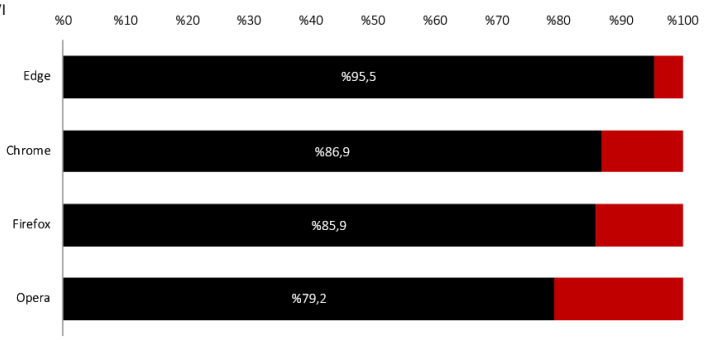
# 2020 2. Çeyrek KARŞILAŞTIRMALI TEST RAPORU

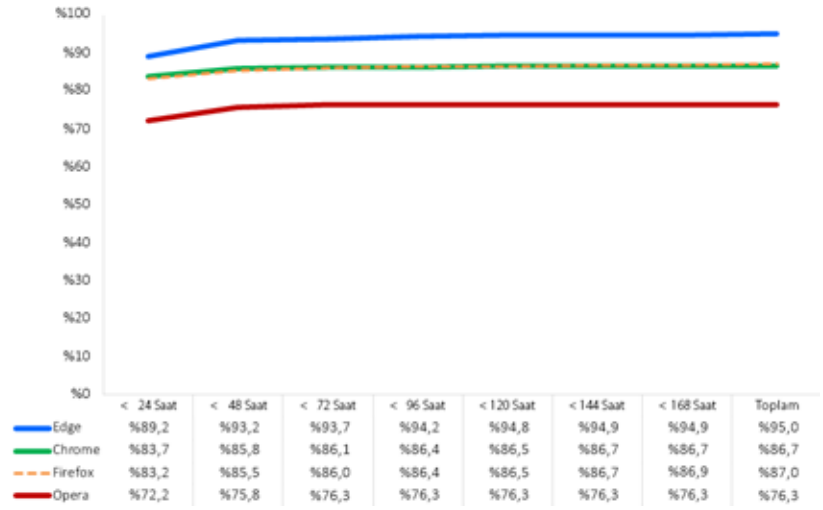
## Genel Bakış

2020'nin 2. Çeyreğinde NSS Labs, web tarayıcılarının sunduğu kimlik avı koruması hakkında bağımsız bir test yürütmüştür: 18 gün boyunca 2.443 tekil kimlik avı URL'si kullanılarak 47.274 ayrı test (her web tarayıcısı için) yapılmıştır. Kimlik avından 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 bir üçüncü taraf engellenenler listesi kombinasyonudur.

En fazla korumayı, kimlik avı URL'lerinin %95,5'ini engelleyen ve en yüksek sıfırıncı saat koruma oranına (%89,2) ulaşan Microsoft Edge sunmuştur. İkinci en fazla korumayı ortalama %86,9 engelleme oranıyla Google Chrome sağlamıştır ve ardından da %85,9 engelleme oranıyla Mozilla Firefox gelmektedir. Opera'nın engelleme oranı %79,2 olmuştur.




## Sonuçların Özeti

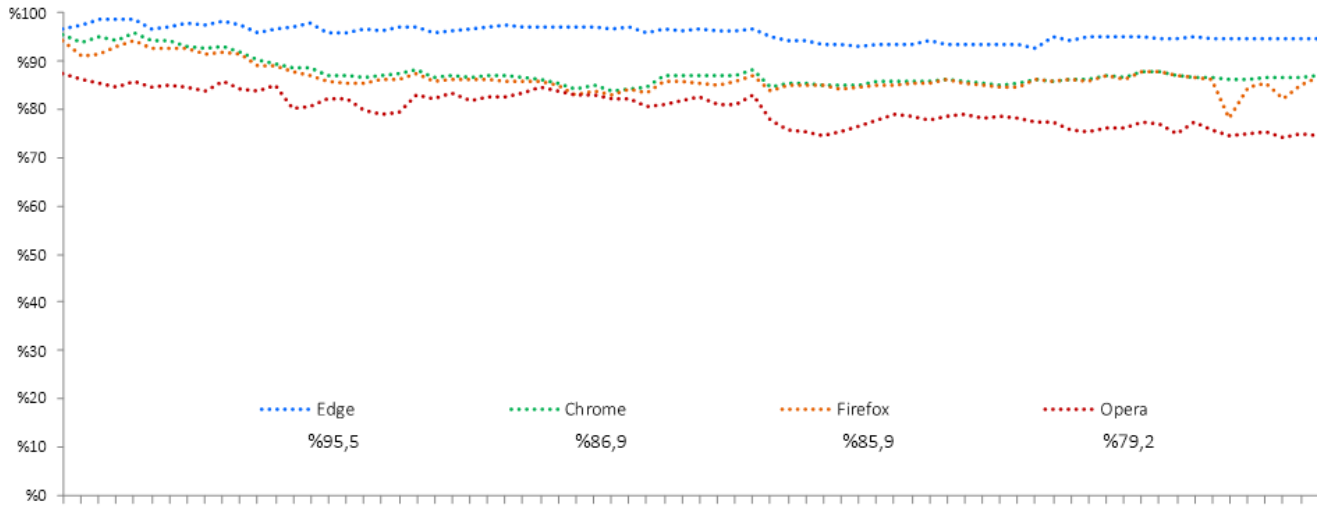



| | < 24 Saat | < 48 Saat | < 72 Saat | < 96 Saat | < 120 Saat | < 144 Saat | < 168 Saat | Toplam |
|---|---|---|---|---|---|---|---|---|
| Edge | %89,2 | %93,2 | %93,7 | %94,2 | %94,8 | %94,9 | %94,9 | %95,0 |
| Chrome | %83,7 | %85,8 | %86,1 | %86,4 | %86,5 | %86,7 | %86,7 | %86,7 |
| Firefox | %83,2 | %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 |

URL saygınlık sistemleri, bilinen bir kimlik avı URL'sini engelleyerek ya da kullanıcıyı bu kimlik avı hakkında uyararak saldırganların hedeflerine ulaşmak için sahip olduğu süreyi kısaltır. Ancak kullanıcılar birçoğu yeni olan çok çeşitli web sitelerini ziyaret ettiğinden, URL saygınlık sistemlerinin tüm yeni URL'leri engellemesi imkansızdır. Bunu bilen saldırganlar, kimlik avı harekatlarında sürekli olarak değişiklikler yapar. Bu nedenle saldırıların büyük bir bölümü, saldırının başlamasını izleyen birkaç saat içinde gerçekleşir.

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

Zaman İçinde Kimlik Avı Koruması




Test boyunca günlük olarak yeni kimlik avı URL'leri eklenmiştir. Bir noktadan sonra erişilemeyen veya kimlik avı saldırısında bulunmayan URL'ler kaldırılmıştır. Her veri noktası, belirli bir andaki korumayı temsil etmektedir. Bir URL ilk anlarda engellendiyse, tarayıcının zaman içinde koruma sürekliliği skoru artırılmıştır. Aynı şekilde, tarayıcı URL'yi engellemediyse bu skor düşürülmüştür.

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

# Arka Plan

Kimlik avı, bir kurbanı hassas kişisel bilgilerini saldırgana vermesi için ikna etme girişimi içeren bir çeşit sosyal mühendislik saldırısıdır. Kredi kartı numaraları, sosyal güvenlik numaraları ve banka hesaplarının oturum açma bilgileri ile parolaları, hassas bilgilere örnek olarak verilebilir. E-posta, anlık mesajlar, SMS mesajları ve sosyal medya sitelerindeki bağlantılar, kimlik avı saldırılarının vektörlerinden bazılarıdır. Bir kimlik avı internet sitesinin açılış sayfası genellikle bir ziyaretçinin bilgisayarındaki açıklardan sessizce yararlanmaya ve kötü amaçlı yazılımlar indirmeye de çalışır.

Hassas kişisel ve kurumsal bilgileri tehlikeye atma veya ele geçirme tehdidi teşkil eden kimlik avı saldırıları, hem bireyler hem de kuruluşlar için ciddi bir risktir. Anti-Phishing Working Group (APWG), 2020 yılının birinci çeyreğinde toplam 165.772 tekil e-posta kimlik avı harekatı yapıldığını raporlamıştır.[1] Kimlik avı saldırıları her geçen gün daha da karmaşık ve detaylı hale geldiğinden, algılanmaları ve önlenmeleri de gittikçe daha da zorlaşmaktadır.

## Web Tarayıcılarının Sunduğu Kimlik Avı Koruması

Kimlik avı koruması, web tarayıcısı içerisinde çalışan ve buluttaki bir saygınlık sunucusundan URL'nin saygınlığı hakkında bilgi isteyen bir uygulama tarafından sağlanır. Saygınlık sunucusu, kimlik avı web siteleri bulmak için interneti etraflıca tarar, ardından her URL'ye bir skor atar ve URL'yi bir engellenenler listesine ekler. Bu sayede, bir web tarayıcısı herhangi bir URL'yi ziyaret etme talimatı aldığında, tarayıcının kimlik avı koruması (Safe Browsing, SmartScreen vb.) bulut tabanlı saygınlık sunucusundan URL'nin saygınlık bilgisini ister. Sonuçlar bir web sitesinin "kötü" olduğunu gösterirse, web tarayıcısı kullanıcıyı URL'nin kötü amaçlı olduğunu açıklayan bir uyarı mesajına yönlendirir. Bazı saygınlık sistemlerinde ek eğitim içerikleri de yer alır. Öte yandan, web sitesinin "iyi" olduğu belirlendiyse web tarayıcısı hiçbir eylemde bulunmaz. Kullanıcı, tarayıcı tarafından bir güvenlik kontrolü gerçekleştirildiğini fark etmez.

## Test Bileşenleri – Kimlik Avı URL'leri

Bu rapordaki veriler, 21 Nisan 2020 ile 8 Mayıs 2020 Cuma arasındaki 18 günlük test süresini kapsamaktadır. Tüm testler, Texas'ın Austin şehrindeki NSS test tesisinde yapılmıştır. Test sırasında NSS mühendisleri, test edilmekte olan tarayıcıların hem kimlik avı URL'lerine hem de buluttaki tarayıcı saygınlık hizmetlerine erişebildiğinden emin olmak için bağlantı durumunu rutin bir şekilde izlemiştir.

Sitelerin yeni olmasına odaklanıldığından, sürekli olarak yeni URL'ler eklenmiş ve kaybolan siteler testten çıkarılmıştır. Bu nedenle, en sonda saklanan test setindekilerden çok daha fazla sayıda site test edilmiştir.

## Testteki Toplam Kötü Amaçlı URL Sayısı

Toplamda 4.020 adet ham ve doğrulanmamış URL her bir web tarayıcısıyla birden fazla kez test edilmiş, 430 saatlik bir sürede (18 gün boyunca her 6 saatte bir) kesintisiz bir biçimde toplamda 222.527 ayrı test yapılmıştır. NSS mühendisleri, güvenlik açığı içerenler dahil olmak üzere (bu testin kapsamında değildir), doğrulama kriterlerini geçemeyen örnekleri kaldırmıştır. Sonuç olarak, birbirinden ayrı 189.096 adet doğrulanmış kimlik avı testi (tarayıcı başına 47.274) içerisinde tekil 2.443 adet doğrulanmış kimlik avı URL'si yer almıştır. Bu rakamlar ışığında hata payı %2'nin altında (<%2), güvenilirlik ise %95'in üstündedir.

## Bir Günde Eklenen Ortalama Kötü Amaçlı URL Sayısı

Her gün test setine ortalama 136 adet doğrulanmış yeni URL eklenmiştir. Suç faaliyeti seviyelerindeki dalgalanmalar sebebiyle bazı günlerde bu sayılarda değişiklikler gözlenmiştir.

## Kimlik Avı URL'lerinin Engellenmesi

NSS, tarayıcıların internette ilk keşfedildikleri anda kötü amaçlı URL'leri engelleme kabiliyetlerini değerlendirmeye tabi tutmuştur. Mühendislerimiz, sağlayıcıların koruma ekleyip eklemediğini ve ekleyenlerin ne kadar hızlı koruma eklediğini belirlemek için bu testleri her altı saatte bir tekrarlamıştır.

Yeni Microsoft Edge, Chromium'a dayalı olarak geliştirilmiş ve 15 Ocak 2020'de kullanıma sunulmuştur. Windows ve macOS'un desteklenen tüm sürümleriyle uyumludur. İndirilen tarayıcı, Windows 10 bilgisayarlardaki eski Microsoft Edge sürümünün yerini alır.

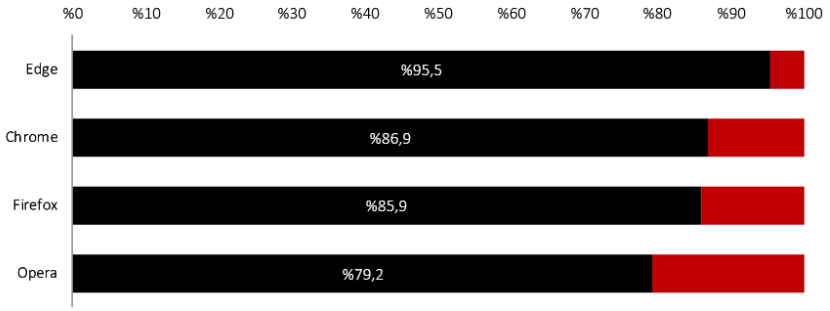
https://support.microsoft.com/tr-tr/help/4501095/download-the-new-microsoft-edge-based-on-chromium

[1] APWG Kimlik Avı Etkinliği Trendleri Raporu

## Kimlik Avı Engelleme Oranı

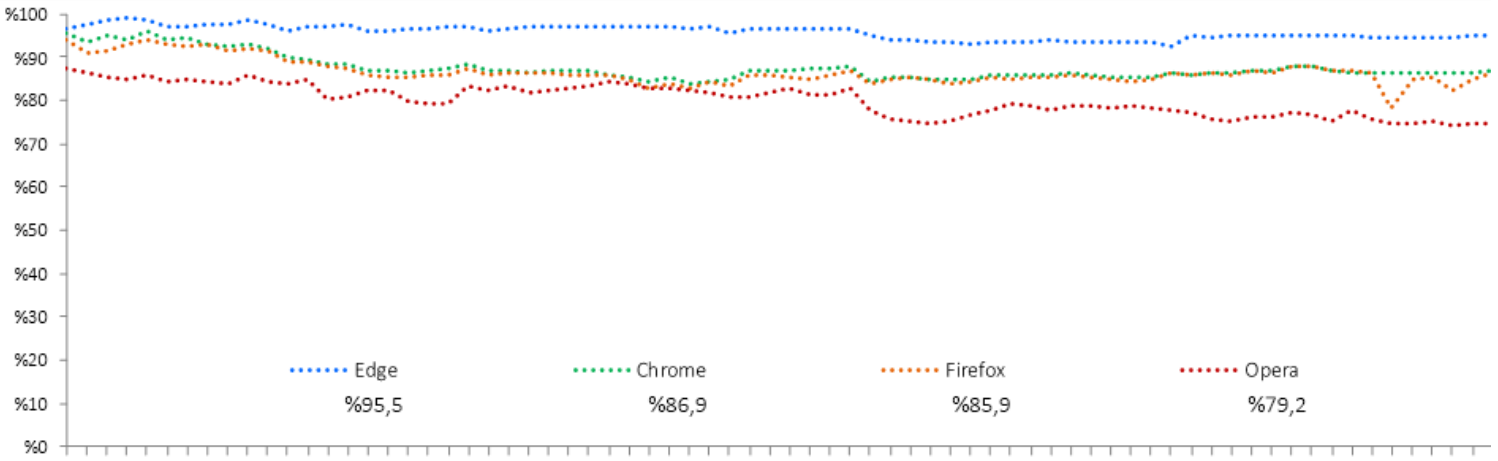
Google Chrome ve Mozilla Firefox, Google'a ait Safe Browsing API'yi kullanmaktadır. Microsoft Edge, kimlik avı ve kötü amaçlı yazılım tehditlerine karşı koruma sağlamak amacıyla, uygulama saygınlık hizmetini de içeren Microsoft Defender SmartScreen'i kullanmaktadır. Opera; Netcraft[2], PhishTank[3] ve Metamask[4] kaynaklı engellenenler listesi kombinasyonunun yanı sıra Yandex'in[5] kötü amaçlı yazılım engelleme listesini kullanmaktadır.

Olası kurbanları kötü amaçlı bir web sitesine girebileceklerine dair uyarma kabiliyeti, web tarayıcılarına kimlik avıyla ve diğer suç faaliyetleriyle mücadele konusunda benzersiz bir pozisyon kazandırır. Kimlik avı sitelerinin ömrü kısa olduğundan, sitenin mümkün olan en kısa sürede keşfedilmesi, doğrulanması, sınıflandırılması ve saygınlık sistemine eklenmesi büyük önem taşır. Burada ortalama engelleme süresi ile yakalama oranı arasındaki ilişki açıklanmaktadır. İyi 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 kimlik avı sitesi engellenmektedir.




Her tarayıcının kendi engelleme performansı sürekli olarak ölçülmüş ve tarayıcı tarafından test edilen tüm URL'lerin genel engellenme oranı kaydedilmiştir. Bir tarayıcının genel engelleme oranı, başarılı engelleme sayısının toplam test vakası sayısına bölünmesiyle hesaplanmıştır. Örneğin, testlerin her 6 saatte bir gerçekleştirildiği bu modelde, 48 saat boyunca çevrimiçi kalan bir URL toplamda 8 defa test edilmektedir. 8 denemenin 6 tanesinde engellemeyi başaran bir tarayıcı, %75 engelleme oranı elde etmektedir.

## Zaman İçinde Koruma Sürekliliği




Test boyunca günlük olarak yeni kimlik avı URL'leri eklenmiştir. Bir noktadan sonra erişilemeyen veya kimlik avı içermeyen URL'ler kaldırılmıştır. Her veri noktası, belirli bir andaki korumayı temsil etmektedir. Bir URL ilk anlarda engellendiyse, tarayıcının zaman içinde koruma sürekliliği skoru artırılmıştır. Aynı şekilde, tarayıcı URL'yi engellemediyse bu skor düşürülmüştür.

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

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

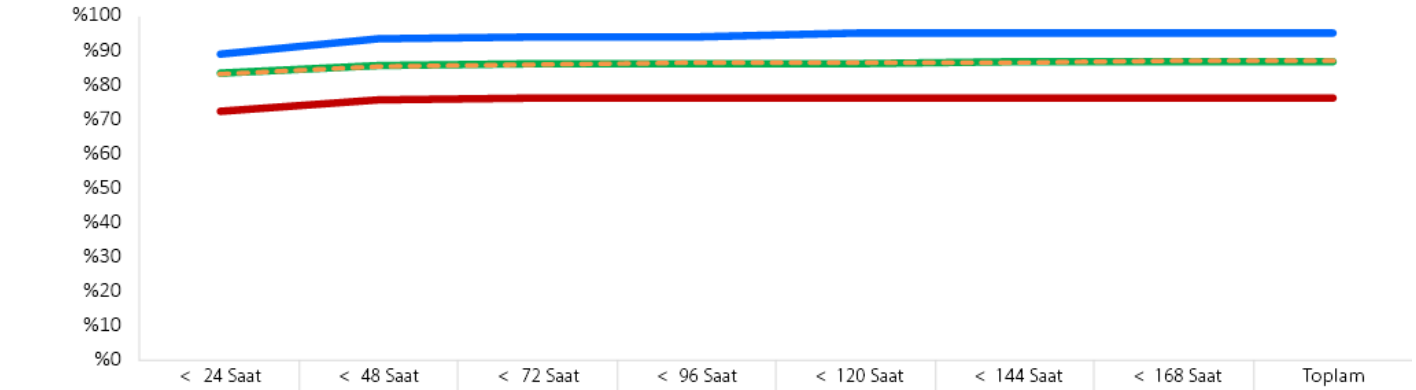
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

## Kimlik Avı Koruması Çubuk Grafiği

Yeni kimlik avı URL'lerine karşı anında koruma kabiliyeti kritik önem taşır. Keşfedilen kimlik avı siteleri, genellikle kısa bir süre içerisinde erişime kapatılır. Koruma önlemlerini zamanında alamayan ürünler, tehditlere yeterince erken karşılık veremeyebilir. Aşağıdaki çubuk grafikte, tehdit test döngüsüne girdikten sonra her bir tarayıcının kimlik avı sitesini engellemesi için geçen süre gösterilmektedir. Yedi günlük dönemde, kümülatif koruma oranları, tehditler engellenene kadar her gün hesaplanmıştır.

Test sırasında Microsoft Edge'in kimlik avı saldırılarına karşı ilk koruma oranı %89,2 olmuştur. Google Chrome ve Mozilla Firefox, sırasıyla %83,7 ve %83,2 ilk koruma oranına ulaşmıştır. Opera'nın ilk koruma oranı %72,2 olarak gerçekleşmiştir. Testlerin yedinci günü itibariyle, tüm web tarayıcılarının koruma oranı artmıştır. Microsoft Edge, %5,7 artışla %94,9'a ulaşmıştır. Mozilla Firefox %3,7 artışla %86,9, Google Chrome %3 artışla %86,7'ye ulaşmıştır. Opera %4,1 artışla 76,3'e çıkmıştır.




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

## 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 – 84.0.502.0
- 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