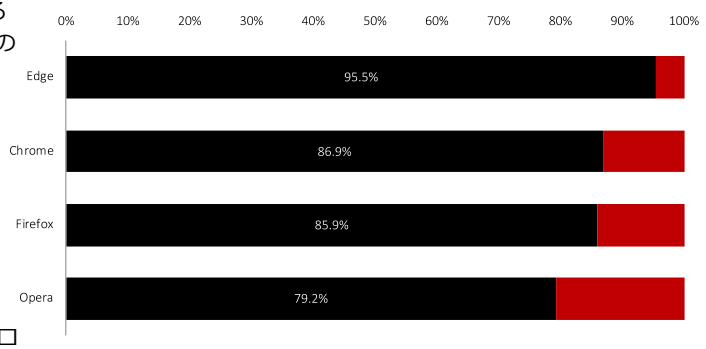
2020 年第 2 四半期 比較テスト レポート

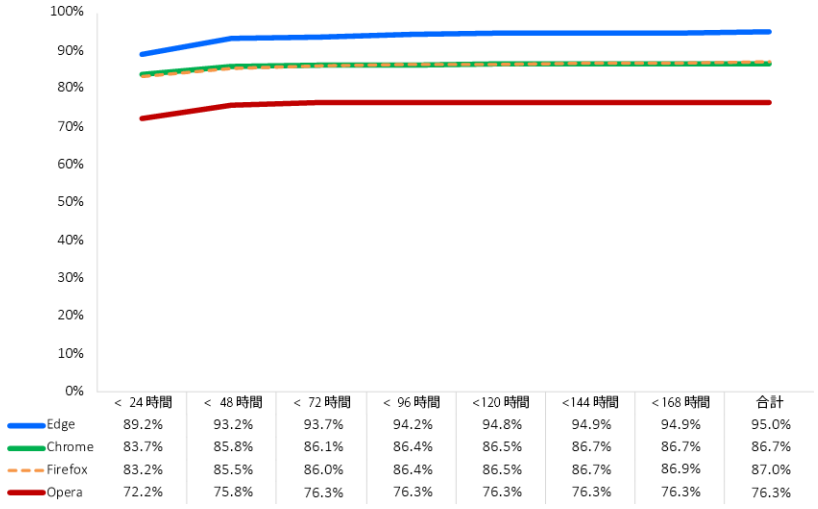
概要

2020 年第 2 四半期中に、NSS Labs は Web ブラウザーが提供するフィッシング保護の独立テストを実施しました。 2,443 の一意のフィッシング URL を使用し、 18 日かけて 47,274 の個別テスト (ウェブブラウザーごと) を行いました。対フィッシング保護に、Microsoft Edge は Microsoft Defender SmartScreen を使用し、Google Chrome と Mozila Firefox は Google Safe Browsing API を、また、Opera はサードパーティのブロックリストの組み合わせを使用しています。



Microsoft Edge が最大の保護を示し、フィッシングの 95.5% をブロックして、最高のゼロ時間保護率 (89.2%) 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 86.9% をブロックしました。次は Mozilla Firefox の 85.9% でした。Opera は、79.2% をブロックしました。

結果の概要

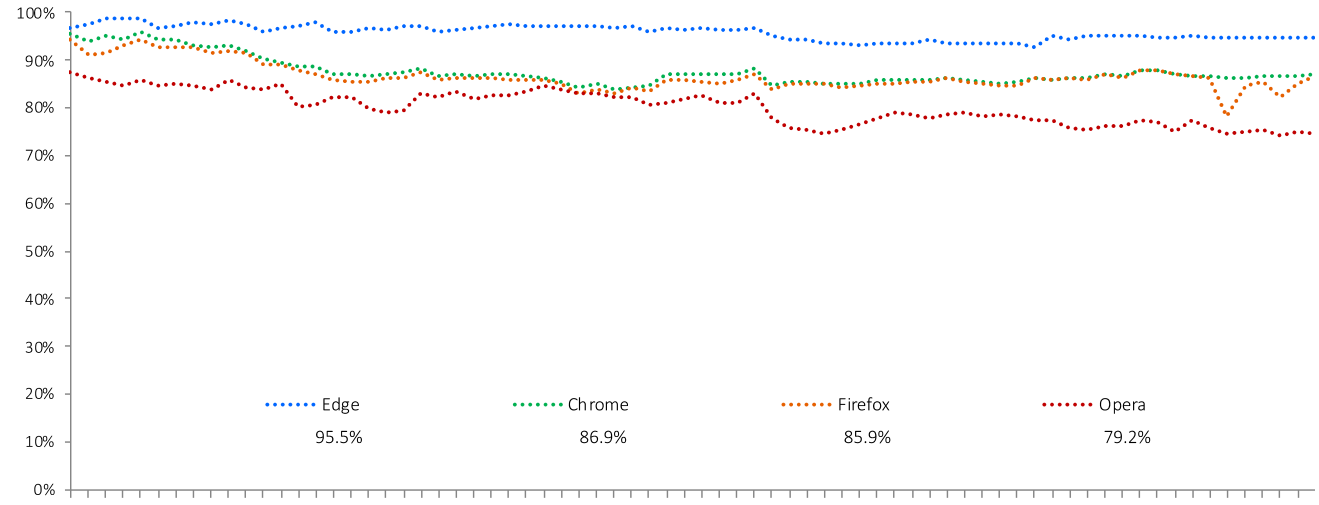


	< 24 時間	< 48 時間	< 72 時間	< 96 時間	<120 時間	<144 時間	<168 時間	合計
Edge	89.2%	93.2%	93.7%	94.2%	94.8%	94.9%	94.9%	95.0%
Chrome	83.7%	85.8%	86.1%	86.4%	86.5%	86.7%	86.7%	86.7%
Firefox	83.2%	85.5%	86.0%	86.4%	86.5%	86.7%	86.9%	87.0%
Opera	72.2%	75.8%	76.3%	76.3%	76.3%	76.3%	76.3%	76.3%

URL レピュテーション システムは、URL を阻止するか、基地のフィッシング サイトであるという旨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、ユーザーは広範な Web サイトにアクセスし、新しいサイトも多いため、URL レピュテーション システムですべての新しい URL 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フィッシィング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。

NSS Labs では、当社が悪意のある URL 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、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、どれぐらい時間がかかるかを判定しました。

時間の経過に伴うフィッシング保護



テスト中には、新しいフィッシング URL が毎日追加され、到達不能になるか、またはフィッシング攻撃を行っていない URL は削除されました。各データ ポイントは、特定の時点の保護を示しています。URL 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 URL 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。

背景

フィッシングは、ソーシャル エンジニアリング攻撃の一種で、機密性の高い個人情報を攻撃者に提供するよう被害者説得を試みるものです。機密情報の例をいくつか挙げると、クレジット カード番号、ソーシャル セキュリティ番号、ログイン情報、銀行口座のパスワードなどがあります。メール、インスタント メッセージ、SMS メッセージ、ソーシャル ネットワーキング サイトのリンクはすべて、フィッシング攻撃のベクトルとなります。フィッシング Web サイトのランディング ページでは、閲覧者のコンピューターを警告なしで悪用し、悪意のあるソフトウェアをインストールしようと試みることがよくあります (ドライブバイの悪用とも呼ばれます)。

フィッシング攻撃は、機密性の高い個人情報や企業情報を危険にさらすか、それらが取得される脅威により、個人と組織に対して同じように著しいリスクを負わせます。Anti-Phishing Working Group (APWG) は、2020 年の第 1 四半期に合計 165,772 の一意のメール フィッシングの攻撃活動が行われたことを報告しています。[1]フィッシング攻撃は、ますます複雑で洗練されたものになっていて、検出したり、防止したりするのがより困難になっています。

フィッシングに対する Web ブラウザーの保護

フィッシング保護は、Web ブラウザー内のアプリケーションが提供し、クラウドのレピュテーション サーバーから URL の評価を得るよう要求します。レピュテーション サーバーは、フィッシング Web サイトを探すためにインターネットをくまなく検索してから、各 URL にスコアを割り当て、ブロックリストに追加します。このようにして、Web ブラウザーに URL へのアクセスを指示すると、ブラウザーのフィッシング保護 (Safe Browsing、SmartScreen など) がクラウドベースのレピュテーション サーバーから URL の評価を得るよう要求します。そして、Web サイトが「悪い」ものだという結果であれば、Web ブラウザーはユーザーを、URL が悪意のあるものであると説明する警告メッセージに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、Web サイトが「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。

テストの構成 - フィッシング URL

このレポートのデータは、2020 年 4 月 21 日～2020 年 5 月 8 日の 18 日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フィッシング URL やクラウドのブラウザー 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、多くのサイトを評価しました。新しい URL が常にテストに追加され、使われていないサイトは削除されたためです。

テストした悪意のある URL の総数

合計で 4,020 の未加工で未検証の URL を、各 Web ブラウザーで複数回テストしました。430 時間 (6 時間ごとに 18 日間) 中断することなく、合計で 222,527 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、189,096 の個別の有効なフィッシングテスト (Web ブラウザーごとに 47,274) に含まれた一意の有効なフィッシング URL は 2,443 で、信頼水準は 95%、誤差範囲は 2% 未満 (<2%) でした。

1 日に追加される悪意のある URL の平均数

平均して、136 の新しい検証済み URL が毎日テスト セットに追加されました。犯罪活動のレベルの変動に伴い、この数字は日によって異なっていました。

フィッシング URL のブロック

NSS は、悪意のある URL がインターネットで見つかるのと同じぐらい、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。エンジニアは、6 時間ごとにこれらのテストを繰り返して、ベンダーが保護を追加する場合、どれぐらい時間がかかるかを判定しました。

新しい Microsoft Edge は Chromium をベースとし、2020 年 1 月 15 日にリリースされました。これは、Windows と macOS のすべてのサポートされているバージョンと互換性があります。ブラウザーをダウンロードすると、Windows 10 PC の Microsoft Edge レガシー バージョンが置換されます。

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

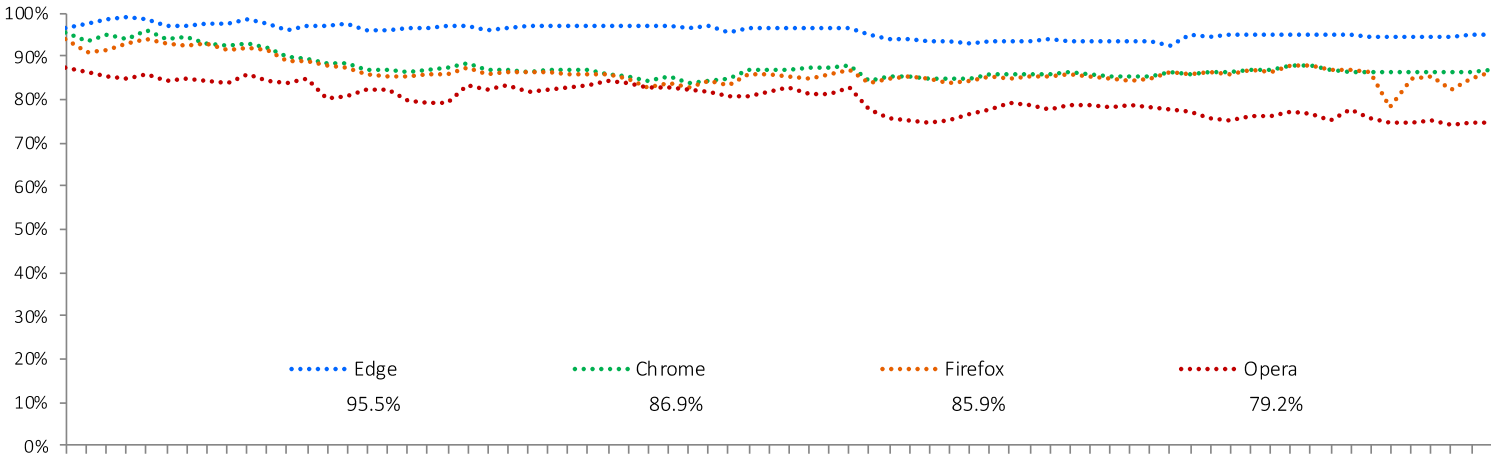
[1] APWG フィッシング活動トレンドレポート

フィッシング ブロック率

Google Chrome と Mozila Firefox は、Google Safe Browsing API を使用しています。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、[2]PhishTank、[3]Metamask[4] のブロックリストを組み合わせたもの、ならびに Yandex[5] のマルウェアブロックリストを利用しています。
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 ブラウザーをフィッシングや他の犯罪活動と戦うというユニークな立場に置いています。フィッシング 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。これは、ブロックするまでの平均時間とキャッチ率の間の相関関係を説明するものです。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フィッシング サイトの数は、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。

各ブラウザーの個別のブロック パフォーマンスを連続測定し、ブラウザーでテストしたすべての URL の全体のブロック率を記録しました。ブラウザー全体のブロック率は、ブロック成功数をテスト ケース合計数で割って計算します。例えば、6 時間ごとに実施するテストの場合、48 時間オンライン上にあった URL は 8 回テストされます。テストの実行で (最大 8 回のうち) 6 回をブロックすると、ブラウザーのブロック達成率は 75% となります。

時間経過に伴う保護の一貫性



テスト中には、新しいフィッシング URL が毎日追加され、到達不能になるか、またはフィッシング URL を配信しなくなっている URL は削除されました。各データ ポイントは、特定の時点の保護を示しています。URL 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 URL をブロックしない場合、このスコアは下がりました。

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

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

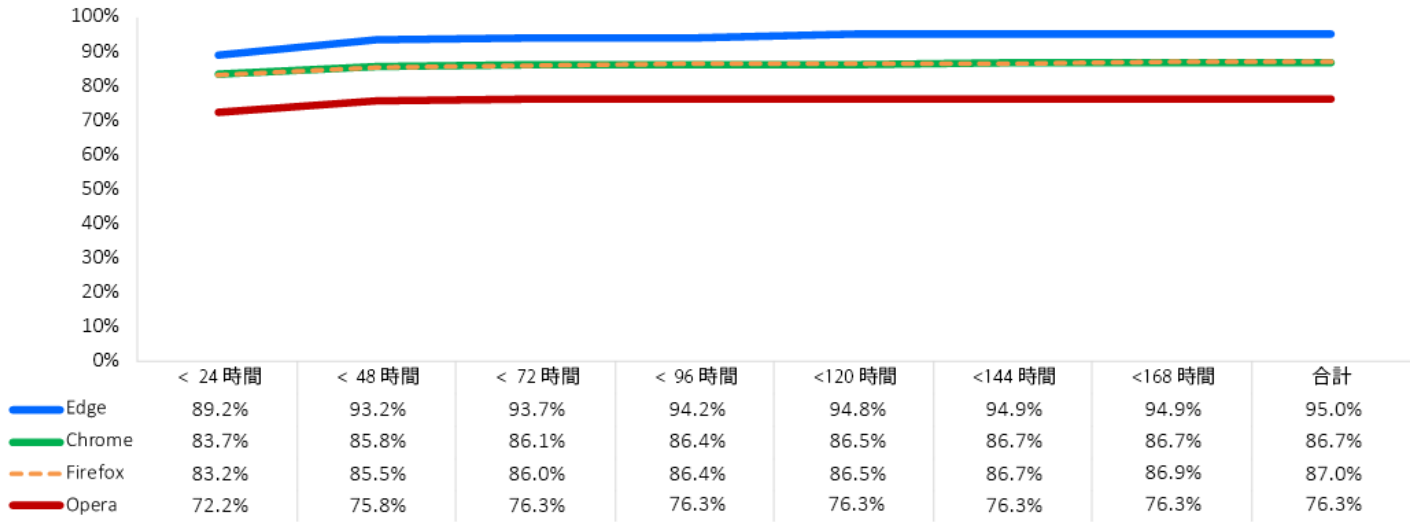
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

フィッシング保護のヒストグラム

新しいフィッシング URL 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。フィッシング サイトは発見されると削除されますが、比較的短時間内にサイトが削除され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。以下のヒストグラムは、脅威をテスト サイクルに導入したときに、フィッシング サイト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。

テスト中に、Microsoft Edge はフィッシング攻撃に対して 89.2% の初期保護率を示しました。Google Chrome と Mozilla Firefox は、それぞれ 83.7% と 83.2% の初期保護率を達成しました。Opera の初期保護率は、72.2% 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、5.7% から 94.9% に増加しました。Mozilla Firefox では 3.7% から 86.9%、Google Chrome では 3% から 86.7% に増加しました。Opera では、4.1% から 76.3% に増加しました。



	< 24 時間	< 48 時間	< 72 時間	< 96 時間	<120 時間	<144 時間	<168 時間	合計
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%

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 – 84.0.502.0
- 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

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