevékenység trendjeiről

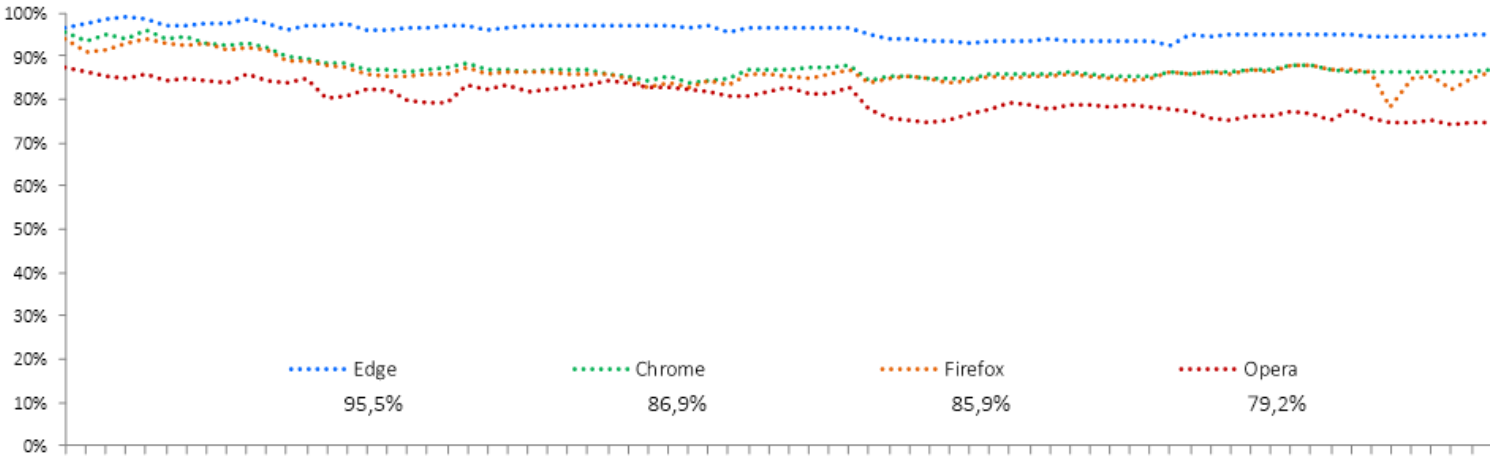
Az adathalászat blokkolási aránya

A Google Chrome és a Mozilla Firefox a Google Safe Browsing API-t használja. 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,[2] a PhishTank[3] és a Metamask[4] tiltólistáinak kombinációját használja, valamint a Yandex rosszindulatú programokra vonatkozó tiltólistáját.[5]
Az a képesség, hogy figyelmeztetni tudják a potenciális áldozatokat a rosszindulatú webhelyek felkeresésekor, kivételes helyzetbe emeli a böngészőket az adathalászati és egyéb rosszindulatú tevékenységek elleni küzdelemben. Mivel az adathalászati célú webhelyek rövid élettartamúak, lényeges, hogy a webhely felderítése, ellenőrzése, besorolása és a besorolási rendszerbe való felvétele a lehető leggyorsabban történjen. Ez magyarázza a blokkoláshoz szükséges átlagos idő és az elkapási arány közötti korrelációt. Ezért 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 adathalászati célú webhelyet sikerül blokkolni az észlelés utáni első 24 órában, mint azután.



Folyamatosan mértük mindegyik böngésző blokkolási teljesítményét, és rögzítettük a böngésző által tesztelt összes URL teljes blokkolási arányát. A böngésző teljes blokkolási arányának kiszámításához a sikeres blokkolások számát el kell osztani a tesztesetek számával. Például a 6 óránként végrehajtott tesztek esetében egy 48 órán keresztül online állapotú URL tesztelése 8-szor történik meg. Ha a böngésző 6 teszt alkalmával blokkolja (a maximális 8 alkalom közül), akkor a blokkolási aránya 75% lesz.

A védelem konzisztenciájának időbeli alakulása



A teszt során naponta adtunk hozzá új adathalászati URL-eket, és a már nem elérhető vagy az adathalászati támadásokat már nem indító URL-eket eltávolítottuk. Minden adatpont egy meghatározott időpillanatban rögzített védelmet jelent. Ha az URL blokkolása korán megtörtént, nő a böngésző pontszáma a védelem időbeli konzisztenciájának terén. Ha a böngésző nem blokkolta az URL-t, akkor a pontszám csökken.

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

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

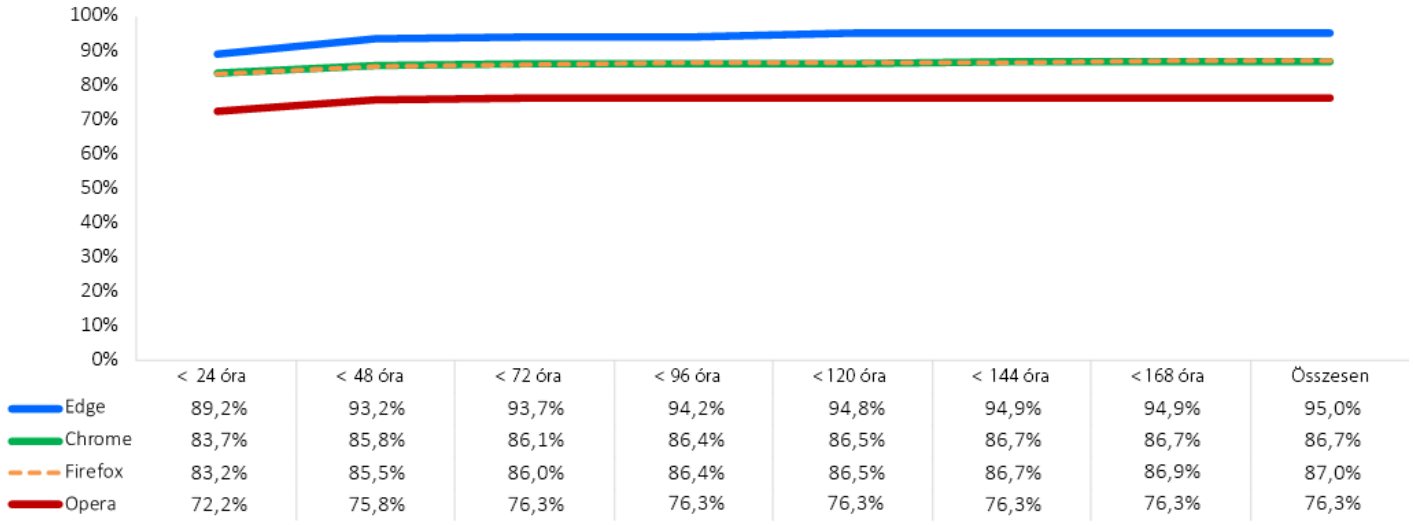
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

Az adathalászat elleni védelem hisztogramja

Az új adathalászati URL-ek elleni azonnali védelem kritikus fontosságú. Az adathalászati célú 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 az adathalászati célú webhelyek blokkolása, miután a minta bekerült a tesztciklusba. A hétnapos időablakon belül összesített védelmi arányokat számítottunk minden nap, amíg meg nem történt a fenyegetések blokkolása.

A teszt során a Microsoft Edge 89,2%-os kezdeti védelmi arányt mutatott az adathalászati célú támadások ellen. A Google Chrome és a Mozilla Firefox kezdeti védelmi aránya 83,7%, illetve 83,2% volt. Az Opera kezdeti védelmi aránya 72,2% volt. A tesztelés hetedik napjának végén mindegyik böngészőnél javulás volt tapasztalható. A Microsoft Edge 5,7%-os javulással 94,9%-ot ért el. A Mozilla Firefox 3,7%-os javulással 86,9%-ot, a Google Chrome 3%-os javulással 86,7%-ot ért el. Az Opera 4,1%-os javulással 76,3%-ot ért el.



	< 24 óra	< 48 óra	< 72 óra	< 96 óra	< 120 óra	< 144 óra	< 168 óra	Összesen
Edge	89,2%	93,2%	93,7%	94,2%	94,8%	94,9%	94,9%	95,0%
Chrome	83,7%	85,8%	86,1%	86,4%	86,5%	86,7%	86,7%	86,7%
Firefox	83,2%	85,5%	86,0%	86,4%	86,5%	86,7%	86,9%	87,0%
Opera	72,2%	75,8%	76,3%	76,3%	76,3%	76,3%	76,3%	76,3%

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 84.0.502.0-s 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