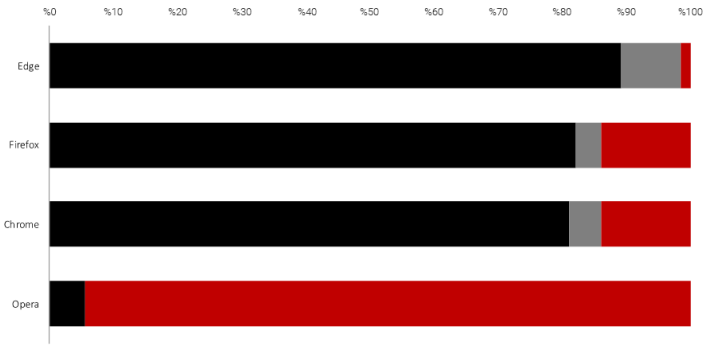
2020 2. Çeyrek KARŞILAŞTIRMALI TEST RAPORU

Genel Bakış

2020'nin 2. Çeyreğinde NSS Labs, web tarayıcılarının sunduğu kötü amaçlı yazılım koruması hakkında bağımsız bir test yürütmüştür: 34 gün boyunca 1.065 tekil örnek kullanılarak 32.267 ayrı test (her web tarayıcısı için) yapılmıştır. Kötü amaçlı yazılımlardan koruma için Microsoft Edge'in kullandığı çözüm Microsoft Defender SmartScreen, Google Chrome ve Mozilla Firefox'un kullandığı çözüm Google Safe Browsing API, Opera'nın kullandığı çözüm ise Yandex'tir.

En fazla korumayı, kötü amaçlı yazılımların %98,5'ini engelleyen ve en yüksek sıfırıncı saat koruma oranına (%96,7) ulaşan Microsoft Edge sunmuştur. İkinci en fazla korumayı ortalama %86,1 engelleme oranıyla Firefox sağlamıştır ve ardından da %86,0 engelleme oranıyla Google Chrome gelmektedir. Opera'nın engelleme oranı %5,6 olmuştur.



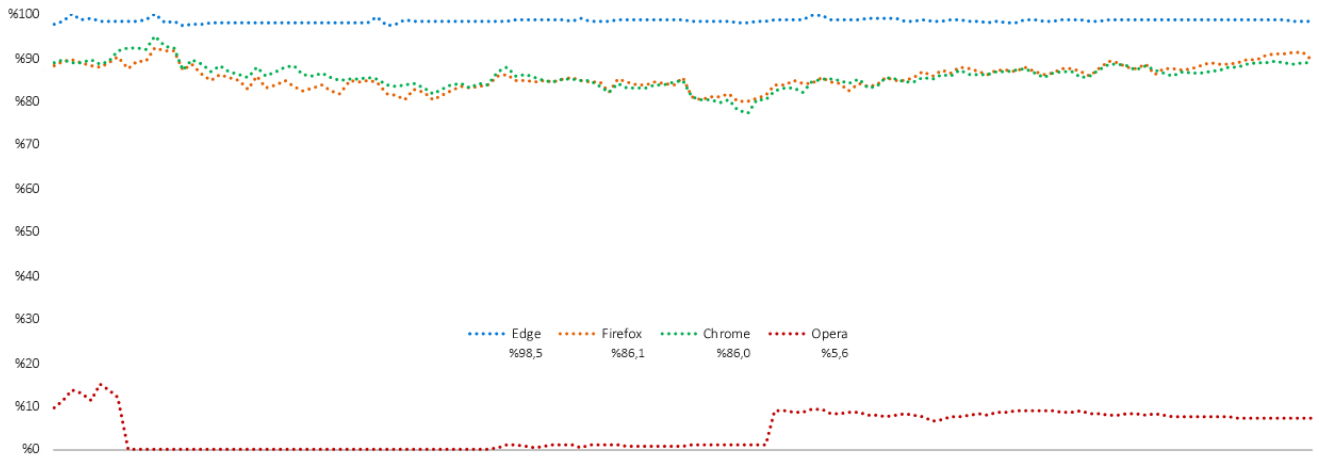
Sonuçların Özeti

	< 24 Saat	< 48 Saat	< 72 Saat	< 96 Saat	< 120 Saat	< 144 Saat	< 168 Saat	Toplam
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

Saygınlık sistemleri, tehlikeli bir URL'yi, dosyayı veya uygulamayı engelleyerek ya da kullanıcıyı bu tehlike hakkında uyararak saldırganların hedeflerine ulaşmak için sahip olduğu süreyi kısaltır. Ancak kullanıcılar sürekli olarak yeni web sayfalarını ziyaret eder, dosyalar indirir ve uygulamalar yükler. Saygınlık sistemlerinin tüm yeni şeyleri engellemesi imkansızdır. Bunu bilen saldırganlar, kötü amaçlı yazılım harekatlarında sürekli olarak değişiklikler yapar. Bu nedenle saldırıların büyük bir bölümü, harekatın başlamasını izleyen birkaç saat içinde gerçekleşir. Dolayısıyla, içeriklerin hızlı bir şekilde başarıyla sınıflandırılması, başarılı koruma açısından kilit öneme sahiptir.

NSS Labs, tarayıcıların internette ilk tespit ettiğimiz anda kötü amaçlı yazılımları engelleme kabiliyetlerini değerlendirmeye tabi tutmuştur. Sağlayıcıların koruma ekleyip eklemediğini ve ekleyenlerin ne kadar hızlı koruma eklediğini belirlemek için kötü amaçlı URL'leri, dosyaları ve uygulamaları her altı saatte bir test etmeye devam ettik.

Zaman İçinde Kötü Amaçlı Yazılım Koruması



Test boyunca sürekli olarak yeni kötü amaçlı yazılımlar eklenmiştir. Bir noktadan sonra erişilemeyen veya kötü amaçlı yazılım barındırmayan URL'ler, dosyalar ve uygulamalar kaldırılmıştır. Her veri noktası, belirli bir anda kaydedilen ölçümlerden hesaplanmıştır. Kötü amaçlı yazılım ilk anlarda engellendiyse, tarayıcının zaman içinde koruma sürekliliği skoru artırılmıştır. Aynı şekilde, tarayıcı kötü amaçlı yazılımı engellemediyse bu skor düşürülmüştür.

Testler, Web Tarayıcısı Test Metodolojisi v4.0 (www.nsslabs.com adresinden erişilebilir) sürümüne dayalı olarak yapılmıştır.

Arka Plan

Sosyal mühendislik içeren kötü amaçlı yazılım (SEM) saldırıları, kullanıcıları kötü amaçlı yazılımları indirmeye teşvik etmek için sosyal medyayı, ele geçirilen e-posta hesaplarını, sahte bilgisayar sorunu bildirimlerini ve diğer aldatıcı öğeleri dinamik şekilde bir araya getirir. Siber suçlular, insanların rehberlerindeki kişilere duyduğu güveni istismar etmek ve kurbanları kandırarak kötü amaçlı dosya bağlantılarının güvenli olduğuna inandırmak için ele geçirilmiş e-posta hesaplarını kullanır. Ele geçirilmiş sosyal medya hesapları da ele geçirilmiş e-posta hesaplarıyla aynı şekilde kullanılır. Ancak sosyal medyada çember daha da genişler. Kişinin arkadaşları ve hatta arkadaşlarının arkadaşları, aldatılma riskiyle karşı karşıya kalır.

Sosyal mühendislik taktiklerinde, örneğin kullanıcılara Adobe Flash Player'ın yüklenmesi gerektiğini, bilgisayarlarına virüs bulaştığını ya da bir yazılımın güncelleştirilmesi gerektiğini belirten açılır pencereler kullanılabilir. Kötü amaçlı yazılım yüklendiği andan itibaren kurbanlar kimlik hırsızlığına, banka hesaplarının ele geçirilmesine ve son derece yıkıcı olabilecek daha pek çok meseleye karşı savunmasız hale gelir.

Web Tarayıcılarının Sunduğu Kötü Amaçlı Yazılım Koruması

Tarayıcılar, kötü amaçlı yazılım koruması sağlamak amacıyla, interneti etraflıca tarayıp kötü amaçlı web siteleri bulan ve ardından içerikleri engellenenler veya izin verilenler listelerine ekleyerek ya da içeriğe bir skor atayarak (sağlayıcının yaklaşımına bağlıdır) sınıflandıran, bulut tabanlı saygınlık sistemleri kullanır.

Bu sınıflandırma teknikleri, manuel veya otomatik yöntemlerle uygulanabilir. Kötü amaçlı yazılım korumasının ikinci işlevsel bileşeni kapsamında web tarayıcısı, bulut tabanlı saygınlık sistemlerinden belirli URL'ler, dosyalar veya uygulamalar hakkında saygınlık bilgileri ister ve ardından kötü amaçlı yazılımlara karşı uyarır veya bunları engeller.

Sonuçlar kötü amaçlı yazılım varlığına işaret ediyorsa, web tarayıcısı kullanıcıyı URL'nin, dosyanın veya uygulamanın kötü amaçlı olduğunu açıklayan bir uyarı mesajına yönlendirir. Bazı saygınlık sistemlerinde ek eğitim içerikleri de yer alır. Öte yandan, içeriğin "iyi" olduğu belirlendiyse web tarayıcısı hiçbir eylemde bulunmaz. Kullanıcı, tarayıcı tarafından bir güvenlik kontrolü gerçekleştirildiğini fark etmez.

Google ve Firefox, hem URL saygınlığı hem de belirli dosya türlerinin indirilmesini önlemek veya bu tür dosyaları indiren kullanıcıları uyarmak için Google Safe Browsing API'yi kullanmaktadır. Microsoft Edge, kimlik avı ve kötü amaçlı yazılım tehditlerine karşı koruma sağlamak amacıyla, uygulama saygınlık hizmetini de içeren Microsoft Defender SmartScreen'i kullanmaktadır. Opera; Netcraft[1], PhishTank[2] ve Metamask[3] kaynaklı engellenenler listesi kombinasyonunun yanı sıra Yandex'in[4] kötü amaçlı yazılım engelleme listesini kullanmaktadır.

Buna ek olarak Microsoft Defender SmartScreen, Ekim 2017 Windows 10 güncelleştirmesiyle birlikte işletim sisteminin tamamını koruyan bir özellik olarak eklenmiştir. SmartScreen korumasının işletim sistemi sürümü, işletim sisteminin kötü amaçlı yazılımlara karşı sağladığı koruma kapsamında tüm tarayıcılar, e-posta istemcileri, USB ve diğer uygulamalar için bir destekleyici niteliğindedir. Dolayısıyla kullanıcılar tarayıcının URL korumasından, tarayıcının uygulama/dosya korumasından ve işletim sisteminin korumasından aynı anda yararlanabilmektedir.

Test Bileşenleri – Kötü Amaçlı Yazılım Örnekleri

Bu rapordaki veriler, 21 Nisan 2020 ile 25 Mayıs 2020 arasındaki 34 günlük test süresini kapsamaktadır. Tüm testler, Texas'ın Austin şehrindeki NSS test tesisinde yapılmıştır. Test sırasında NSS mühendisleri, test edilmekte olan tarayıcıların hem kötü amaçlı yazılımlara hem de buluttaki saygınlık hizmetlerine erişebildiğinden emin olmak için bağlantı durumunu rutin bir şekilde izlemiştir.

Örneklerin yeni olmasına odaklanıldığından, sürekli olarak yeni örnekler eklenmiş ve kaybolan örnekler testten çıkarılmıştır. Bu nedenle, en sonda saklanan test setindekilerden çok daha fazla sayıda örnek test edilmiştir.

Test Edilen Toplam Kötü Amaçlı Örnek Sayısı

Toplamda 1.844 adet ham ve doğrulanmamış örnek her bir web tarayıcısıyla birden fazla kez test edilmiş, 822 saatlik bir sürede (34 gün boyunca her 6 saatte bir) kesintisiz bir biçimde toplamda 182.676 ayrı test yapılmıştır. NSS mühendisleri, güvenlik açığı içerenler dahil olmak üzere (bu testin kapsamında değildir), doğrulama kriterlerini geçemeyen örnekleri kaldırmıştır. Sonuç olarak, birbirinden ayrı 129.068 adet doğrulanmış kötü amaçlı yazılım testi (tarayıcı başına 32.267) içerisinde tekil 1.065 adet doğrulanmış kötü amaçlı yazılım örneği yer almıştır. Bu rakamlar ışığında hata payı %2'nin altında (<%2), güvenilirlik ise %95'in üstündedir.

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

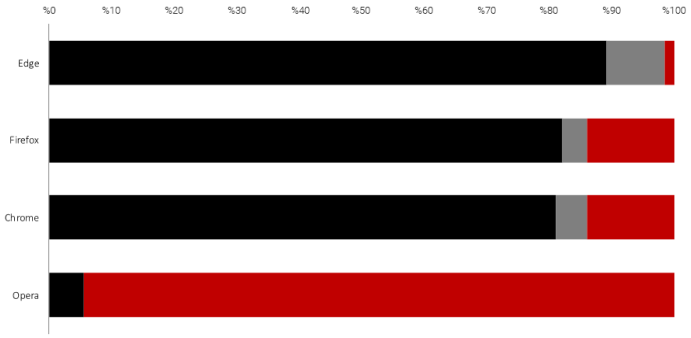
[2] http://www.phishtank.com/

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

[4] https://yandex.com

Kötü Amaçlı Yazılım Engelleme Oranı

Olası kurbanları kötü amaçlı bir web sitesine girebileceklerine dair uyarma kabiliyeti, web tarayıcılarına sosyal mühendislik içeren kötü amaçlı yazılımlarla mücadele konusunda benzersiz bir pozisyon kazandırır. Kötü amaçlı yazılım sitelerinin ömrü kısa olduğundan, sitenin mümkün olan en kısa sürede keşfedilmesi, doğrulanması, sınıflandırılması ve saygınlık sistemine eklenmesi büyük önem taşır. Bu nedenle, iyi bir saygınlık sisteminin yüksek yakalama oranlarına ulaşması için hem isabetli hem de hızlı olması gerekir. Tarayıcı geliştiricileri bu ilişkinin açıkça farkındadır. Algılamayı izleyen ilk 24 saat içerisinde, sonrasına kıyasla çok daha fazla kötü amaçlı yazılım engellenmektedir.



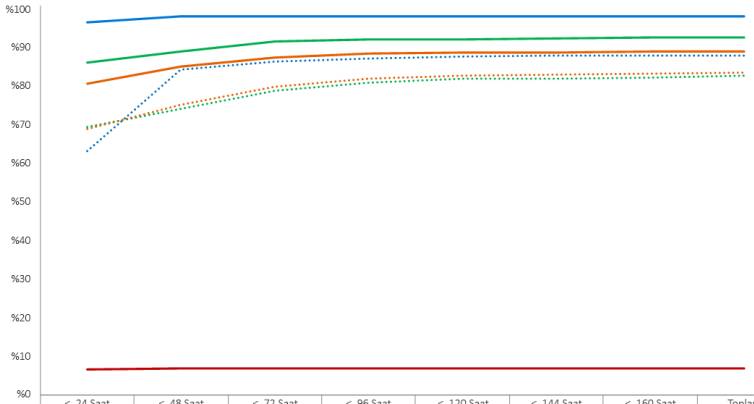
	Opera	Chrome	Firefox	Edge
URL Saygınlığı	%5,6	%80,9	%82,1	%89,2
URL + Uygulama Saygınlığı	%0,0	%5,0	%4,0	%9,3
URL + Uygulama + IS Saygınlığı	%93,1	%13,1	%13,0	%0,7
Kaçırılan	%1,4	%0,9	%0,9	%0,8

Edge'deki temel koruma teknolojisi olan SmartScreen, saldırılara karşı hem bulut tabanlı entegre URL saygınlığı hizmeti aracılığıyla URL tabanlı koruma hem de kötü amaçlı dosyaları engellemek için uygulama saygınlığı sistemi sağlamaktadır. Uygulama saygınlığıyla birlikte SmartScreen, Edge'de %98,5 engelleme oranına ulaşmıştır. Mozilla Firefox ve Google Chrome, Safe Browsing API'yi kullanmaktadır. Firefox, %86,1 engelleme oranı elde etmiştir. Google Chrome, %86,0 engelleme oranı elde etmiştir. Çeşitli kaynaklardan temin ettiği engellenenler listesi kombinasyonunu kullanan Opera, %5,6 engelleme oranı elde etmiştir.

Ayrıca bunları yürütmeye çalıştığımızda, Microsoft Defender SmartScreen, kötü amaçlı dosyaları engelleme oranlarını Opera için %93,1, Chrome için %13,1, Firefox için %13,0 ve Edge için %0,7 artırmıştır.

Kötü Amaçlı Yazılım Koruması Çubuk Grafiği

Yeni kötü amaçlı yazılımlara karşı anında koruma kabiliyeti kritik önem taşır. Kötü amaçlı yazılım barındırdığı keşfedilen siteler, genellikle kısa bir süre içerisinde erişime kapatılır. Koruma önlemlerini zamanında alamayan ürünler, tehditlere yeterince erken karşılık veremeyebilir. Çubuk grafikte, örnek test döngüsüne girdikten sonra her bir tarayıcının kötü amaçlı yazılımı engellemesi için geçen süre gösterilmektedir. Yedi günlük dönemde, kümülatif koruma oranları, tehditler engellenene kadar her gün hesaplanmıştır.



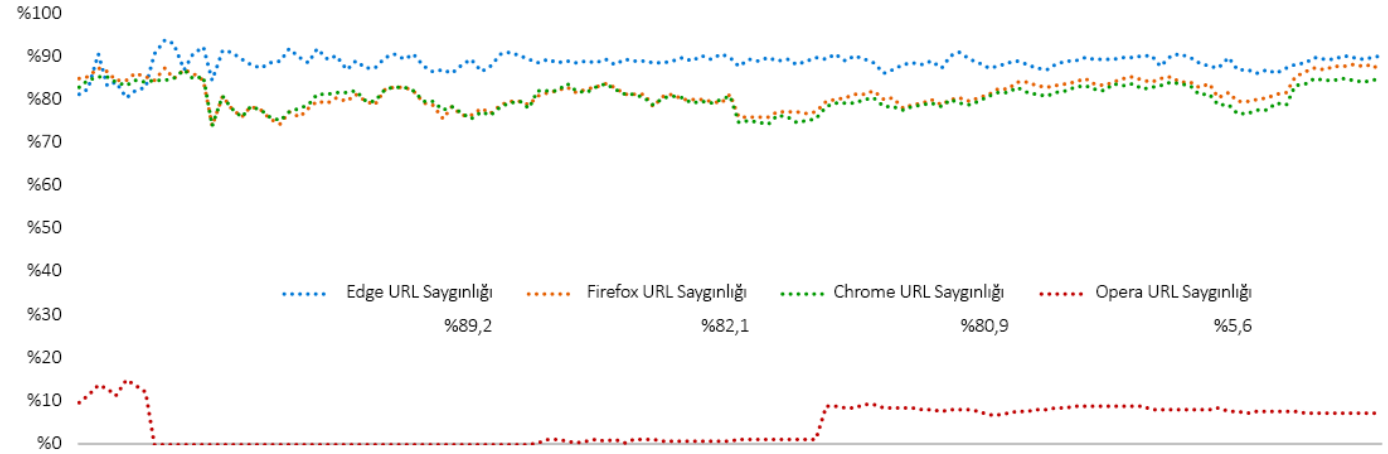
	< 24 Saat	< 48 Saat	< 72 Saat	< 96 Saat	< 120 Saat	< 144 Saat	< 160 Saat	Toplam
Uygulama Saygınlığıyla Edge	%96,7	%98,1	%98,1	%98,1	%98,2	%98,2	%98,2	%98,2
URL Saygınlığıyla Edge	%63,4	%84,5	%86,5	%87,3	%87,8	%88,1	%88,1	%88,1
Uygulama Saygınlığıyla Chrome	%86,2	%89,1	%91,7	%92,2	%92,3	%92,5	%92,7	%92,9
URL Saygınlığıyla Chrome	%69,7	%74,4	%79,0	%81,0	%82,0	%82,2	%82,4	%82,7
Uygulama Saygınlığıyla Firefox	%80,8	%85,2	%87,6	%88,5	%88,8	%88,9	%89,1	%89,2
URL Saygınlığıyla Firefox	%69,1	%75,3	%80,0	%82,1	%82,9	%83,0	%83,4	%83,6
URL Saygınlığıyla Opera	%6,8	%6,9	%6,9	%6,9	%6,9	%6,9	%6,9	%6,9

Test sırasında Microsoft Edge'in kötü amaçlı yazılımlara karşı ilk koruma oranı %96,7 olmuştur. Google Chrome ve Mozilla Firefox, sırasıyla %86,2 ve %80,8 ilk koruma oranlarına ulaşmıştır. Opera'nın ilk koruma oranı %6,8 olarak gerçekleşmiştir. Testlerin yedinci günü itibariyle, tüm web tarayıcılarının koruma oranı artmıştır. Microsoft Edge, %4,5 artışla %98,2'ye ulaşmıştır. Google Chrome %6,7 artışla %92,9'a, Mozilla Firefox %8,4 artışla %89,2'ye, Opera ise %0,1 artışla %6,9'a çıkmıştır.

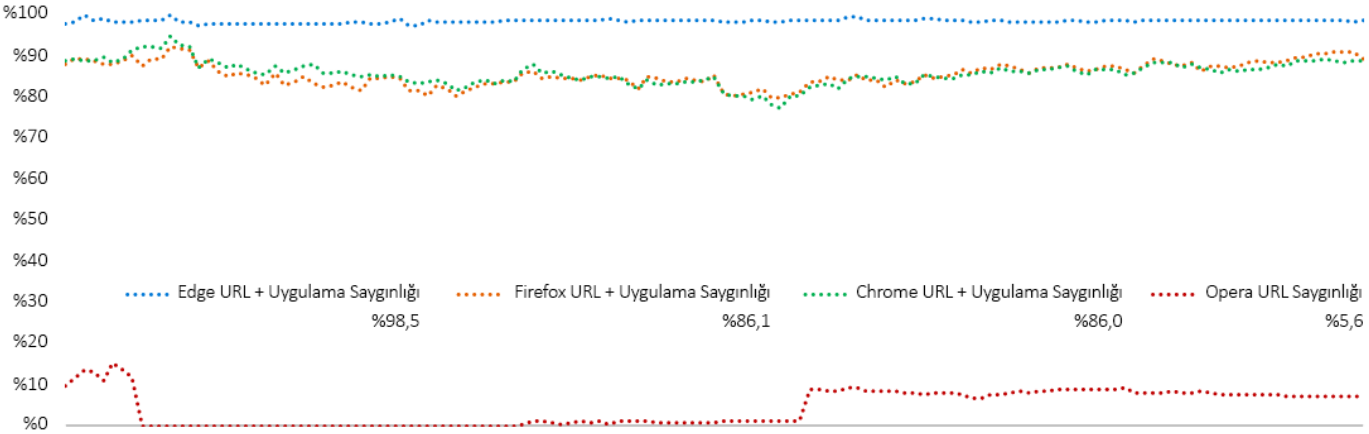
Zaman İçinde Koruma Sürekliliği

Test boyunca sürekli olarak yeni kötü amaçlı yazılımlar eklenmiştir. Bir noktadan sonra erişilemeyen veya kötü amaçlı yazılım barındırmayan URL'ler, dosyalar ve uygulamalar kaldırılmıştır. Her veri noktası, belirli bir anda kaydedilen ölçümlerden hesaplanmıştır. Kötü amaçlı yazılım ilk anlarda engellendiyse, tarayıcının zaman içinde koruma sürekliliği skoru artırılmıştır. Aynı şekilde, tarayıcı kötü amaçlı yazılımı engellemediyse bu skor düşürülmüştür.

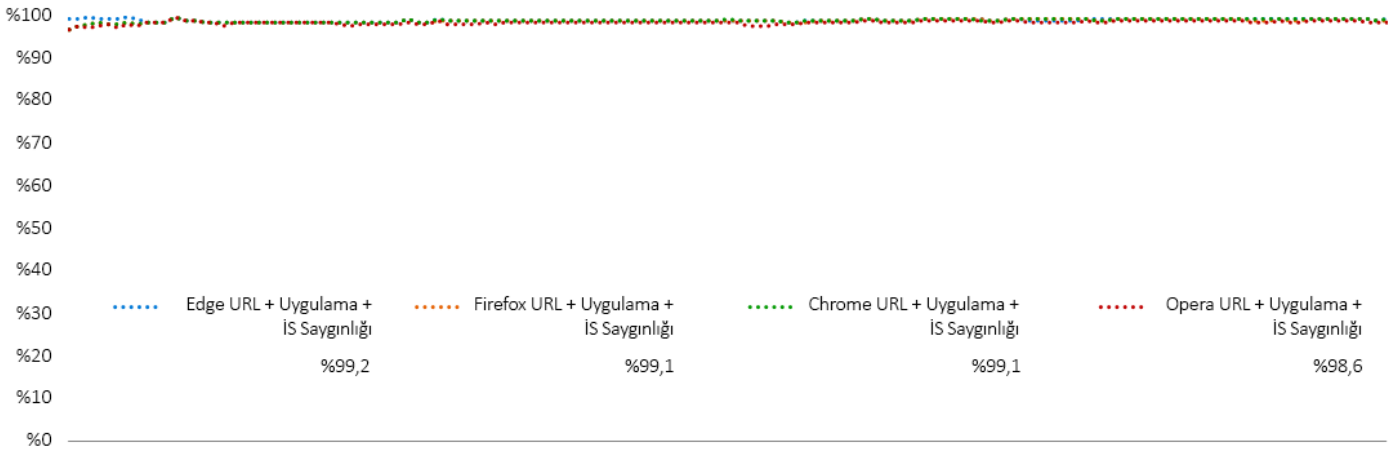
Yapılan testler, üç ayrı koruma katmanını ortaya çıkarmıştır: URL saygınlığı, tarayıcıdaki uygulama saygınlığı ve işletim sistemi uygulama saygınlığı. URL saygınlığı, makul ölçüde koruma sağlamıştır.



Uygulama saygınlığı katmanını eklemek, korumayı artırmıştır.



İşletim sistemi saygınlığı, koruma seviyesini bir kat daha artırmıştır. En ideal senaryo, kötü amaçlı yazılımın web tarayıcısı tarafından engellenmesi ve dolayısıyla işletim sistemine asla ulaşamamasıdır. Ancak yapılan testlerde, işletim sistemi saygınlığının oldukça etkili olduğu görülmüştür.



Test Ortamı

- BaitNET™ (NSS Labs Proprietary)
- 64-bit Microsoft Windows 10 Pro (sürüm 1909 Derleme: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (Kernel sürümü 4.19.0-kali5-amd64)
- VMware vCenter (Sürüm 6.7u2 Derleme 6.7.0.30000)
- VMware vSphere (Sürüm 6.7.0.20000)
- VMware ESXi (Sürüm 6.7u3 Derleme 14320388)
- VMware Tools 10.3.5
- Wireshark sürüm 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (Derleme 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Test Edilen Ürünler

- Google Chrome: Sürüm 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge: Sürüm 83.0.478.10 – 84.0.516.1
- Mozilla Firefox: Sürüm 75.0 – 76.0.1
- Opera: Sürüm: 67.0.3575.137 – 68.0.3618.125

Yazarlar

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Test Metodolojisi

NSS Labs Web Browser Security (WBS) Test Metodolojisi v4.0 sürümüne www.nsslabs.com adresinden erişilebilir.

İletişim Bilgileri

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com