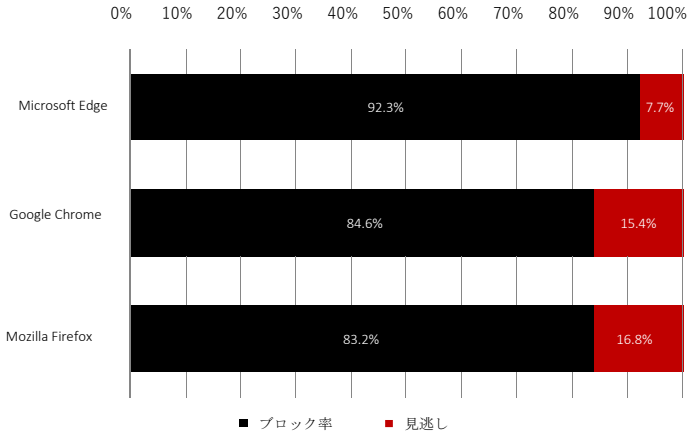
2021 年第 2 四半期 Web ブラウザー vs. フィッシング

概要

2021 年第 2 四半期中に、CyberRatings.org は Web ブラウザーが提供する対フィッシング保護の独立テストを実施しました。20 日かけて、80 の個別テストを行いました。対フィッシング保護に、Microsoft Edge は Microsoft Defender SmartScreen を使用し、Google Chrome と Mozilla Firefox は Google Safe Browsing API を使用しています。

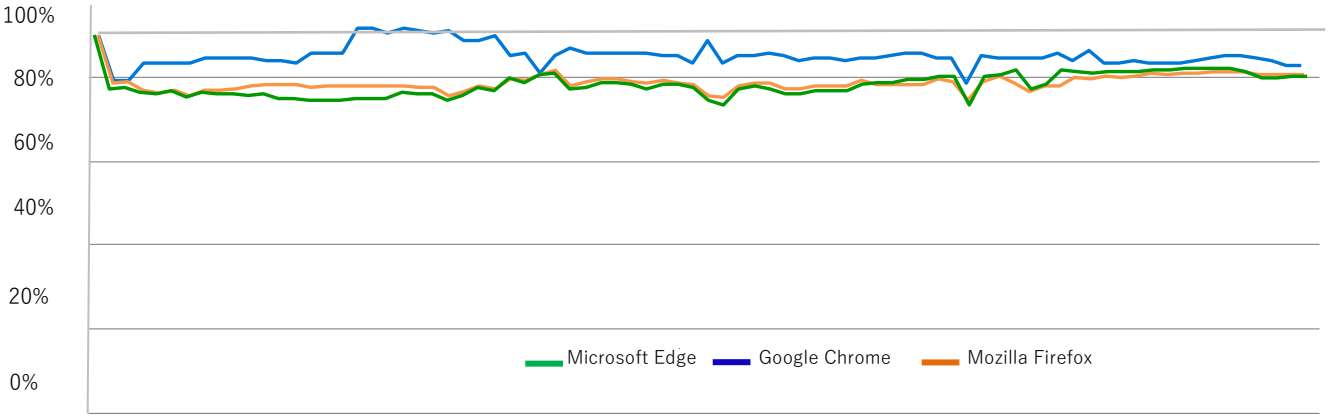
Microsoft Edge が最大の保護能力を示し、フィッシング URL の 92.3% をブロックして、最高のゼロ時間保護率 (93.5%) を提供しました。Google Chrome は 2 番目に大きな保護能力を示し、平均で 84.6% をブロックしました。その次が Mozilla Firefox の 83.2% でした。



結果の概要

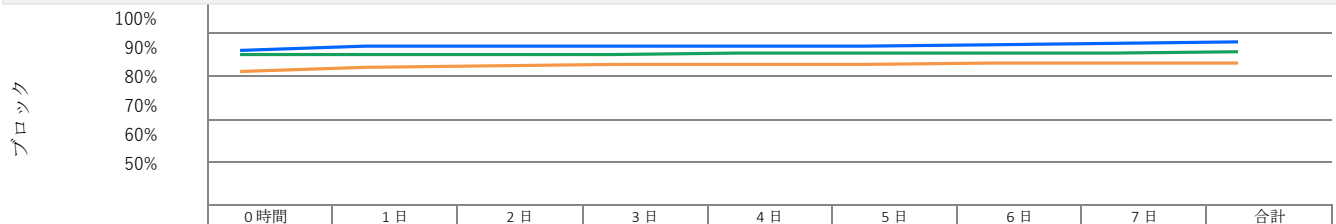
URL レピュテーション システムは、URL を阻止するか、既知のフィッシング サイトであるという旨をユーザーに警告し、攻撃者が目標達成に使える時間を短縮します。しかし、ユーザーは広範な Web サイトにアクセスし、新しいサイトも多いため、URL レピュテーション システムですべての新しい URL を単純にブロックすることはできません。これを知る攻撃者はフィッシングの攻撃活動を常に変化させ、新たな攻撃の大半は攻撃活動の立ち上げ後数時間内に発生しています。

時間の経過に伴う対フィッシング保護



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。

時間の経過に伴うフィッシ



	0 時間	1 日	2 日	3 日	4 日	5 日	6 日	7 日	合計
Microsoft Edge	93.5%	94.4%	94.5%	94.5%	94.5%	94.7%	94.9%	95.1%	95.4%
Google Chrome	92.4%	92.6%	92.7%	92.7%	92.8%	92.8%	92.8%	92.9%	93.2%
Mozilla Firefox	88.7%	89.7%	90.0%	90.4%	90.4%	90.4%	90.5%	90.6%	90.6%

当社では、インターネット上で見つかった悪意のある URL をすばやくブロックする、各ブラウザーの機能評価を行いました。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、どのくらい時間がかかるかを判定しました。上の数字は、サンプルをテスト 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。

フィッシング攻撃

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、被害者を説得して機密性の高い個人情報を攻撃者に提供させようとするものです。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進路となります。フィッシング詐欺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。The Anti- Phishing Working Group (APWG) は、2020 年の第 4 四半期に合計 396,688 の一意のメール フィッシィングの攻撃活動が行われたことを報告しています。1

フィッシングに対する Web ブラウザーの保護

対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、フィッシング詐欺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、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、ブラウザーの対フィッシング保護 (Safe Browsing、SmartScreen など) が、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ユーザーを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しません。

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 は統合クラウドサービスへの攻撃に対する URL ベースの保護、並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する Microsoft Defender SmartScreen を利用します。

1 日に追加される悪意のある URL の平均数

平均して、50 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。

テスト環境

- Microsoft Windows 10 Pro、21H1

テストした悪意のある URL の総数

合計 26,976 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。480 時間 (6 時間ごとに 20 日間) 中断することなく、合計で 80 テスト サイクルを実施しました。当社のエンジニアは、(このテストの一環ではなく) 悪用で汚染されたものを含めて、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、61,605 の個別のフィッシング テスト (Web ブラウザーごとに 20,535) に含まれた一意の有効なフィッシング URL は 996 で、信頼度は 95%、誤差範囲は 3.1% でした。

テストの構成 ー フィッシング URL

このレポートのデータは、2021 年 5 月 11 日～2021 年 5 月 31 日の 20 日間のテスト期間にまたがっています。テスト期間中、当社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、テストには常に新しい URL が追加され、使われていないサイトは削除されました。

結果の評価方法

当社では、インターネット上で見つかった悪意のある URL をすばやくブロックする、各ブラウザーの機能評価を行いました。エンジニアは 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、どのくらい時間がかかるかを判定しました。

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 に対するブラウザー全体のブロック率を記録しました。各ブラウザーの総合ブロック率は、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。たとえば、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) 6 回をブロックした場合に、ブロック率は 75% となります。

テスト対象製品

- Google Chromeバージョン 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge: バージョン: 91.0.864.19 - 91.0.864.37
- Mozilla Firefox: バージョン 88.0.1 - 88.0.1

1 APWG フィッシング活動トレンド レポート

作成者

Thomas Skybakmoen、Vikram Phatak

テスト方法

CyberRatings Web Browser Security Test Methodology v1.0 は www.cyberratings.org で提供されています

連絡先情報

CyberRatings.org

2303 Ranch Road 620 South

Suite 160, #501

Austin, TX 78734

info@cyberratings.org

www.cyberratings.org