— AUS（アルテミス・ユーザ・サポート）便り 2018/06/04号 —
https://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。

●CSVファイルを開いたら感染？　Excelの「仕様」が話題に

http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00535/
https://security.srad.jp/story/18/06/01/0532257/

このニュースをザックリ言うと･･･

- 5月30日（日本時間）、デジタルメディア「日経 xTECH」において「覆された常識、CSVファイルでウイルス感染」と題した記事が掲載され、話題となっています。

- CSVファイルをExcelで開いた際、セル中にExcelの関数が記載されているとそれをExcelファイルの場合と同様に実行するという「仕様」となっており、攻撃者が不正なマクロを含んだCSVファイルを送り付け、それを開いた相手をマルウェアに感染させる等の可能性が挙げられています。

- 記事によれば2014年の時点でこの攻撃シナリオについての指摘があり、また今年第1四半期（2018年1月～3月）には、サイバー情報共有イニシアティブ（J-CSIP）の参加組織に、不正なCSVファイルが送りつけられる攻撃が実際にあったとのことです。

- なお、グループウェア等で知られるサイボウズ社の2016年のブログ記事によれば、同社はマイクロソフトにこのExcelの仕様について問い合わせたところ、「ユーザがマクロを有効にする必要があることから、本件は脆弱性ではないと判断している」と回答されたとのことです。

AUS便りからの所感等

- この話題に対する議論の中では、テキストファイルだからといって開いても絶対に安全なわけではないという指摘、さらにはテキストエディタでも不正なテキストファイルで脆弱性を突かれる場合もあるという指摘も出てきています。

- いずれにしろ、どういった攻撃が存在するかの情報収集あるいは組織内への啓発を行うことが肝要であり、CSVファイルでもExcelファイル（.xlsx等）と同様、マクロを含むファイルを開いた場合に警告が出るとされることから、そこで不審な点に気付き、確実に対処するようにしてください。

日経 xTECH

2018/05/30 05:00

ニュース解説

覆された常識、CSVファイルでウイルス感染

勝村 幸博＝日経 xTECH/NETWORK

テキストファイル(
識が覆された。テキ
確認されたのだ。CS
ある。CSVファイル

CSVファイルとは、
こと。CSVはComma
イルの中にはテキス

だが、拡張子がtxt
フォルト）でExcelと
ザーが設定変更しな
ブルクリックするな
読み込まれる。

CSVファイルに書かれている内容が単なるテキストなら、それを表示するだけなので害はない。だが、関数などが記述されていると、Excelはそれを読み込んで解釈し、その内容に従って動作する。コマンド（プログラム）を実行する関数を記述することもできる。

このため、Excelがインストールされている環境で細工が施されたCSVファイルを開くと、攻撃者が意図したコマンドを実行させられる恐れがある。

任意のコマンドを実行させられるので、ローカル（CSVファイルを開いたパソコン）にあるプログラムはもちろん、インターネット上のサーバーに置いたウイルスをダウンロードさせて実行させるといったことも可能になる。そのようなコマンドが書かれたCSVファイルが、危険なCSVファイルの正体である。

「CSVファイルを悪用した攻撃が可能であることは、2014年ごろから一部の記事やブログなどで指摘されていた」（情報処理推進機構（IPA）の技術本部 セキュリティセンター 情報セキュリティ技術ラボラトリー伊藤博康 職員）。

この懸念は現実のものとなる。2018年第1四半期（2018年1月～3月）、サイバー攻撃情報を共有する取り組みであるサイバー情報共有イニシアティブ（J-CSIP）の参加組織（企業）に、細工が施された危険なCSVファイルが送られてきたのだ。J-CSIPではIPAをハブとして、重要インフラ事業者など11業界227組織がサイバー攻撃に関する情報を共有して対策に役立てている。

スラド

CSVファイル経由で感染するウイルス（ただしExcel限定）が話題に

ストーリー by hylom 2018年06月01日 15時31分 本題はこれを使った攻撃が観測されたというところだね 部門より

あるAnonymous Coward曰く、

> CSVファイルを開くだけでウイルスに感染するという話が報じられている。
>
> ExcelではExcelの関数が記述されたCSVファイルを開くと、状況によってはその関数を実行する仕組みになっているようだ。そのため、Excelで開いた際に悪意のある処理を実行するようなCSVを意図的に作成できてしまうという。
>
> 開いた時の話で問題があるのはExcelの方であり、またExcelはちゃんと怪しいCSVファイルを開いた時に警告を出すためどちらかというと利用者側の問題のような気もするが、実際にこの手法を使った攻撃が今年第一四半期に行われていたそうだ。
>
> 対策としては、不審なCSVファイルはExcelで開かなければ良いと思われる。

なお、ExcelがCSVファイル内の関数を実行するという問題については以前から指摘されてはいたが、MicrosoftはユーザーがマクロをExcelで有効にする必要があることから脆弱性ではないとしている（2016年のサイボウズエンジニアブログ）。また、「安全なファイル形式」などというものは存在しないという指摘もある（twitterセキュリティネタまとめ）。

31 コメント

セキュリティ　security

●ランサムウェア依然として脅威、「復元したければPUBGを1時間プレイしろ」と要求するものも…ESET発表

http://www.itmedia.co.jp/news/articles/1805/25/news114.html

このニュースをザックリ言うと・・・

- 5月25日（日本時間）、セキュリティソフトウェア「ESET」の販売代理店であるキヤノンITソリューションズ社より、2018年4月期のマルウェアレポートが発表されました。

- レポートでは3つのトピックのうち2つがランサムウェアについてのもので、1つ目はFlash Playerの脆弱性を突いて感染する「GandCrab」が挙げられています。

- 2つ目のランサムウェア「PUBG Ransomware」は、ファイルを暗号化した上で「PUBG」というゲームを1時間プレイするよう指示する脅迫画面を表示するものですが、金銭目的ではなく、画面に表示されるコードを入力することでファイルは復元可能とのことです。

AUS便りからの所感等

- GandCrabが悪用するFlash Playerの脆弱性は2月にリリースされたバージョン28.0.0.161で修正済み（6/1時点の最新バージョンは29.0.0.171）であり、通常の設定であれば自動更新されているはずです。

- PUBG Ransomwareの方はその分析結果から、全くの冗談目的に作成されたと推測されていますが、「他のランサムウェアと同様に、個人の大事な情報資産(画像や音楽、書類など)が、勝手に暗号化される」ことや「ファイルも正しく復元されないケースがある」こと、さらには「他の攻撃者がコードを流用して悪用する」可能性を指摘しています。

- 一時期大きく騒がれたことから年月が経っていますが、決してその脅威がなくなったわけではなく、アンチウイルスとUTMによる防御、そして随時の適切なデータバックアップを心がけるよう改めて認識してください。

●データベース経由サイバー攻撃注意…警察庁、「Redis」など4システムで警告

http://www.risktaisaku.com/articles/-/6310

このニュースをザックリ言うと・・・

- 5月21日（日本時間）、警察庁より、インターネット定点観測システムの結果などをもとにしたサーバ攻撃の兆候についての注意喚起が発表されました。

- 発表によれば、3月下旬以降、データベースシステム「Redis」のサーバが使用するTCPポート6379番の検索が急増しており、Redisサーバをマルウェアに感染させようとする攻撃の一環と推測されています。

- この他、Webアプリケーションサーバ「WebLogic Server」、CMS「Drupal」およびCisco機器の管理ツール「Cisco Smart Install Client」への攻撃の兆候が見られるとして、これらについても注意喚起が出されています。

AUS便りからの所感等

- 発表では、Redisを内部から、あるいは外部の必要なクライアントからのみアクセスできるようアクセス制限を行うことを呼び掛けています。

- WebLogic ServerおよびCisco Smart Install Clientともども、使用するポートへの想定外のアクセスに注意し、サーバ自体、あるいはその前面においてファイアウォールによるフィルタリングを行うことは必須です。

- DrupalはWordPressと同様のWebサイトコンテンツ管理システムとして人気がある一方、やはりこちらも脆弱性が頻繁に報告され、攻撃者に悪用されることが多く、コンテンツの改ざん等が行われないよう、セキュリティパッチの適用は欠かさず行い、可能であればやはりサーバ自体等にWAFを導入して攻撃パターンを遮断することを推奨致します。