— AUS（アルテミス・ユーザ・サポート）便り 2016/09/20号 —
http://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Microsoft、社内のデバイス約60万台で半年間に41件のマルウェア感染も、多層防御で被害最小に

http://internet.watch.impress.co.jp/docs/news/1019081.html
https://blogs.technet.microsoft.com/jpsecurity/2016/09/07/msit_malware/

このニュースをザックリ言うと･･･

- 9月7日（日本時間）、Microsoft社より、同社内でのデバイス（PC・スマホ等）の利用におけるマルウェアの検出・感染の発生状況および対策等について、同社のブログ記事が発表されました。

- 記事では、100カ国で約15万人の社員が約60万台のデバイスを利用している同社において、2015年下半期には約200万件のウイルスが検出、また41件の感染が確認されたとしています。

- 41件はいずれも、同社のセキュリティソフト「Windows Defender」の定義ファイルで検出されなかったために侵入されたものでしたが、後日アップデートにより検出されたものとのことです。

- 一方で同社では、アンチウイルスソフト等によるマルウェア対策に加え、多数の防御策による「多層防御」を行っており、約60万台のデバイスが稼働する巨大組織であることを鑑み、「セキュリティ対策のゴールは標的型メールの開封率やマルウェア感染率をゼロにすることではない」として、マルウェアを用いる攻撃者にとってのゴール、即ち「セキュリティ侵害による情報漏えい」を可能な限り防ぎ、また、実際に侵害にあった際には被害を最小限にすることにあるとしています。

AUS便りからの所感等

- マイクロソフトが行っている防御策は、侵入検知システムや脆弱性緩和ツールといったものから、「利用するソフトウェアは最新のバージョンを利用し、セキュリティ更新プログラムを適用し、最新の状態に保つ」あるいは「攻撃の糸口となり得る問題を含む技術の利用（Java・Flashなど）の必要性を検討し、利用を最小限にする」といったポリシー的なものまで多岐にわたります。

- 防御策の全てを中小企業等で一通り実施することは難しいでしょうが、それでも、アンチウイルスだけではない、UTMだけでもない、複数の対策の組み合わせにより、一つの対策で遮断できなかった攻撃を別の対策で捕捉できるような体制を作るのが大事であることは、これまで当便りで推奨してきたとおりです。

INTERNET Watch

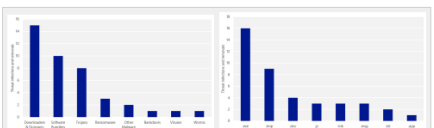
Microsoft、社内のデバイス約60万台で約200万件のウイルスを検出、感染は41件

100%の防御は不可能、感染前提の「多層防御」で被害を最小限に

岩崎 宰守　2016年9月8日 16:19

Microsoftでは、100カ国で約15万人の社員が約60万台のデバイスを利用しているが、2015年下半期には約200万件のウイルスが検出され、41件の感染が確認されたという。Microsoftは7日に日本のセキュリティチーム公式ブログでこれを公表するとともに、対策方法について解説を行っている。

Microsoft社内で検出された約200万件のマルウェアは、マルウェア対策ソフトにより検出され、ブロックされた件数となる。感染した41件は、定義ファイルに反映されていない新種のマルウェアで、後日定義ファイルがアップデートされて発見されたものを指している。



Microsoftの社内ネットワークに接続されたデバイスでは、6日以内の定義ファイルが適用された最新バージョンの「Windows Defender」か、「System Center Endpoint Protection 2012（SCEP）」が稼働している必要があり、月平均で約98%のデバイスがこのポリシーに準拠している。

Microsoft | TechNet

マイクロソフトだってウイルスに感染します

Rate this article

YURIKAM　2016/09/07

こんにちは、村木ゆりかです。

マイクロソフト社では、100 以上の国に約 15 万人の社員が在籍し、社内 IT 環境 (Microsoft IT) では、約 60 万台のデバイスが利用されています。社内 IT 環境では、最先端のソフトウェアや技術が利用されており、物理的にも IT システム的にも最新のセキュリティ対策が施されています。

そんな最新の社内環境ゆえに、「マイクロソフトは、ウイルスになんて感染しないでしょ?」と聞かれることがあります。

いいえ、そんなことはありません。実は、2015 年下半期、社内環境では、約 200 万件のウイルスを検出し、41 件の感染を確認しています。

マイクロソフトのマルウェア感染状況

マイクロソフト社内 IT 環境では、社内ネットワークに接続するすべてのデバイスは、リアルタイム監視が動作しているマルウェア対策ソフト (ウイルス対策ソフト

す。Windows 8 以降に無償

ア対策ソフトとして利用さ

期 (7 月から 12 月) では、

ウイルスをはじめとした悪意

ウェアの検出報告がありま

す。

単に「ゼロ」を目指さないセキュリティ対策

マイクロソフトの社内 IT 環境におけるセキュリティ対策のゴールは、マルウェアが添付されているかもしれない標的型メールの開封率をゼロにしたり、マルウェア対策ソフトの稼働率を 100% にしてウイルス感染率ゼロにしたりすることではありません。

たとえば、2015 年下半期では、月の平均で約 98% のデバイスがマルウェア対策ソフトを最新の状態で稼働させていますが、60 万台を抱える組織で、常に 100% を目指すのは、コストや現実的な運用を鑑みると実現不可能です。ある程度のユーザー (Microsoft IT でいえば 2% ぐらい) は準拠していないデバイスを保持している可能性として認識し、それによるリスクを多層防御により軽減することを目指しています。

攻撃者のゴールは、マルウェアに感染させることではなく、マルウェアなどの方法を利用して、情報を盗み、金銭を得ることにあります。ですから、私たち防御側のゴールも、攻撃者のゴールを達成させない、すなわち、セキュリティ侵害による情報漏えいを可能な限り防ぎ、また、実際に侵害にあった際には被害を最小限にすることにあります。

このためには、マルウェア対策がどの程度効果をなしているのか、基本的な対策をきちんと行うことでの効果を図り、必要な侵入を前提とした対策を計画することが重要です。マイクロソフトでは、マルウェア対策だけに絞ったり、それぞれの対策に画一的な数値目標をもつのではなく、全体的な運用と対策を俯瞰して現実的な目標を見定め、分析をし、定期的に見直しを図ることで、対策をすることが重要だと考えています。

●Microsoft、Windows7上のIE11で古いバージョンのFlash Player等をブロックする方針

http://forest.watch.impress.co.jp/docs/news/1020228.html

このニュースをザックリ言うと・・・

- 9月13日（現地時間）、Microsoft社より、Windows7上のInternet Explorer（IE）11において、古いバージョンのFlash PlayerをはじめとするActiveXコントロールをブロックする方針が発表されました。

- 10月11日（日本時間では12日）に月例のセキュリティパッチ配信とともに有効となる模様で、これにより、現時点での最新バージョンである21.0.0.198より前のバージョンのFlash Playerがインストールされている場合、Flashコンテンツを再生しようとすると警告が出るようになる他、JavaやSilverlightのActiveXコントロールについても同様に、古いバージョンはブロックされます。

- なお、Flash Playerについては、Windows 8.1以降ではWindows Updateによってアップデートされるため、上記のブロック機能は提供されないとのことです。

AUS便りからの所感等


窓の杜
Microsoft、「IE 11」で古いActiveX版「Flash Player」をブロックする方針を明らかに
Windows 7 SP1/Windows Server 2008 R2が対象。10月11日から順次アップデートを配信
椿井 秀人　2016年9月15日 12:30
米Microsoft Corporationは13日（現地時間、以下同）、「Internet Explorer 11」で、古いバージョンのActiveX版「Adobe Flash Player」をブロックする方針を明らかにした。
同社によると、古いバージョンのActiveXコントロールをブロックする機能は10月11日から順次配信されるとのこと。ActiveX版「Adobe Flash Player」の場合は、
- 「Adobe Flash Player」v21.0.0.198以前（v21.0.0.198は含まず。以下同）
- 「Adobe Flash Player」延長サポートリリースv18.0.0.241以前

- ActiveXコントロールや、Firefoxのプラグインで提供されるもので著名なのはやはりFlashであり、毎月のように重大な脆弱性が発見されてはアップデートされるという一面もあります。

- 古いActiveXコントロールのブロック機能自体は2014年9月にリリースされていたものであり、今回はブロックする範囲が拡大されることになるようです（なお、Firefoxにも同様のブロック機能が提供されており、Google Chromeでは最新のFlash Playerを同梱したバージョンを随時リリースしています）。

- 特に最新のバージョンにアップデートしていないソフトウェアはすべからく攻撃者のターゲットとなり得るものと意識し、PCにインストールされているソフトウェアが全て最新に保たれているかも適宜チェックし、そういったソフトウェアへの攻撃を食い止めるため、アンチウイルスやUTMによる防御もまた必要不可欠です。

●MySQLに重大な脆弱性、SQLインジェクションによりサーバ乗っ取りも可能か

http://www.itmedia.co.jp/news/articles/1609/13/news055.html

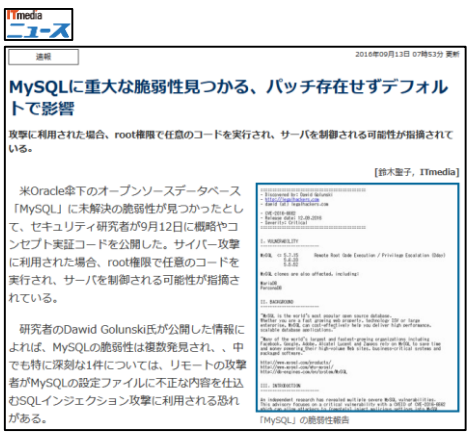
このニュースをザックリ言うと・・・

- 9月12日（現地時間）、Linux等で利用されているオープンソースデータベースソフト「MySQL」に未修正の脆弱性が存在するとして、セキュリティ研究者のDawid Golunski氏により発表がありました。

- 脆弱性は複数存在し、うち1点（CVE-2016-6662）は、リモートの攻撃者がMySQLサーバ上で任意のコードを実行し、サーバを乗っ取ることが可能なものとされています。

- MySQLからフォークした「MariaDB」「PerconaDB」では8月30日にパッチがリリースされていましたが、MySQLについては10月18日にリリース予定の定例パッチで対策予定とのことです。

AUS便りからの所感等


ITmedia ニュース
速報
2016年09月13日 07時53分 更新
MySQLに重大な脆弱性見つかる、パッチ存在せずデフォルトで影響
攻撃に利用された場合、root権限で任意のコードを実行され、サーバを制御される可能性が指摘されている。
[鈴木聖子，ITmedia]
米Oracle傘下のオープンソースデータベース「MySQL」に未解決の脆弱性が見つかったとして、セキュリティ研究者が9月12日に概略やコンセプト実証コードを公開した。サイバー攻撃に利用された場合、root権限で任意のコードを実行され、サーバを制御される可能性が指摘されている。
研究者のDawid Golunski氏が公開した情報によれば、MySQLの脆弱性は複数発見され、、中でも特に深刻な1件については、リモートの攻撃者がMySQLの設定ファイルに不正な内容を仕込むSQLインジェクション攻撃に利用される恐れがある。
「MySQL」の脆弱性概要

- 攻撃者が「MySQLサーバ上の特定の権限を持つユーザとして接続し、任意のSQLリクエストを送信できること」が脆弱性を悪用する条件とされています。

- 通常はMySQLサーバに直接SQLリクエストを送信することは困難と思われますが、WebアプリケーションにSQLインジェクションの脆弱性がある場合はこの限りではなく、脆弱性を悪用される恐れに注意する必要があるでしょう。

- SQLインジェクションは、今回の件に限らずとも危険な脆弱性であり、UTM等でWebアプリケーションファイアウォール（WAF）機能が有効であればある程度防げる場面もあるものの、Webアプリケーション自体の修正が根本的な対策には欠かせません。