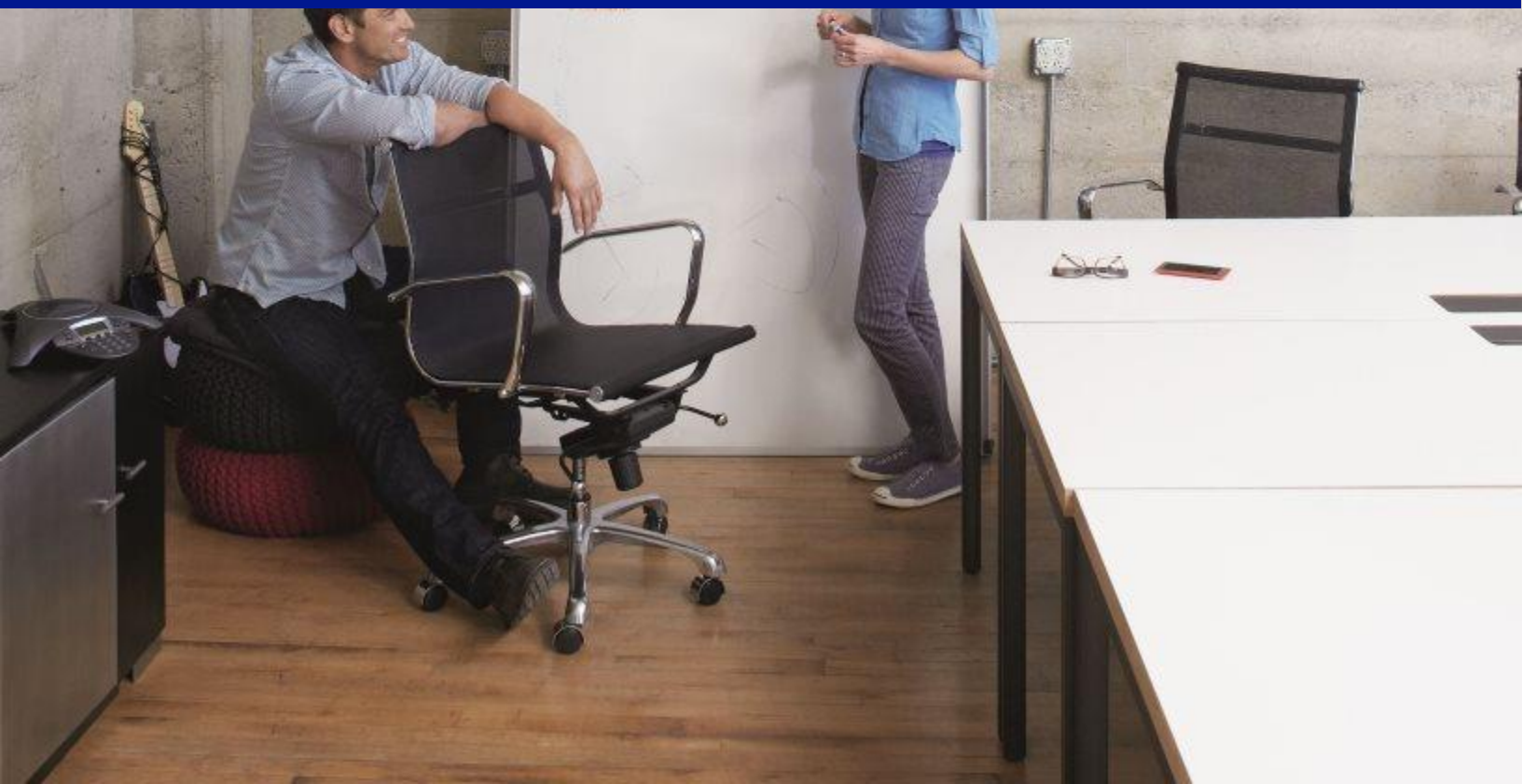
Microsoft

マイクロソフト セキュリティ インテリジェンス レポート

第 21 版 | 2016 年 1 月～ 6 月

主な調査結果の概要



脆弱性

業界全体の脆弱性露見は、2H15 から 1H16 にかけて 9.8% 減少し、3,000 件をやや上回っています。[1]Android アプリケーションにおける SSL の脆弱性に関する CERT/CC 研究プロジェクトの実施によって急増した 2H14 を除き、過去 3 年間にわたって露見は一般的に上昇傾向にあります。

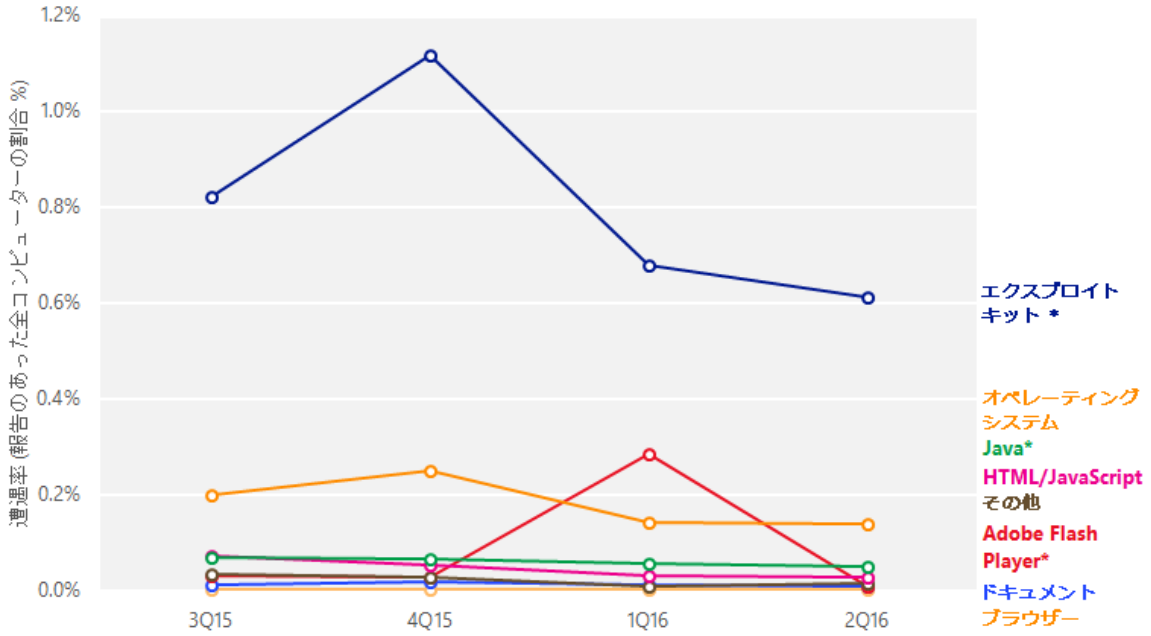
図 1. ソフトウェア業界全体での脆弱性 (CVE) の深刻度、複雑さ、タイプ別露見数、マイクロソフト製品およびマイクロソフト以外の製品の露見数の推移 (2H13 ～ 1H16)

[1] このレポートでは、半期および四半期を表すために *nHyy* または *nQyy* の形式の略記が使用されています。yy は暦年を n は半期または四半期のどの期間にあたるかを示します。

エクスプロイト

図 2 では、3Q15 から 2Q16 までの各四半期に、マイクロソフトのマルウェア対策製品が検出したさまざまな種類のエクスプロイトの蔓延状況を遭遇率で示しています。遭遇率とは、マイクロソフトのリアルタイムのセキュリティ製品を実行しているコンピューターのうち、マルウェアに遭遇したコンピューターの割合です。

図 2. さまざまな種類のエクスプロイトの遭遇率 (3Q15 ～ 2Q16)



複数のエクスプロイトを報告したコンピューターは、検出した種類ごとにカウントされています。* エクスプロイト キット、Java、および Adobe Flash Player のエクスプロイトの数は、多くの脅威との遭遇を未然にブロックする、Internet Explorer の IExtensionValidation の影響を受けます。詳細については、レポート全文をご参照ください。

- エクスプロイト キットとの遭遇回数は、3Q15 と 4Q15 の間に大幅に増加した後、4Q15 から 1Q16 にかけて 3 分の 1 を上回る減少となりました。エクスプロイト キットの遭遇率は、ついで遭遇率の高いエクスプロイトの 4 倍を超えており、2016 年下半期においても引き続き最も遭

遇の可能性が高い種類のエクスプロイトとなっています。これらのエクスプロイトの詳細については、レポート全文をご参照ください。

- Adobe Flash Player が関係するエクスプロイトの件数は、1Q16 に SWF/Netis の登場を受けて大幅に増加したものの、2Q16 には Netis との遭遇件数が減少したため、かなり低い水準に戻っています。
- オペレーティング システムを標的とするエクスプロイトは、1H16 の両方の四半期には遭遇回数がやや減少しましたが、Flash エクスプロイトも減少したため、当該期間末には 2 番目に多いエクスプロイトとなっています。詳細については、レポート全文をご参照ください。
- Java エクスプロイト、HTML/JavaScript エクスプロイト、およびその他の種類のエクスプロイトとの遭遇回数は、それぞれ 1H16 におけるマルウェアとの全遭遇回数の 0.1% 未満でした。これらのエクスプロイトの詳細については、このセクションの残りの部分を参照してください。

エクスプロイト ファミリ

図 3 では、2016 年上半期に最も頻繁に検出されたエクスプロイト関連のマルウェア ファミリを示しています。

図 3. 1H16 に マイクロソフトのリアルタイムのマルウェア対策製品が最も多く検出し、ブロックしたエクスプロイト ファミリの四半期ごとの遭遇率の傾向 (相対的な蔓延率に応じて色分けしたもの)

エクスプロイト	種類	3Q15	4Q15	1Q16	2Q16
JS/Axpergle	エクスプロイト キット	0.71%	0.92%	0.53%	0.40%
SWF/Netis	Adobe Flash Player	0.00%	0.00%	0.27%	0.00%
CVE-2010-2568 (CplLnk)	オペレーティング システム	0.18%	0.24%	0.13%	0.13%
HTML/Meadgive	エクスプロイト キット	0.07%	0.17%	0.08%	0.10%
JS/NeutrinoEK	エクスプロイト キット	0.01%	0.11%	0.04%	0.10%
HTML/IframeRef	ジェネリック	0.04%	0.05%	0.03%	0.02%
シェルコード	Adobe Flash Player	0.01%	0.03%	0.02%	0.02%
SWF/Dlcypt	Adobe Flash Player	ー	ー	0.01%	0.01%
JS/Anogre	エクスプロイト キット	0.01%	0.01%	0.01%	0.01%
Win32/Pdfjsc	ドキュメント	0.01%	0.01%	0.01%	0.00%

表に示している各脆弱性の合計には、エクスプロイト キットの一部として検出されたエクスプロイトは含まれません。

- 1H16 において、エクスプロイト キットは最も遭遇したエクスプロイトの上位 10 種類のうち 4 種類を占めています。
- SWF/Netis は、感染したコンピューターでファイルをダウンロードして実行するために、Adobe Flash Player の重大な脆弱性 (CVE-2015-5119) を利用します。Adobe は、2015 年 7 月にセキュリティ情報 APSB15-16 を公開し、この問題に対処しました。
- CVE-2010-2568 は、Windows シェルに存在する脆弱性です。他のいくつかのマルウェア ファミリにもこの脆弱性を悪用しようとするものはありますが、Win32/CplLnk ファミリの亜種として検出されることが一般的です。攻撃者は、不正な形式のショートカット ファイルを作成して CVE-2010-2568 を悪用します。このファイルは一般的に、ソーシャル エンジニアリングなどの方法で配布され、脆弱性のあるコンピューターでそのショートカット アイコンが

エクスプローラーに表示されると、悪意のあるファイルが強制的に読み込まれます。この脆弱性は、2010 年半ばにマルウェア ファミリ Win32/Stuxnet での使用が最初に確認されました。それ以降、他のさまざまなファミリで悪用されていますが、その多くはこの脆弱性の露見より前から存在しており、後からこの脆弱性を悪用するように改変されたものです。マイクロソフトは、2010 年 8 月にセキュリティ情報 MS10-046 を公開し、この問題に対処しました。Windows 8 およびそれ以降にリリースされた Windows のバージョンには、CVE-2010-2568 のエクスプロイトに対する脆弱性はありません。

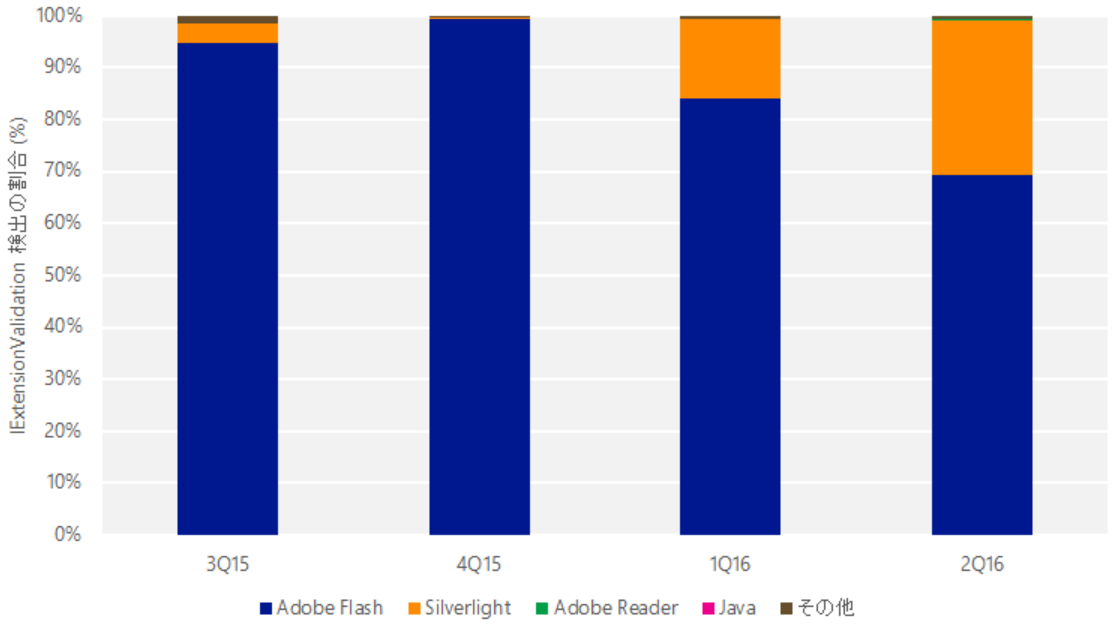
- HTML/IframeRef は、特別に作成された HTML インライン フレーム (IFrame) タグのジェネリックな検出で、有害なコンテンツを含む Web サイトへリダイレクトします。実際のエクスプロイトよりも考えて作られたエクスプロイト ダウンローダーであり、これらの有害なページはさまざまな手法を使用してブラウザーやプラグインの脆弱性を悪用します。唯一の共通点は、攻撃者がインライン フレームを使用してユーザーにエクスプロイトを配布することです。こうしたインライン フレームのいずれかによって配布および検出される実際のエクスプロイトは、頻繁に変更される可能性があります。
- SWF/Dlcypt は、暗号化された JavaScript ファイルを攻撃者が解除して実行するために使用できる Adobe Flash Player ファイルです。サイズが 0 × 0 ピクセルのフレームで実行するように構成されているため、気づかれずに実行できます。

Internet Explorer と IExtensionValidation でのエクスプロイト検出

IExtensionValidation は、Internet Explorer 11 で導入されたリアルタイム セキュリティ ソフトウェアが実装できるインターフェイスであり、ActiveX コントロールが悪意のあるページに読み込まれないようにブロックします (マイクロソフトの最新の Web ブラウザーで Windows 10 の既定のブラウザーである Microsoft Edge は、ActiveX プラグインをまったくサポートしていないため、IExtensionValidation を使用しません)。セキュリティ ソフトウェアが IExtensionValidation を実装している場合、Internet Explorer で ActiveX コントロールを含む Web ページが読み込まれるときに、コントロール自体が読み込まれる前にブラウザーによってセキュリティ ソフトウェアが呼び出され、そのページの HTML とスクリプトの内容がスキャンされます。セキュリティ ソフトウェアは、そのページに悪意があると判断した場合 (たとえば、ページがエクスプロイト キットのランディング ページであると識別した場合など)、Internet Explorer で個々のコントロールまたはページ全体が読み込まれないようにします。

図 4 では、3Q15 から 2Q16 までの四半期ごとに、Internet Explorer 11 において悪意のある Web ページで識別された ActiveX コントロールの種類を示しています。

図 4. IExtensionValidation を通じて悪意のあるページで検出された ActiveX コントロール (3Q15 ～ 2Q16、コントロールの種類ごと)



- Adobe Flash Player オブジェクトは、過去 4 四半期のいずれにおいても、悪意のあるページでホストされるオブジェクトの種類として最も多く検出されたものです。4Q15 に 99.2% に達してからは、2Q16 に 69.3% と減少しています。
- 悪意のある Silverlight オブジェクトをホストするページは、複数のエクスプロイト キットが最近露見した 2 つの Silverlight の脆弱性 CVE-2015-1671 および CVE-2016-0034 のエクスプロイトを追加したため、1H16 に増加しました。マイクロソフトは、2015 年 5 月にセキュリティ情報 MS15-044、2016 年 1 月に MS16-006 をそれぞれ公開し、この脆弱性に対処しました。

マルウェアと望ましくないソフトウェア

マイクロソフトでは、マルウェアと望ましくないソフトウェアの蔓延状況を測定するため、2 種類の指標を使用しています。[2]

- 遭遇率とは、マイクロソフトのリアルタイムのセキュリティ製品を実行しているコンピューターのうち、マルウェアに遭遇したコンピューターの割合です。[3]マイクロソフトへのデータ提供を許可したユーザーのコンピューターだけが、遭遇率のカウント対象となります。
- Computers Cleaned per Mille (CCM) は、感染率を示す指標であり、悪意のあるソフトウェアの削除ツール (MSRT) を実行した一意のコンピューター 1,000 台のうち、実際に駆除が実行されたコンピューターの台数を示すものです。このツールは Microsoft Update サービスを通じて無料で配布されており、200 種類以上の最も広く蔓延した脅威または深刻な脅威をコンピューターから削除します。MSRT はリアルタイムツールではなく、コンピューター内に既に存在している脅威のみを検出して削除するため、感染を未然に防ぐことはできません。

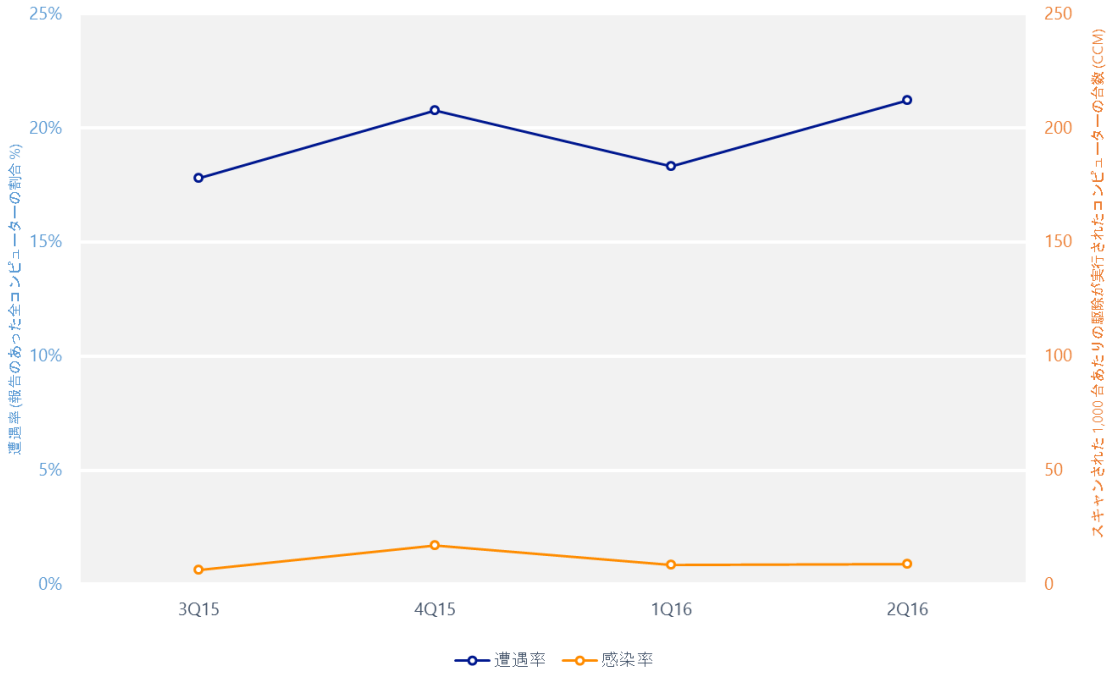
図 5 では、これら 2 種類の指標の違いを示しています。

---

[2] Brantall、Rotbrow、および Filcout ファミリは遭遇率と感染率に含まれていません。詳細については、レポート全文をご参照ください。

[3] マルウェア対策ソフトウェアが検出する前に Web ブラウザーによってブロックされた脅威は遭遇率に含まれません。具体例として、Internet Explorer 11 に実装された IExtensionValidation によってセキュリティ ソフトウェアの機能が拡充されると、エクスプロイトを含むページの読み込みがブロックされます (詳細については、レポート全文をご参照ください)。このため、コンピューターのユーザーが遭遇する脅威のすべてが遭遇率に反映されているわけではありません。

図 5. 四半期ごとの世界全体の遭遇率と感染率 (3Q15 ～ 2Q16)

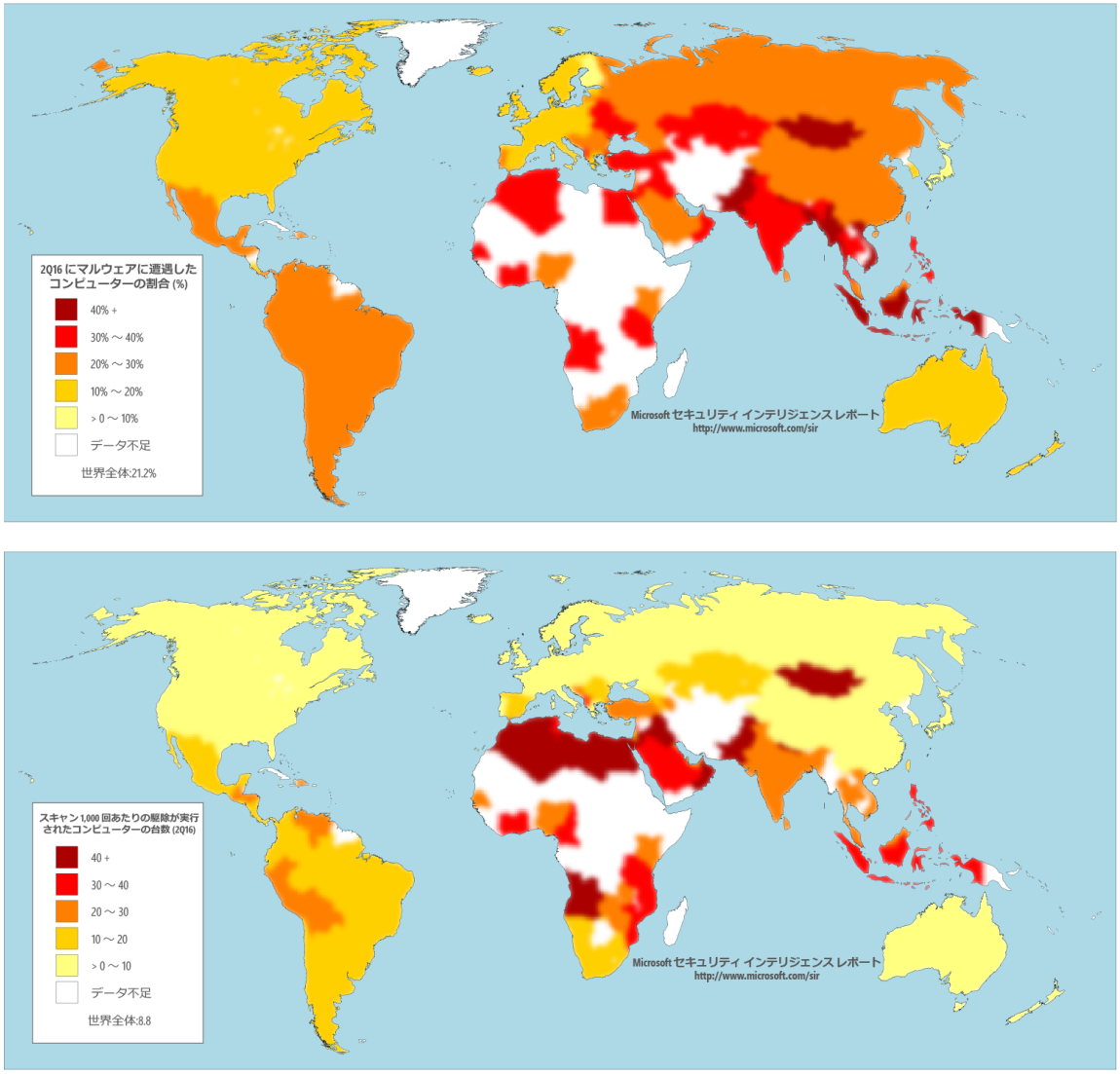


過去 4 四半期において、平均して世界全体で報告のあったコンピューターの約 20.6% が脅威に遭遇しました。それと同時に、MSRT は 1,000 台のうち約 10.1 台 (1.01%) のコンピューターから脅威を削除しました。

世界全体のマルウェアと望ましくないソフトウェア

図 6 では、2Q16 の世界各地での感染率と遭遇率を示しています。

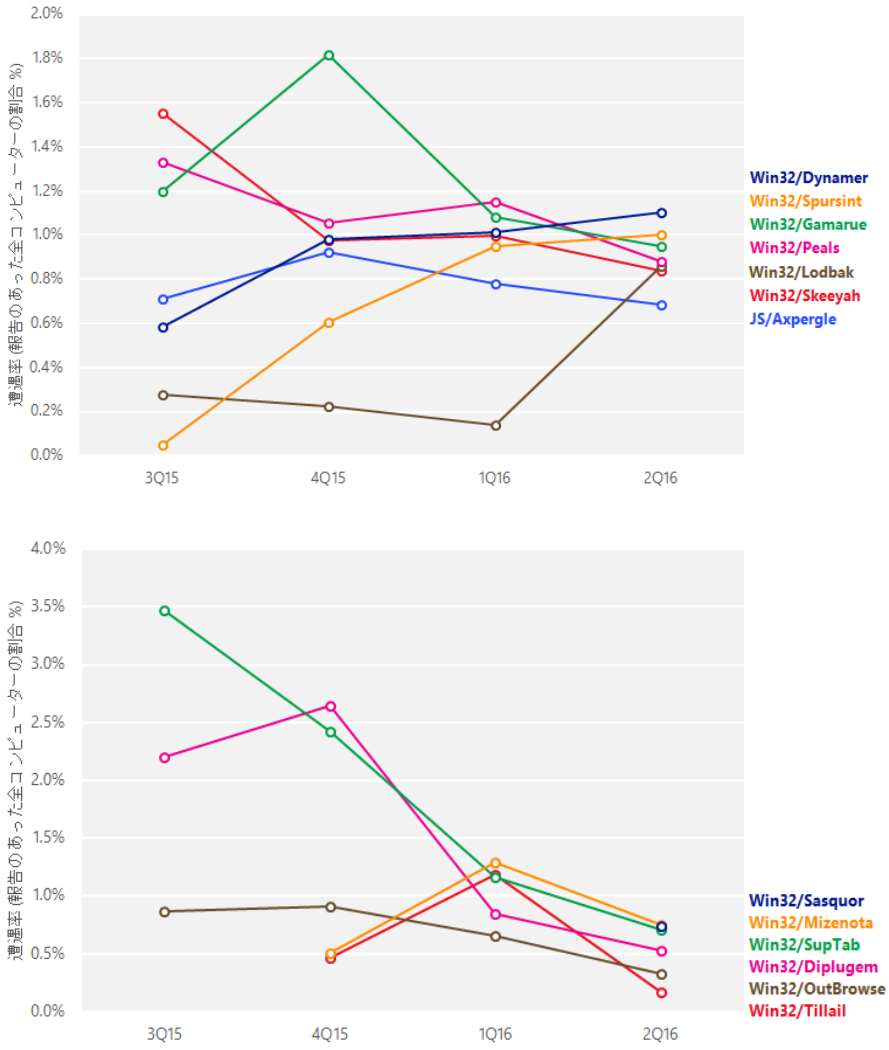
図 6. 国/地域別遭遇率 (上) と感染率 (下) (2Q16)



脅威ファミリ

図 7 は、1H16 にマイクロソフトのリアルタイムのマルウェア対策製品が世界全体で最も多く検出したマルウェアと望ましくないソフトウェア ファミリに関する傾向を示しています。

図 7. さまざまな有名マルウェア ファミリ (上) と望ましくないソフトウェア ファミリ (下) の遭遇率に関する傾向 (1H16)

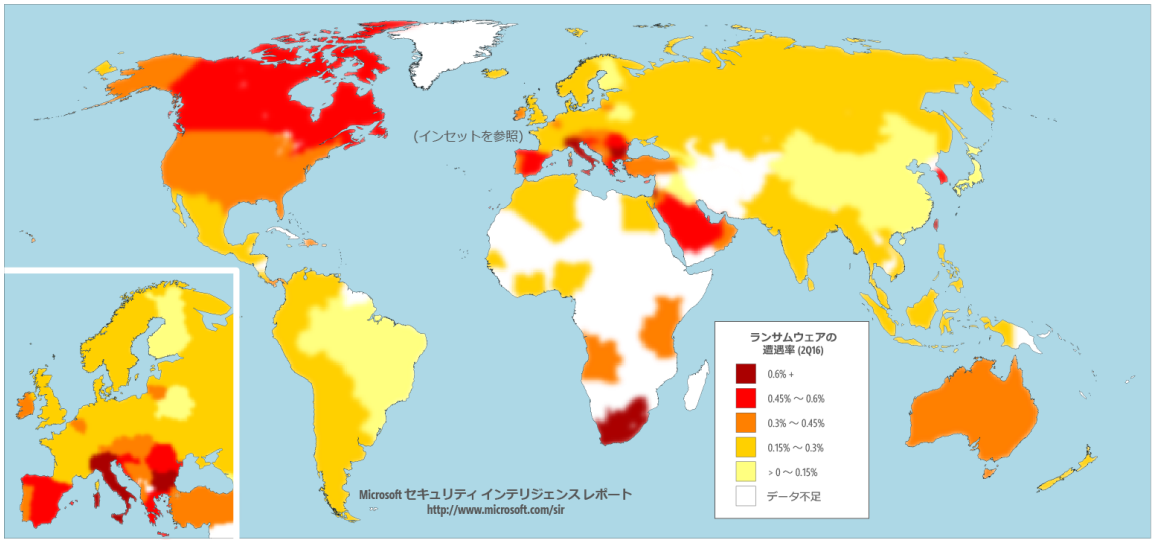


- Win32/Dynamer、Win32/Peals、および Win32/Skeeyah は、いくつかの特徴を共有するさまざまな脅威のジェネリックな検出です。
- 1H16 に最も多く遭遇した非ジェネリックの脅威である Win32/Gamarue は、主にエクスプロイト キットとソーシャル エンジニアリングを介して配布されるワームです。

ランサムウェア

ランサムウェアは、コンピューター ユーザーが攻撃者に一定の金額を支払うなどの行動を取るまで、コンピューターやそのファイルを使用不能にすることを意図して設計された種類のマルウェアです。

図 8. ランサムウェア ファミリの国/地域別遭遇率 (2Q16)

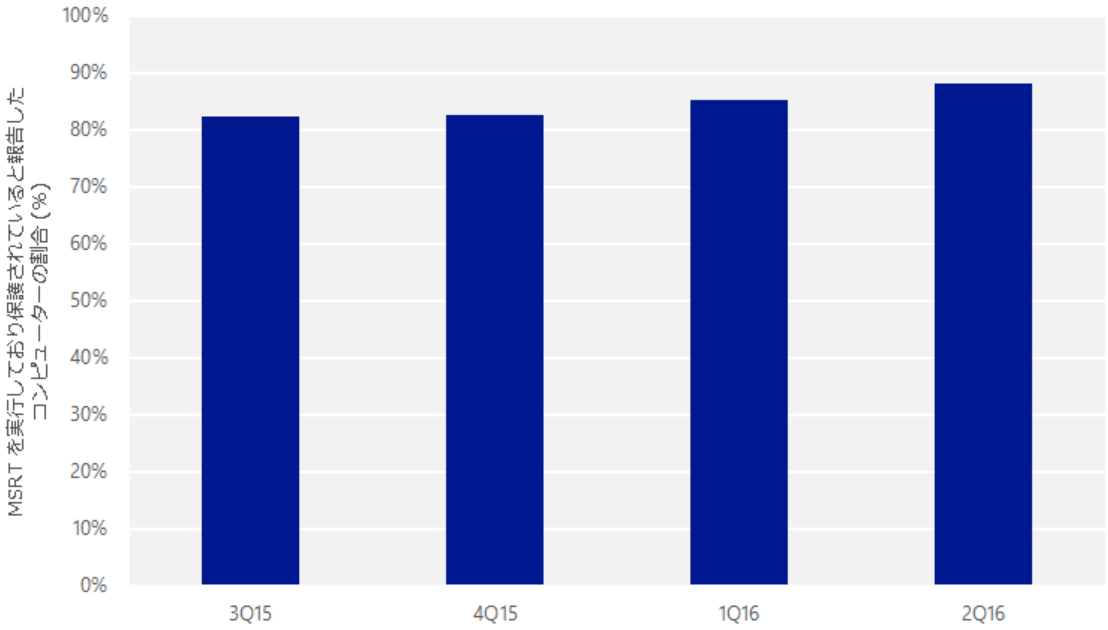


2Q16 にランサムウェアの遭遇率が最も高かった地域はイタリア (0.82%) で、ついでブルガリア (0.74%)、台湾 (0.67%) でした。

セキュリティ ソフトウェアの使用

最近の MSRT のリリースでは、コンピューター上のリアルタイムのマルウェア対策ソフトウェアの状態に関する詳細を収集し、報告しています。図 9 は、2H15 から 1H16 までの四半期ごとに、世界全体のコンピューターのうち、最新のリアルタイム セキュリティ ソフトウェアが実行されていることを MSRT が検出したものの割合を示しています。

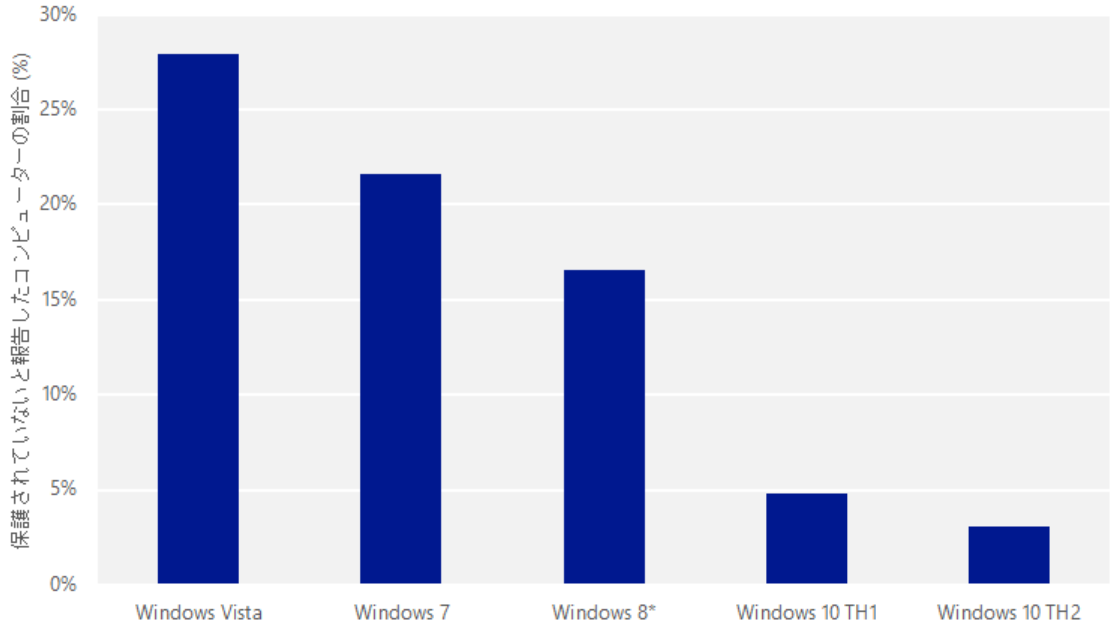
図 9. セキュリティ ソフトウェアが有効になっていると報告したコンピューターの月平均割合 (3Q15 ～ 2Q16)



- 過去 4 四半期のどの期間にも、リアルタイム セキュリティ ソフトウェアが有効になっていると報告したコンピューターの割合は 80% を超えており、2Q16 までに 88% に増加しました。この増加の主な理由は、Windows 10 の採用が伸び、以前のバージョンの Windows に置き換わったことです。Windows 10 には Windows Defender がプレインストールされており、他のセキュリティ ソフトウェアがインストールされていない場合は自動的に有効になります。この機能は、以前のバージョンの Windows にはありませんでした。

図 10 に示すように、保護率はオペレーティング システムによっても異なる場合があります。

図 10. セキュリティ ソフトウェアによるサポート対象の Windows クライアント バージョンの月平均保護状態 (1H16)



* Windows 8.1 を含む

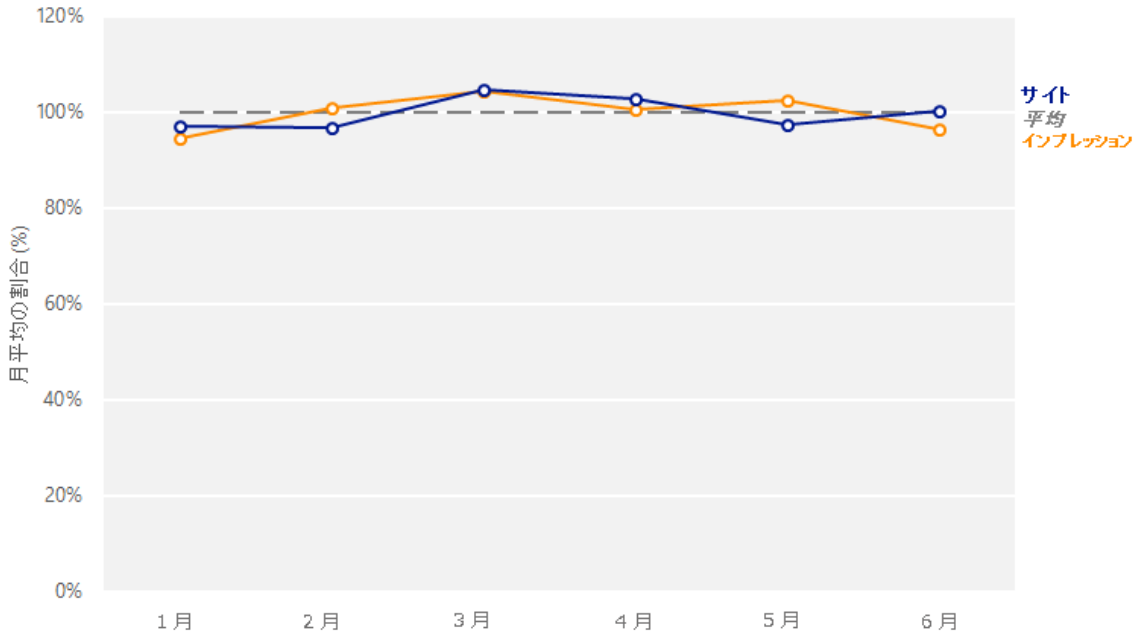
- 一般に、新しいバージョンの Windows を実行しているコンピューターの方が、以前のバージョンを実行しているコンピューターよりも保護されていないと報告することが少ない傾向があります。
- Windows 10 での保護率が高い理由は主に、Windows Defender の動作方法の変更によるものです。Windows 10 ユーザーが特に設定することなくマルウェアから保護されるように、Windows Defender は Windows 10 のインストール時に他のリアルタイム セキュリティ製品がインストールされない場合、自動的に有効になります。一方、Windows 8 や Windows 8.1 ではインストール後数日経ってから有効になります。

悪意のある Web サイト

フィッシング サイト

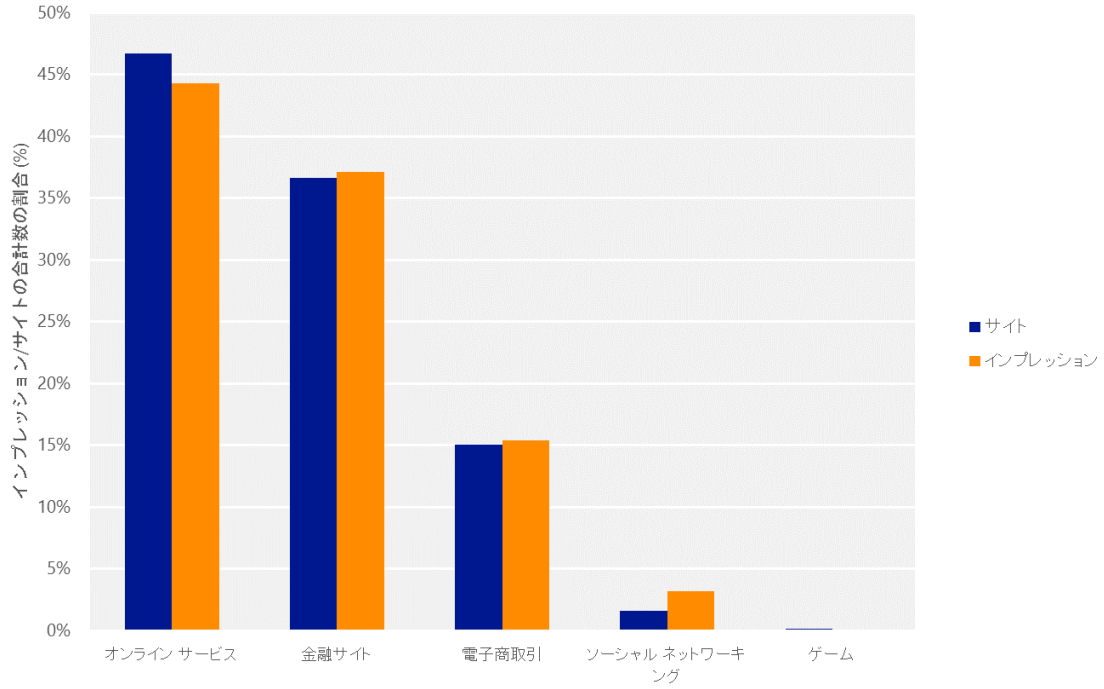
マイクロソフトでは、Microsoft Edge と Internet Explorer の SmartScreen フィルターによって追跡されたフィッシング インプレッションから、フィッシュング サイトとインプレッションの情報を収集します。フィッシング インプレッションとは、SmartScreen フィルターをオンにした状態で 1 つの既知のフィッシング サイトを訪問しようとして警告されたユーザーの単一のインスタンスです。

図 11. SmartScreen フィルターが報告した月別のフィッシング サイトとインプレッションの数 (それぞれの月平均との比較) (1H16)



当該期間中、オンライン サービスを標的としたフィッシング サイトが最も多いインプレッションの割合を占め、アクティブなフィッシング URL の最大数を占めました。

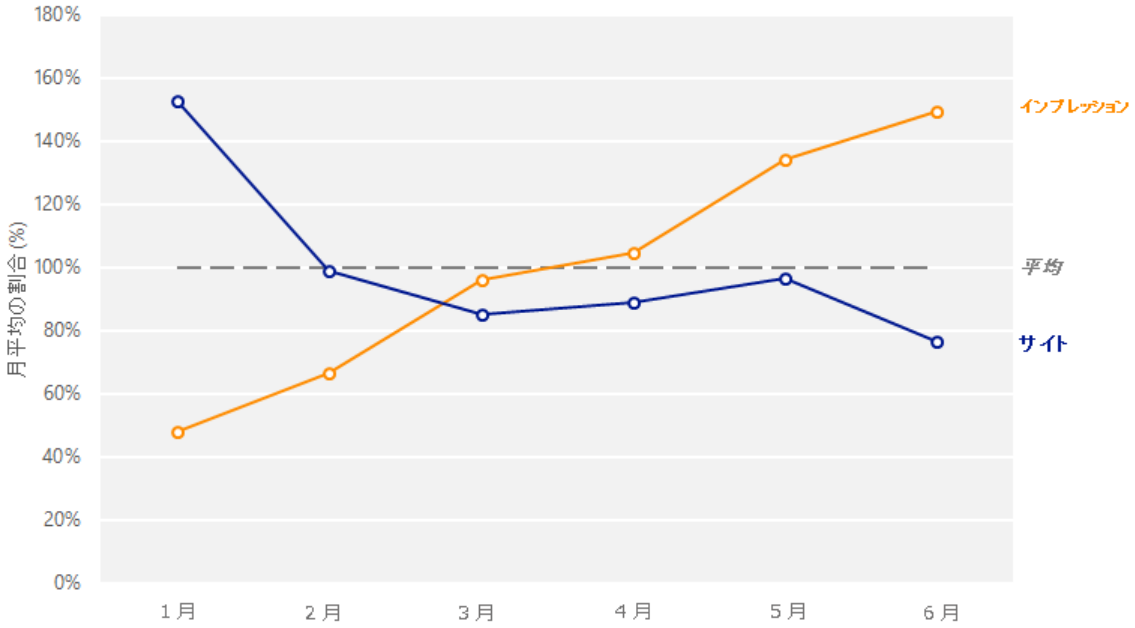
図 12. フィッシング サイトの種類ごとに SmartScreen フィルターが報告したフィッシング サイトとインプレッションの数 (1H16)



マルウェア ホスティング サイト

SmartScreen フィルターは、マルウェアをホストすることで知られるサイトから保護します。図 13 は、月ごとに、Microsoft データベースに登録されたアクティブなマルウェア ホスティング サイトの数を、追跡されたマルウェア インプレッションの数と比較したものです。

図 13. 追跡された月別のマルウェア ホスティング サイトとインプレッションの数 (それぞれの月平均との比較) (1H16)



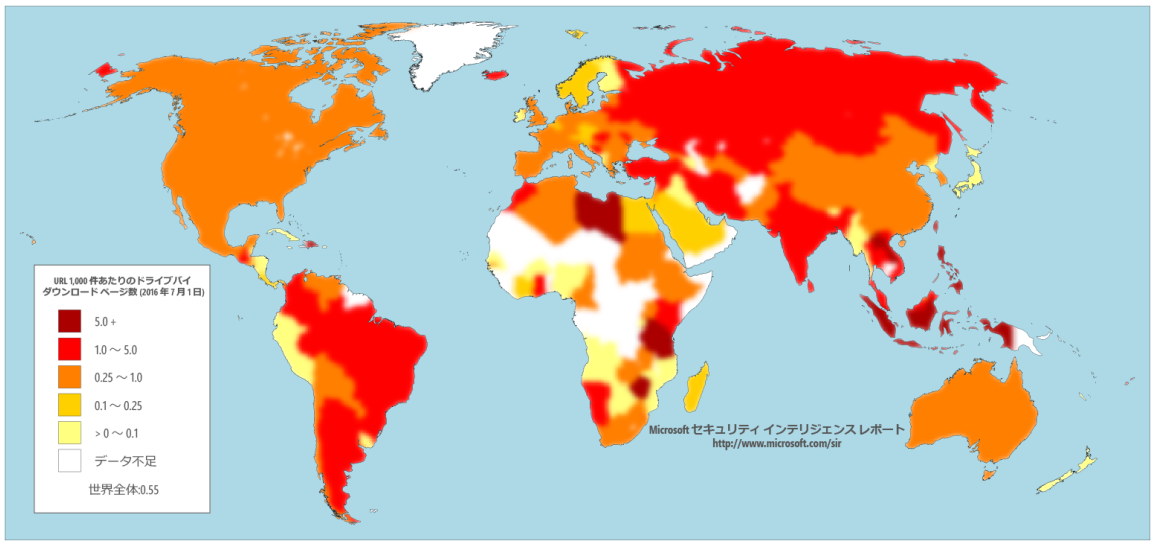
月別のマルウェア インプレッションは、1 月から 6 月の間で 3 倍を上回る伸びを見せました。これは、攻撃者による活発なキャンペーンや SmartScreen フィルターの検出および分類性能の向上など、複数の要因によるものです。2015 年には、MMPC のマルウェア評価基準が詐欺につながったり誤解を招いたりする広告を含めるように更新されました。このような広告は、現在 SmartScreen フィルターでもマルウェアに分類され、ブロックされます。この 1 年で、テクニカル サポートを求めているユーザーにつけこむように設計された広告も出現するなど、この基準を満たす広告の量は増加しています。

ドライブバイ ダウンロード サイト

ドライブバイ ダウンロード サイトとは、Web ブラウザーとブラウザー アドオンの脆弱性を標的とするエクスプロイトを 1 つ以上ホストしている Web サイトのことです。脆弱性のあるコンピューターを使用しているユーザーが、マルウェアが仕込まれた Web サイトにアクセスすると、

ファイルなどをダウンロードしなくても、閲覧しただけで感染してしまうおそれがあります。図 14 では、世界の国や地域を対象に、2Q16 末時点でのドライブバイ ダウンロードの集中率を示しています。

図 14. 2Q16 末に Bing が指標とした各国/地域における 1,000 URL あたりのドライブバイ ダウンロード ページ数



両方の四半期を通じてドライブバイ ダウンロード URL が集中的に存在する場所として、2Q16 末に 1,000 URL あたりの 7.4 ドライブバイ URL が Bing でトラックされた台湾、3.1 のモンゴル、2.6 のイランが挙げられます。

このドキュメントは、レポートの主要な調査結果をまとめたものです。www.microsoft.com/sir から完全版をダウンロードして、より詳細な分析内容をご確認ください。100 以上の国と地域を対象としたセキュリティ データと分析に加え、数々の重要なセキュリティ トピックに関するインテリジェンス レポートも特集されています。