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。

●今回の件名は「重要書類」「口座振替払い」等…マルウェア添付メールに注意

http://internet.watch.impress.co.jp/docs/news/1071306.html
https://www.jc3.or.jp/topics/vm_index.html

このニュースをザックリ言うと・・・

- 7月19日（日本時間）、警視庁と日本サイバー犯罪対策センター（JC3）より、ウイルスが添付されたメールが同日より拡散しているとして警告が出されています。

- 警告では以下の2種類のメールが挙げられており、いずれもExcelファイルに偽装したウイルスが添付されているとのことです。

① 件名が「重要書類」、本文が「お世話になります。昨日お話した重要書類です。」で、「(数字).xls」等が添付

② 件名が「口座振替払い」「7.2017」「Fwd:」、本文が「御依頼の登記が完了しましたので、お手数ですが、費用のお振り込みをお願いします。」で始まり、「サービス請求書.xls」や「(数字).xls」が添付

- これらのメールは、国内のオンラインバンキングやクレジットカード利用者を狙うマルウェア「URSNIF(gozi)」への感染を意図したものであるとされています。

AUS便りからの所感等

- 特に今年に入り、このようなウイルス添付メールが様々な件名・文面で拡散していることから、JC3では確認されたウイルス添付メールの件名・添付ファイル名といった特徴をまとめたインデックスページを用意しており、定点観測のための情報源としてこれらのページを随時チェックし、不審なメールが受信された場合に慎重に行動できるようにしましょう。

- もちろん、マルウェアへの感染をたくらむ動きはこれに限るものではなく、いわゆる「標的型攻撃」にも注意が必要であり、ターゲットとなる組織を綿密に調査した上で、その組織向けに違和感のない文面のなりすましメールを送ってくるケースもあります。

- マルウェアへの感染を効果的に防ぐには、そういった攻撃の手口についての知識を得ること、加えて手元のPCにおけるOS・各種ソフトウェア・そしてアンチウイルスのパターンファイルを最新に保ち、かつUTMの設置による水際での不正なメールを遮断することといった多層防御を行うことが肝要です。


INTERNET Watch

件名「重要書類」の添付Excelファイルに注意、ウイルス付きメールの拡散に警視庁が注意呼び掛け

岩崎 宰守　2017年7月19日 16:21

ツイート リスト いいね！268 シェア B! 17 Pocket 38

「重要書類」という件名のウイルス付きメールが拡散中だとして、警視庁サイバー犯罪対策課が19日、警戒を呼び掛けるツイートを発した。添付されているExcelファイルはウイルスだという。

具体的なメールの文面や添付ファイル名などは、一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime
まとめている。これによると、今回
文は「お世話になります。昨日お話
ルは「xxxxxxxxxx.xls」という名前

警視庁サイバーセキュリティ対策本部 @MPD_cybersec フォローする

【サイバー犯罪対策課】
ウイルス付メールが拡散中！件名は「重要書類」。本文は添付書類を開くよう誘導する内容となっていますが、添付されているエクセルファイルはウイルスです。ご注意ください！

2017年Jul19日 15:49

193 86


JC3

ウイルス付メール INDEX版

2017年07月
2017年06月
2017年05月
2017年04月
2017年02月
2017年01月
2016年11月
2016年10月

※青字は右記のランダムな文字列が入ります　A：英字　X：英字または数字　0：数字
※表の枠が表示されていない場合は、ブラウザの再読込(Ctrl+F5等)を行ってください。　最新の具体例はこちら

送信年月日	件　名	添付ファイル	本文
2017/07/19	①口座振替払い ②7.2017 ③Fwd:	0000.2017.xls	本文
2017/07/19	重要書類	xx00000000.xls	本文
2017/07/19	口座振替払い	サービス請求書.xls	本文
2017/07/19	重要書類	0000000000.xls	本文
2017/07/06	請求書を添付	xxx_00000.zip	本文
2017/07/06	請求書を添付	必要書類一覧及び御請求書を.xls	本文
2017/07/06	2017.6支払依頼書	0000000.xls	本文
2017/07/06	①本日、添付の請求書を郵送します ②支払いして下さい ③納付期限	0000000000.xls	本文

●WannaCry/WannaCryptが突いた脆弱性、多くのマシンで放置

http://www.itmedia.co.jp/enterprise/articles/1707/14/news058.html

このニュースをザックリ言うと・・・

- 7月11日（現地時間）、セキュリティ研究者のエラド・エレス氏より、ランサムウェア「WannaCry」等に悪用されている脆弱性が依然修正されていないPCが多く確認されているとして警告が出されています。

- 同氏はWannaCry等に組み込まれる攻撃ツール「EternalBlue」の影響を受けるLAN上のPCを検査するツール「Eternal Blues」を提供しており、2週間の間にこれを用いて検証された133ヶ国800万以上のIPアドレスのうち、SMB（Windowsの共有フォルダ等に関連する機能）が使用するポートがオープンになっていたものが537,000件、また脆弱性があるとされる古いバージョンのSMB（SMBv1）が許可されているものが258,000件、そしてEternalBlueの影響を受けるホストは60,000台に上るとしています。

- 同氏によれば、フランスのあるネットワークで1万台近いホストからなるネットワークのうち2台に脆弱性があったケースも確認されており、たった1台でもネットワーク全体が危機にさらされかねないとして警告しています。

AUS便りからの所感等

- このツールでは使用しているOSまでは検出できませんが、影響を受けるとされるホストの中にはパッチ未適用のものの他に、Windows XP以前を使い続けているものも少なからず存在すると思われます。

- EternalBlueを利用するWannaCryや便乗するマルウェアの登場を受け、国内大手セキュリティベンダーからもネットワーク設定等を検証する無料サービスが提供される等の動きが出ています（AUS便り 2017/6/26号参照）。


ITmedia エンタープライズ

2017年07月14日 10時30分 更新

WannaCryが突いた脆弱性、多くのマシンで放置　無料スキャンツール公開へ

あるネットワークでは、1万台近いホストのうち2台に脆弱性が見つかった。こうしたホストが1台でもあれば、ネットワーク全体が危険にさらされかねない。

[鈴木聖子，ITmedia]

印刷／PDF　79 ツイート　29 いいね！　29 シェア　11 B! Bookmark　34 Pocket　G+　通知

WannaCryやPetya亜種など世界で猛威を振るったマルウェアに利用された脆弱性は、今も世界の多数のエンドポイントで修正されないまま放置されている――。脆弱性スキャンツール「Eternal Blues」を提供しているセキュリティ研究者が、そんな実態を報告した。

- 各ツールやサービスがチェックする範囲はそれぞれ異なる場合がありますので、可能な限り複数のチェックを行った上で、各PCへのパッチの適用、UTMの設置あるいはネットワーク構成の見直し等の検討材料とするのが良いでしょう。

●Javaにリモートからの攻撃許す脆弱性、IPAもアップデート呼び掛け

http://forest.watch.impress.co.jp/docs/news/1071239.html

このニュースをザックリ言うと・・・

- 7月19日（日本時間）、米Oracle社より、Java SE 8（以下Java8）の最新版である「Java SE 8 Update 141」がリリースされました。

- 今回のバージョンでは30件前後の脆弱性が修正されていますが、これらが未修正の場合、悪用されるとリモートからPCを乗っ取られる可能性もある他、既にサポートが終了したJava7やJava6等にも影響するとされています。

- JPCERT/CCやIPAからもアップデートを行うよう呼び掛けられており、JPCERT/CCではPCにあらかじめインストールされているJavaのバージョンに注意するよう警告されている他、IPAからは独自のバージョンチェックツール「MyJVNバージョンチェッカ for .NET」で他のソフトウェアも含めバージョンチェックを行うよう推奨されています。

AUS便りからの所感等

- Webブラウザに組み込まれたJavaプラグインに対し、Webページから不正なJavaアプレットにより攻撃を行う手口が多くみられたこと等から、EdgeやGoogle Chromeのような新しいブラウザではJava等多くのプラグインが読み込まれないようになっています。

- こういう状況を鑑み、攻撃者はより現実的に攻撃しやすいケースに照準を絞ることとなり、例えば、「Flash Player(今も広く使われ続けており、かつJava同様に脆弱性が頻繁に報告されている)をターゲットとする」「依然Javaアプレットの利用が要求される一部官公庁等のサイトのために IEやFirefoxを使うことになるケースを狙う」等が挙げられます。


窓の杜

Oracle、32件の脆弱性を修正した「Java SE 8 Update 141」を公開

うち28件はリモートから認証なしに悪用可能。"CVSS 3.0"の基本値は最大で"9.6"

楢井 秀人　2017年7月19日 13:22

米Oracle Corporationは18日（現地時間、以下同）、「Java Platform, Standard Edition（Java SE）」の最新版「Java SE 8 Update 141」を公開した。現在、公式サイト"java.com"から無償でダウンロード可能。すでにインストール済みの場合は、更新機能を利用してアップデートすることもできる。

今回のアップデートは四半期ごとに実施されるOracle製品の定例セキュリティアップデートの一環で、「Java SE」では新たに発見された32件の脆弱性が修正されている。

「Java SE 8 Update 141」

- 攻撃者の思うつぼにならないようにするには、狙われやすいアプリケーションについて、脆弱性情報・アップデート情報を随時チェックしつつ、確実にアップデートを行い、アップデートがリリースされてから活発化するであろう攻撃、もしくはリリース前に発生するゼロデイ攻撃への対応のため、アンチウイルスとUTMによる防御も重ねて行うことが必要です。