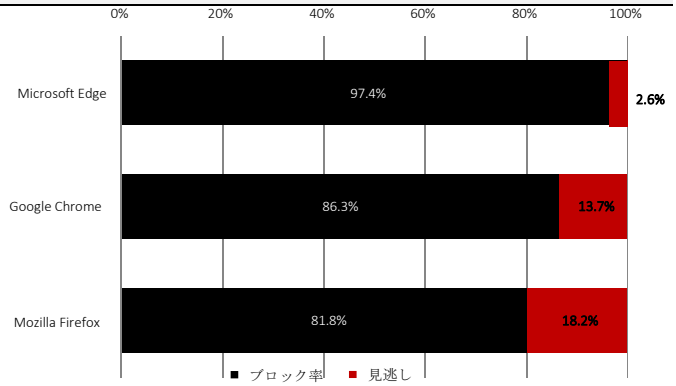
2021 年第 2 四半期　Web ブラウザー vs.マルウェ

概要

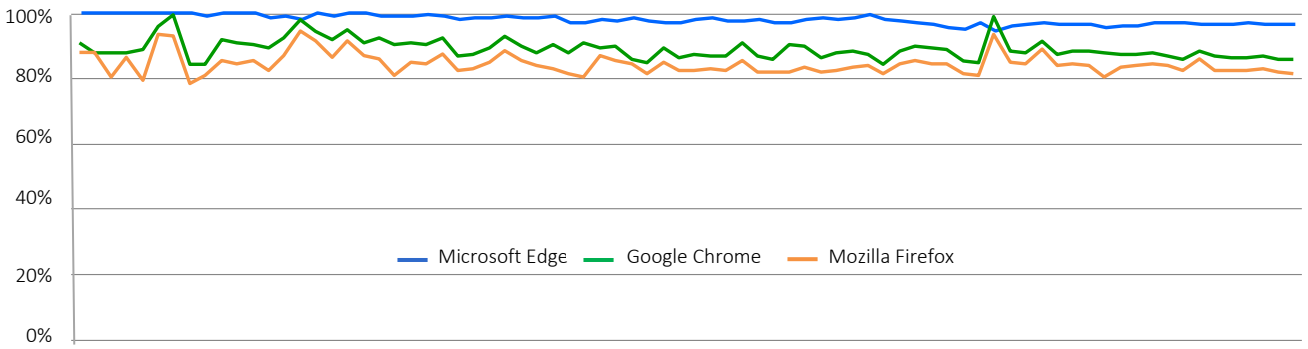
2021 年第 2 四半期中に、CyberRatings.org は Web ブラウザーが提供する対マルウェア保護の独立テストを実施しました。20 日かけて、80 の個別テストを行いました。対マルウェア保護に、Microsoft Edge は Microsoft Defender SmartScreen を使用し、Google Chrome と Mozilla Firefox は Google Safe Browsing API を使用しています。Microsoft Edge が最大の保護能力を示し、マルウェアの 97.4% をブロックして、最高のゼロ時間保護率 (97.7%) を提供しました。Google Chrome は 2 番目に大きな保護能力を示し、平均で 86.3% をブロックしました。その次が Mozilla Firefox の 81.8% でした。



結果の概要

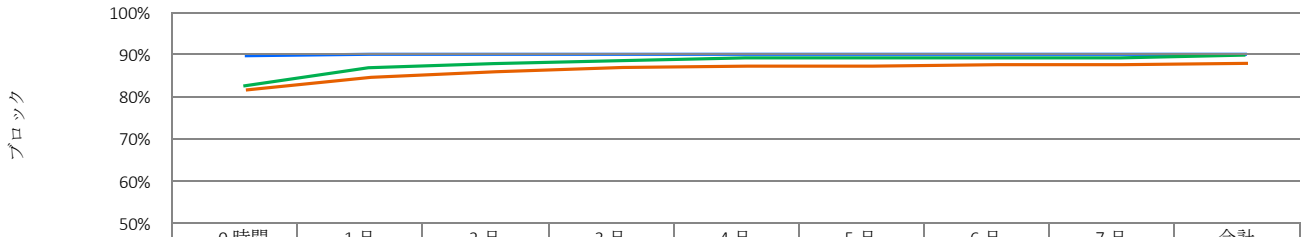
悪意のある Web サイトに迷い込みそうな潜在的な犠牲者に警告を出す機能は、Web ブラウザーをマルウェアと戦うというユニークな立場に置いています。ユーザーを騙して (ソーシャルエンジニアリング) マルウェアをダウンロードさせる Web サイトの寿命は短いため、できるだけ早くサイトを発見して、レピュテーション システムに追加することが基本です。よいレピュテーション システムは、高いキャッチ率を実現するために、正確かつすばやいものである必要があります。

時間の経過に伴う対マルウェア保護



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 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。

時間の経過に伴うマルウェア ブロック率



	0 時間	1 日	2 日	3 日	4 日	5 日	6 日	7 日	合計
Microsoft Edge	97.7%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%
Google Chrome	86.4%	90.6%	91.7%	92.5%	92.9%	93.1%	93.1%	93.1%	93.6%
Mozilla Firefox	82.8%	85.9%	87.1%	88.0%	88.3%	88.4%	88.6%	88.7%	89.1%

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、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。Microsoft 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。Google Chrome と Mozilla 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。

マルウェア攻撃

ソーシャル エンジニアリング マルウェア (SEM) 攻撃は、ユーザーを騙してマルウェアをダウンロードさせます：ハイジャックされたメールとソーシャル メディア アカウントを利用して、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ます。また、ポップアップ メッセージを利用して、Adobe Flash Player などのアプリケーションのインストールが必要であるとアドバイスする、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と警告するという手口もあります。

マルウェアがインストールされると、認証情報漏洩、なりすまし、預金口座の情報漏洩などの手口に対し、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

対マルウェア保護のため、クラウドベースのレピュテーション システムは、インターネット上の悪意のある Web サイトを選別し、コンテンツを適宜分類します。すると 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と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。

Google Chrome と Mozilla Firefox は、悪意のあるファイルをブロックするための URL 評価とアプリケーション評価に、Google Safe Browsing API を利用します。Microsoft Edge は、クラウドベースのレピュテーション サービスによる URL 評価および、悪意のあるファイルをブロックするためのアプリケーション評価サービスを提供する Microsoft Defender SmartScreen を利用します。

1 日に追加される悪意のあるマルウェアの平均数

平均して、49 の新しい検証済みマルウェア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。

テストした悪意のあるサンプルの総数

合計 18,621 の未加工で未検証のサンプルを、各 Web ブラウザーで複数回テストしました。468 時間 (6 時間ごとに 20 日間) 中断することなく、合計で 78 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、48,672 の個別のマルウェア テスト (Web ブラウサーごとに 16,224) に含まれた一意の有効なマルウェア サンプルは 950 で、信頼度は 95%、誤差範囲は 3.2% 未満 (<3.2%) でした。

テストの構成 ー マルウェアのサンプル

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、CyberRatings 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、テストには常に新しいサンプルが追加され、使われていないサンプルは削除されました。

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マルウェア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マルウェア サンプル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マルウェアは 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。

テスト環境

- Microsoft Windows 10 Pro、21H1

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

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