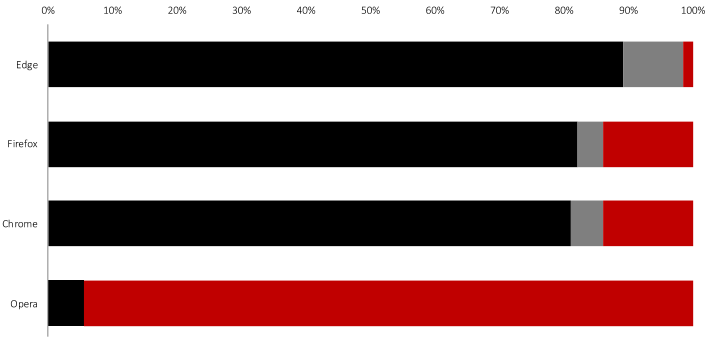
2020 年第 2 四半期 比較テスト レポート

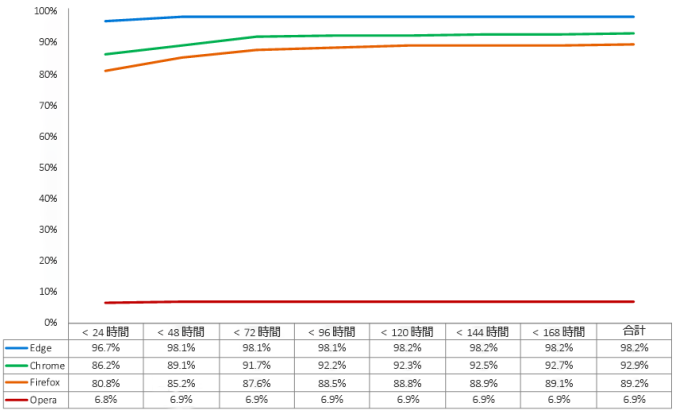
概要

2020 年第 2 四半期中に、NSS Labs は Web ブラウザーが提供するマルウェア保護の独立テストを実施しました。1,065 の一意のサンプルを使用し、34 日かけて 32,267 の個別テスト (Web ブラウザーごと) を行いました。対マルウェア保護に、Microsoft Edge は Microsoft Defender SmartScreen を使用し、Google Chrome と Mozila Firefox は Google Safe Browsing API を、また、Opera は Yandex を使用しています。



Microsoft Edge が最大の保護を示し、マルウェアの 98.5% をブロックして、最高のゼロ時間保護率 (96.7%) を提供しました。Firefox は 2 番目に多くの保護を提示し、平均で 86.1% をブロックしました。次は Google Chrome の 86.0% でした。Opera は 5.6% をブロックしました。

結果の概要

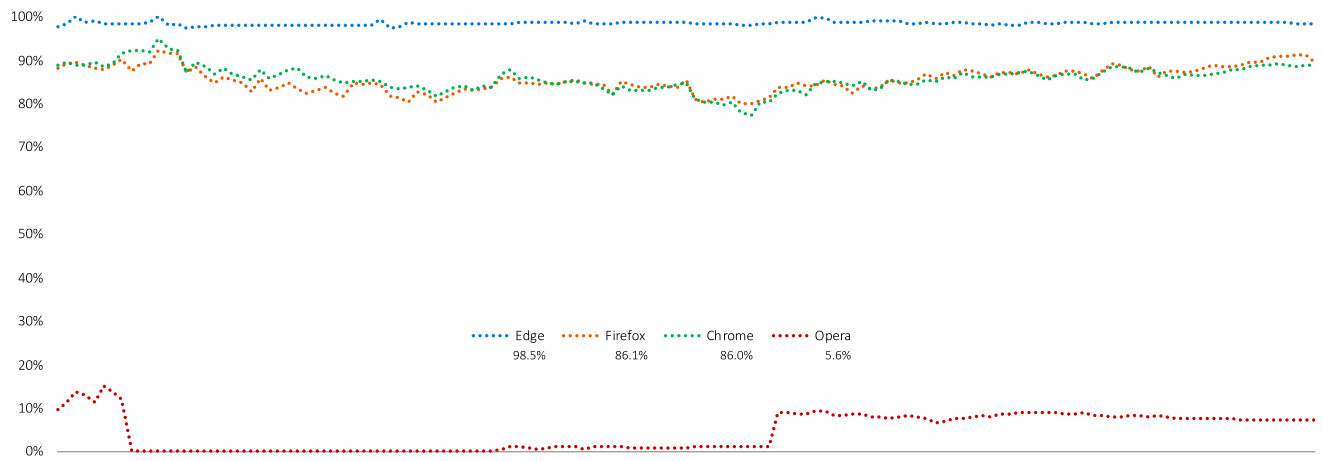


	< 24 時間	< 48 時間	< 72 時間	< 96 時間	< 120 時間	< 144 時間	< 168 時間	合計
Edge	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Chrome	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Firefox	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Opera	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

レピュテーション システムは、URL、ファイル、アプリケーションを阻止するか、または危険をユーザーに警告し、攻撃者が目標達成に使える時間を短縮します。しかし、ユーザーは常に新しい Web サイトにアクセスし、ファイルをダウンロードし、アプリケーションをインストールします。レピュテーション システムは、新しいものすべてを単純にブロックすることはできません。これを知る攻撃者はマルウェアの攻撃活動を常に変化させ、すべての攻撃の大半は攻撃活動の立ち上げ後数時間に発生しています。したがって、コンテンツをすばやく正確に分類することが、保護を成功させるための鍵となります。

NSS Labs では、当社がマルウェアをインターネットで見つけるのと同じぐらいすばやくブロックするブラウザー機能の評価を行いました。当社は、悪意のある URL、ファイル、アプリケーションについて 6 時間ごとのテストを継続し、ベンダーが保護を追加する場合、どのぐらい時間がかかるかを判定しました。

時間の経過に伴うマルウェア保護



テスト中には、常に新しいマルウェアの追加がありました。到達不能になるか、またはマルウェアをホストしていない URL、ファイル、アプリケーションは削除されました。各データ ポイントは、特定の時点で記録した測定値から計算します。マルウェアが早期にブロックされると、時間の経過に伴う保護の一貫性に対するブラウザーのスコアが上がりました。または、ブラウザーがマルウェアをブロックしない場合、このスコアは下がりました。

テストは、Web Browser Test Methodology v4.0 (www.nsslabs.com で提供) に基づいて行われました。

このレポートは秘密情報であり、明示的に NSS Labs のライセンス クライアント限定とします。

背景

ソーシャル エンジニアリング マルウェア (SEM) 攻撃は、ソーシャル メディア、ハイジャックされたメール アカウント、コンピューターの問題に関する偽の通のルウェアをユウユーザーにンロ、そのードさせることを促す他の手口をダイナミックに組み合わせて利用します。サイバー犯罪者は、連絡先間の絶対的な信頼を利用し、被害者に悪意のあるファイルが信頼できるものであると信じさせるために、ハイジャックされたメール アカウントを利用します。ハイジャックされたソーシャル メディアアカウントも、ハイジャックされたメール アカウントと同じ方法で利用されます。しかし、ソーシャル ネットワークの場合、被害は広範囲になります。友達だけでなく、友達の友達が騙されるリスクがあります。

ソーシャル エンジニアリングの戦術では、ポップアップ メッセージを利用することがあります。例えば、ユーザーに対して、Adobe Flash Player のインストールが必要であること、またはコンピューターがウイルスに感染したか更新が必要であるなどのアドバイスを行います。マルウェアがインストールされると、なりすまし、預金口座の情報漏洩、および他の破滅的な結果となりうる手口に対し、被害者は脆弱になります。

マルウェアに対する Web ブラウザーの保護

対マルウェア保護を行うには、ブラウザーはクラウドベースのレピュテーション システムを用いて、悪意のある Web サイトをインターネット上で探し出し、コンテンツをブロックリストまたはホワイトリストに追加するかまたはスコアを割り当てて (ベンダーのアプローチにより異なります) 適宜分類します。

これらの分類技術は、手動または自動で実行できます。対マルウェア保護の 2 つ目の機能コンポーネントでは、Web ブラウザーが特定の URL、ファイル、アプリケーションのレピュテーション情報をクラウドベースのレピュテーション システムに要求してから、マルウェアに対する警告を出すか、マルウェアをブロックします。

結果がマルウェアが存在することを示している場合、Web ブラウザーはユーザーを、URL、ファイル、アプリケーションが悪意のあるものであることを説明する警告メッセージへリダイレクトします。レピュテーション システムの一部には、追加的な教育コンテンツも含まれています。逆に、コンテンツが「良好」であると判定されれば Web ブラウザーは何もアクションを起こさず、ブラウザーが今しがたセキュリティ チェックを行ったということにユーザーが気づくことはありません。

Google と Firefox は、URL 評価、および特定タイプのファイルのダウンロードをブロックするかユーザーに警告を出す場合の両方で、Google Safe Browsing API を利用します。Microsoft Edge は、フィッシングやマルウェアの脅威に対して保護を提供するアプリケーションの評価サービスを含む Microsoft Defender SmartScreen を利用しています。Opera は、Netcraft、[1]PhishTank、[2]Metamask[3] のブロックリストを組み合わせたもの、ならびに Yandex[4] のマルウェア ブロックリストを利用しています。

さらに、2017 年 10 月の Windows 10 の更新プログラムにより、Microsoft Defender SmartScreen が OS 全体の機能として組み込まれています。SmartScreen 保護のオペレーティング システム版は、マルウェアに対する OS 保護の一環として、すべてのブラウザー、メール クライアント、USB、他のアプリケーションの防御策となります。したがって、ユーザーはブラウザーの URL 保護、ブラウザーのアプリケーション/ファイル保護、ならびにオペレーティング システムの保護という利益を享受することができます。

テストの構成 - マルウェアのサンプル

このレポートのデータは、2020 年 4 月 21 日～2020 年 5 月 25 日の 34 日間のテスト期間にまたがっています。すべてのテストはテキサス州オースティンにある NSS のテスト施設で行われました。テスト期間中、NSS のエンジニアは接続の監視をルーチンとして行い、テスト対象のブラウザーがマルウェアやクラウドのレピュテーション サービスに確実にアクセスできる状態となるようにしました。

強調されたのは鮮度です。したがって、結果となるテスト セットの一環として最終的に保持するよりも、多くのサンプルを評価しました。新しいサンプルが常にテストに追加され、使われていないサンプルは削除されたためです。

テストした悪意のあるサンプルの総数

合計 1,844 の未加工で未検証サンプルを、各 Web ブラウザーで複数回テストしました。822 時間 (6 時間ごとに 34 日間) 中断することなく、合計で 182,676 の個別のテストを実施しました。NSS のエンジニアは、(このテストの一環ではなく) 悪用で汚染されたものも含めて、検証基準をパスしなかったサンプルを削除しました。最終的には、129,068 の個別の有効なマルウェア テスト (Web ブラウザーごとに 32,267) に含まれた一意の有効なマルウェア サンプルは 1,065 で、信頼度は 95%、誤差範囲は 2% 未満 (<2%) でした。

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

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

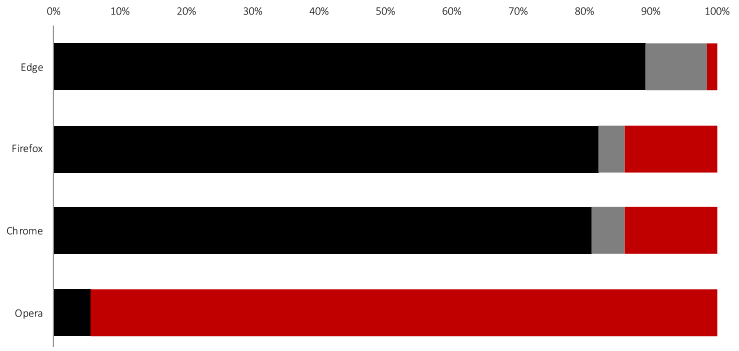
[3] https://github.com/metamask/eth-phishing-detect

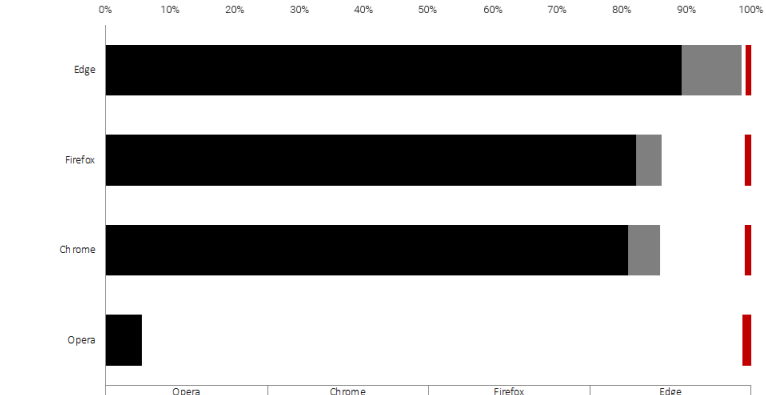
[4] https://yandex.com

このレポートは秘密情報であり、明示的に NSS Labs のライセンス クライアント限定とします。

マルウェア ブロック率

悪意のある Web サイトに迷い込みそうな潜在的な犠牲者に警告を出す機能は、Web ブラウザーをソーシャル エンジニアリング マルウェアと戦うというユニークな立場に置いています。マルウェア サイトの寿命は短いため、できるだけ早くサイトを発見して、検証、分類を行い、レピュテーション システムに追加することが基本です。このように、よいレピュテーション システムは、高いキャッチ率を実現するために、正確かつすばやいものである必要があります。ブラウザーの開発者は、この関係をはっきりと理解しており、最初の 24 時間の検出でブロックされるマルウェアの数は、その後にブロックされるものよりも実質的に多くなっています。





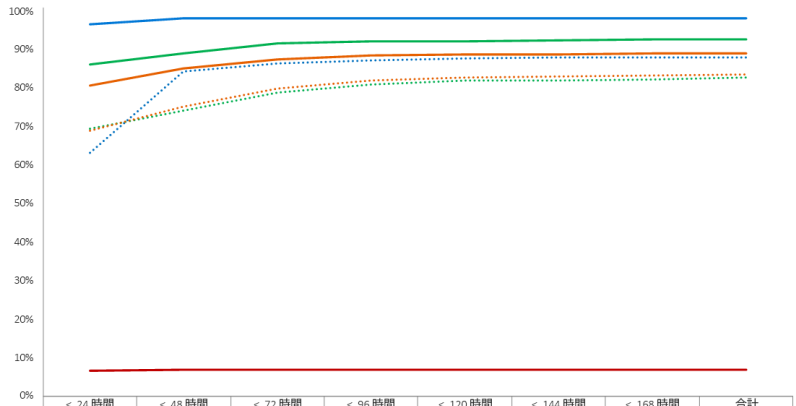
	Opera	Chrome	Firefox	Edge
URL 評価	5.6%	80.9%	82.1%	89.2%
URL + アプリ評価	0.0%	5.0%	4.0%	9.3%
URL + アプリ + OS 評価	93.1%	13.1%	13.0%	0.7%
ミス	1.4%	0.9%	0.9%	0.8%

Edge の中核となる保護技術は SmartScreen で、これは統合クラウドベースの URL のレピュテーション サービスへの攻撃に対する URL ベースの保護、ならびに悪意のあるファイル ブロッキングに対するアプリケーションの評価を提供します。アプリケーション評価を持つ SmartScreen は、Edge で 98.5% をブロックしました。Mozilla Firefox と Google Chrome は、Safe Browsing API を利用しています。Firefox は、86.1% をブロックしました。Google Chrome は、86.0% をブロックしました。複数のソースのブロックリストを組み合わせて利用している Opera は、5.6% をブロックしました。

さらに Microsoft Defender SmartScreen は、悪意のあるファイルを実行しようとした際に、Opera で追加的に 93.1%、Chrome では 13.1%、Firefox で 13.0% 、Edge で 0.7% をブロックしました。

マルウェア保護のヒストグラム

新しいマルウェアに対しては、速やかに保護を提供することが極めて重要です。マルウェアをホストするサイトは発見されると削除されますが、比較的短時間での削除となることがよく見られます。タイミングよく保護を追加できない製品は、脅威への対処が遅すぎとなる可能性があります。このヒストグラムは、サンプルをテスト サイクルに導入したときに、マルウェアをブロックするのに各ブラウザーでかかった時間を示しています。7 日間の時間枠内で、脅威がブロックされるまで、累積保護率が毎日計算されます。



	< 24 時間	< 48 時間	< 72 時間	< 96 時間	< 120 時間	< 144 時間	< 168 時間	合計
Edge とアプリ評価	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Edge と URL 評価	63.4%	84.5%	86.5%	87.3%	87.8%	88.1%	88.1%	88.1%
Chrome とアプリ評価	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Chrome と URL 評価	69.7%	74.4%	79.0%	81.0%	82.0%	82.2%	82.4%	82.7%
Firefox とアプリ評価	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Firefox と URL 評価	69.1%	75.3%	80.0%	82.1%	82.9%	83.0%	83.4%	83.6%
Opera と URL 評価	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

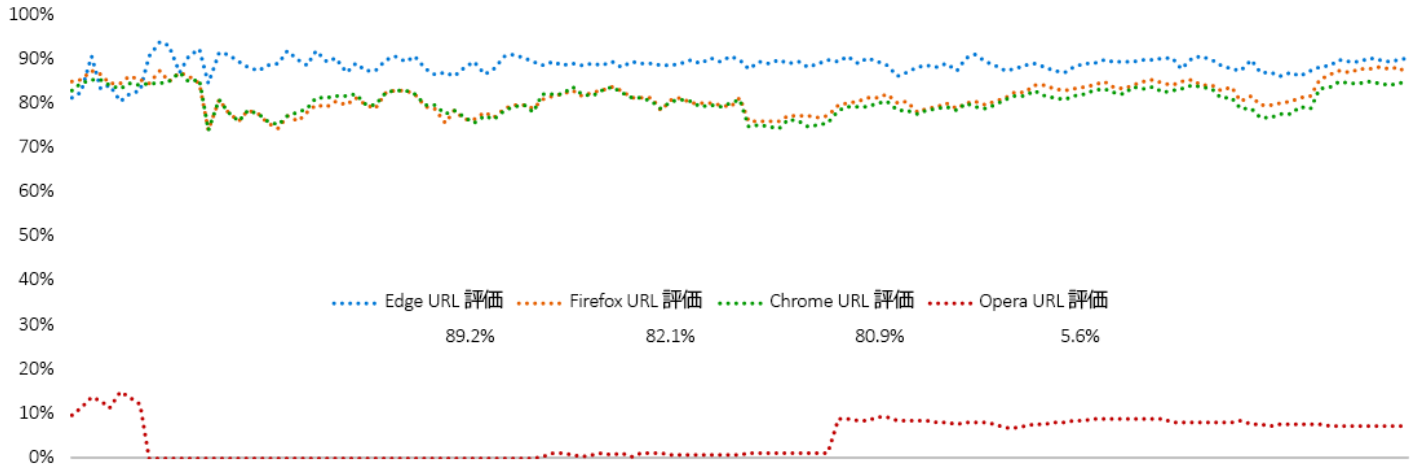
テスト中、Microsoft Edge はマルウェアに対して 96.7% の初期保護率を示しました。Google Chrome と Mozilla Firefox は、それぞれ 86.2% と 80.8% の初期保護率を達成しました。Opera の初期保護率は、6.8% でした。テスト 7 日目の終わりには、すべての Web ブラウザーで保護が強化されました。Microsoft Edge では、4.5% から 98.2% に増加しました。Google Chrome では 6.7% から 92.9%、Mozilla Firefox では 8.4% から 89.2%、Opera では 0.1% から 6.9% に増加しました。

このレポートは秘密情報であり、明示的に NSS Labs のライセンス クライアント限定とします。

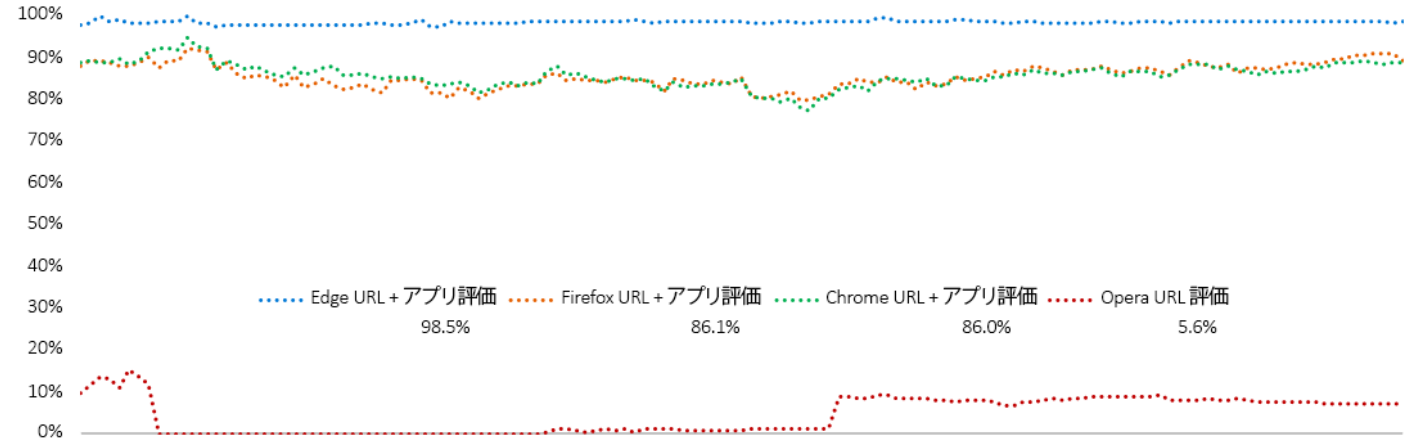
時間経過に伴う保護の一貫性

テスト中には、常に新しいマルウェアの追加がありました。到達不能になるか、またはマルウェアをホストしていない URL、ファイル、アプリケーションは削除されました。各データ ポイントは、特定の時点で記録した測定値から計算します。マルウェアが早期にブロックされると、時間の経過に伴う保護の一貫性に対するブラウザーのスコアが上がりました。または、ブラウザーがマルウェアをブロックしない場合、このスコアは下がりました。

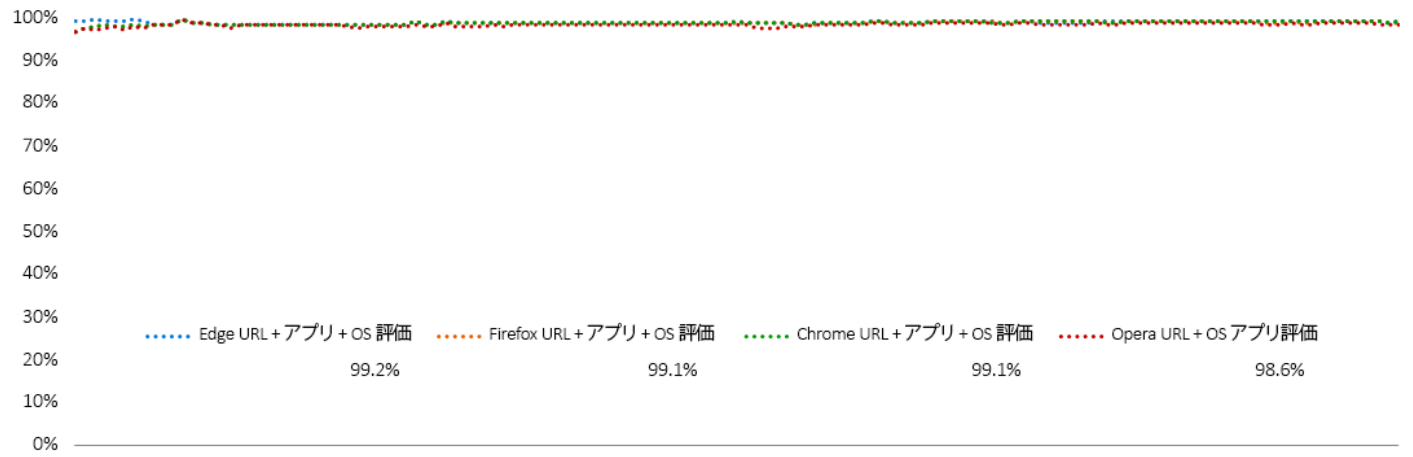
テストでは、3 つの保護レイヤーが明らかにされました。ブラウザーの URL 評価、アプリケーション評価、および OS アプリケーション評価です。URL 評価は、かなり満足で、よい保護を提供しました。



アプリケーション評価にレイヤーを重ねると、保護が強化されました。



オペレーティング システム評価は、さらに追加的な保護を提供しました。Web ブラウザーがマルウェアをブロックし、オペレーティング システムに到達させないようにすることが理想的です。しかしテストでは、オペレーティング システム評価には非常に効果があることが示されました。



このレポートは秘密情報であり、明示的に NSS Labs のライセンス クライアント限定とします。

テスト環境

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

テスト対象製品

- Google Chrome: バージョン 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge: バージョン 83.0.478.10 – 84.0.516.1
- Mozilla Firefox: バージョン 75.0 – 76.0.1
- Opera: バージョン: 67.0.3575.137 – 68.0.3618.125

このレポートは秘密情報であり、明示的に NSS Labs のライセンス クライアント限定とします。

Authors

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

テスト方法

NSS Labs Web Browser Security (WBS) Test Methodology v4.0 は、www.nsslabs.com で提供されています。

連絡先情報

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com

本書と他の関連ドキュメントは、以下の URL で提供されています。www.nsslabs.com ライセンス コピーを受け取るか、誤用を報告する場合は、NSS Labs にご連絡ください。

© 2020 NSS Labs, Inc. All rights reserved.このパブリケーションは、いずれの部分についても、NSS Labs, Inc. (以下「当社」) の書面による明示的な同意を得ずに、複製、コピー/スキャン、情報検索システムへの保存、メールあるいは他の手段による拡散や送信を行うことを禁じます。

この枠線内の免責条項をお読みください。読者に対する法的拘束力のある重要な情報が含まれています。これらの条件に同意しない場合は、読者はこのレポートの残りの部分は読まずに、レポートを当社に速やかに返却する必要があります。「読者」とは、このレポートにアクセスした者、および読者の代理にこのレポートを入手したエンティティを指します。

1.このレポート内の情報は事前の通知なしに変更されることがあり、当社には更新の義務はありません。

2.このレポート内の情報は、発行時に当社が正確かつ信頼性があると信じるものですが、保証はされません。このレポートを利用し、信頼することにより生じるリスクは、読者のみが負うものとなります。このレポート内のエラーや脱落により生じるいかなる性質の損害、損失、費用に対しても、当社は責任を負いません。

3.当社は明示的または暗示的を問わず、いかなる保証も提供しません。商品性、特定の目的への適合性、権利侵害の不存在についての保証を含むすべての黙示の保証を、当社はここに否認し、除外します。直接的、結果的、付随的、懲罰的、典型的、間接的な損害、または利益、収益、データ、コンピューター プログラムの損失、あるいは他の資産の損失に対して、当社はいかなるときも責任を負わないこととします。これは、そうした可能性があると指摘があった場合でも変わりません。

4.このレポートは、テスト対象となるいかなる製品 (ハードウェアまたはソフトウェア)、製品のテストに使用されるハードウェアおよび / またはソフトウェアを承認、推奨、保証するものではありません。テストは、製品にエラーや欠陥がないこと、製品が読者の期待、要件、ニーズを満たすこと、製品が中断なく操作されることを保証するものではありません。

5.このレポートは、このレポート内で言及される組織による承認、スポンサー、提携、検証を意味するものではありません。

6.このレポートで使用されるすべての商標、サービス マーク、商号は、それぞれの所有者の商標、サービス マーク、商号です。