

覆された常識、CSV ファイルでのウイルス感染

【報告内容】

テキストファイルは開いても安全との常識を覆すウイルスが発生し出した。その一つがCSV形式のでのウイルスです。CSV ファイルを開いただけでウイルス（マルウェア）に感染する恐れがあります。CSV ファイルも危ないファイル形式の一つだと認識すべきです。注意して下さい。

CSV ファイルとは、表の要素などをカンマや改行を使って記述したテキストファイルのこと。CSV は Comma Separated Value の略である。ファイルの拡張子は csv。CSV ファイルの中にはテキストの情報しかない。CSV データ例) 123,234,345,999,AAA,危険,.....

CSV ファイルの問題点は、初期設定（デフォルト）で Excel と関連付けられている点です。Excel をインストールした時にユーザーが設定変更しなければ、CSV ファイルが関連付けられてしまい、CSV ファイルを開こうとすると Excel が起動される様になります。つまり、CSV ファイルをダブルクリックするなどして開こうとする事で Excel が起動され、その CSV ファイルの内容を読み込まれます。

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在りません。しかしながら、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します。コマンド（プログラム）を実行する関数を記述することも出来るのです。従って、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ります。

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ります。そのようなコマンドが書かれた CSV ファイルが、危険な CSV ファイルの正体なのです。

情報処理推進機構（IPA）の報告では、「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」との事です。その懸念は現実のものとなりました。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来たのです。

【対策は、「無効」にする事】

実際の攻撃に使われ始めた CSV ファイルが今後悪用される可能性は非常に高いと思われます。

問題は、以下の様に一般的なウイルス対策は通用しない事です。

- CSV ファイルはテキストファイルなので、それ自体には悪質なプログラムは仕込まれていません。従って、ウイルス対策ソフトでの検知するのは難しいのです。
- CSV ファイルに書かれている関数を解釈して実行する事自体は、Excel の挙動は仕様に従ったものです。脆弱性ではありません。従って、修正プログラム (パッチ) をきちんと適用していても防げないのです。

しかしながら、対策はあります。Excel は CSV ファイルに記述されたコマンドなどを実行する前に、Excel は警告ダイアログを表示します。ここで「無効にする」を選択すればコマンドなどは実行されません。



危険な CSV ファイルを Excel で開いた際に表示される警告ダイアログ (出所: IPA)

初期設定では「無効にする」が指定されていますので、警告ダイアログが表示された際に **Enter** キーを押せば無効になります。従って、警告ダイアログが表示されたら、「無効にする」が指定された状態で **Enter** キーを押すことが、CSV ファイルを使った攻撃の対策になります。

逆に、「有効にする」を選択した場合には、コマンドが実行され、バックグラウンドでウイルスがダウンロードおよび実行されることになります。実際は、「有効にする」をクリックしてもすぐにはコマンドなどが実行されずに、別の警告ダイアログが表示されることが多いです。警告メッセージに関しては、必ず注意を払う様にして下さい。

以上

上記は、皆様にご注意頂きたい事項として記載させて頂きました。
ご参考にして頂ければ幸いです。

SWM (Support to Worlds Member)

《夢ある明日を貴方と共に》

情報作成／システム教育サポート

代表 石川光信

Tel/FAX: 042-422-0593

Mail : mishikawa@wswm.jp

<https://www.wswm.jp>