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。

●ダウンロードフォルダーからのインストールは危険…JVNが注意喚起

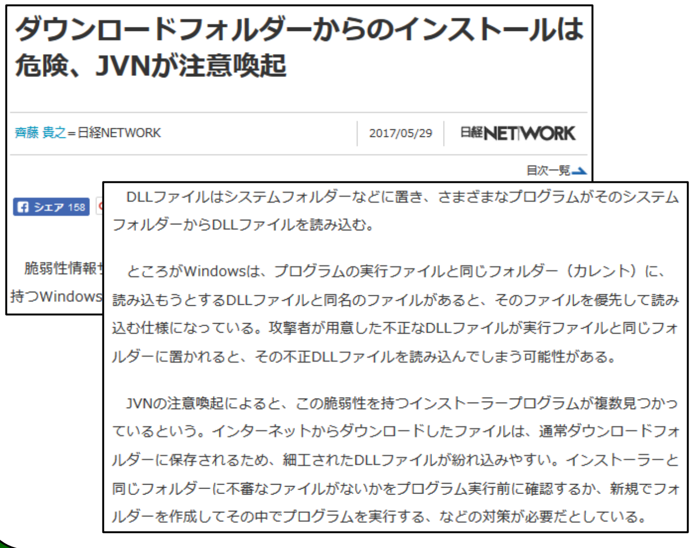
http://itpro.nikkeibp.co.jp/atcl/news/17/052601516/
https://jvn.jp/ta/JVNTA91240916/

このニュースをザックリ言うと…

- 5月25日（日本時間）、IPA（独立行政法人情報処理推進機構）とJPCERT/CC（JPCERT コーディネーションセンター）が運営する脆弱性情報サイト「JVN」より、Windows上における、いわゆる「DLLインジェクション攻撃」の可能性について注意喚起が出されています。
- DLLインジェクション攻撃とは、あるプログラムがDLL(動的ライブラリ)ファイルを読み込もうとする際、不正なDLLファイルを読み込ませるよう誘導し、不正な動作を行うよう仕向ける攻撃で、今回JVNでは、あるプログラムと同じフォルダーに不正なDLLファイルが置かれることによるDLLインジェクション攻撃のケースについて注意喚起をしています。
- この攻撃の影響を受けるとみられるインストーラープログラムが複数確認されており、Windowsの「ダウンロード」フォルダーに保存されたインストーラーを実行しようとするケースを狙い、そこに不正なDLLファイルを置くことが攻撃の一例として挙げられています。
- JVNでは回避策として、当該フォルダーに不審なDLLファイルがないか確認することや、新規にフォルダーを作成しそこでインストーラーを実行することが推奨されています。

AUS便りからの所感等

- DLLは複数のプログラムが共通の処理を行う等の目的で利用され、特にWindowsでは、システムが提供しないDLLファイルをアプリケーションに同梱することも珍しくありません。
- 今回指摘された攻撃ケースは、「プログラムが読み込もうとするDLLファイルと同じ名前のDLLファイルをプログラムと同じフォルダーに置いた場合、そちらが優先して読み込まれる」というWindowsの仕様と「ダウンロードフォルダー上にインストーラープログラムを保存してそのまま実行する」というユーザの行動を想定しています。
- ダウンロードフォルダー（およびデスクトップ）に不正なDLLファイルがないかアンチウイルスでスキャンする等も有用ですが、日頃からそれらのフォルダーの整理を行っておくことも不審なファイルが紛れ込んで見分けづらくなるという事態を防ぐ意味でも重要です。



ダウンロードフォルダーからのインストールは危険、JVNが注意喚起

齊藤 貴之＝日経NETWORK　2017/05/29　日経NETWORK

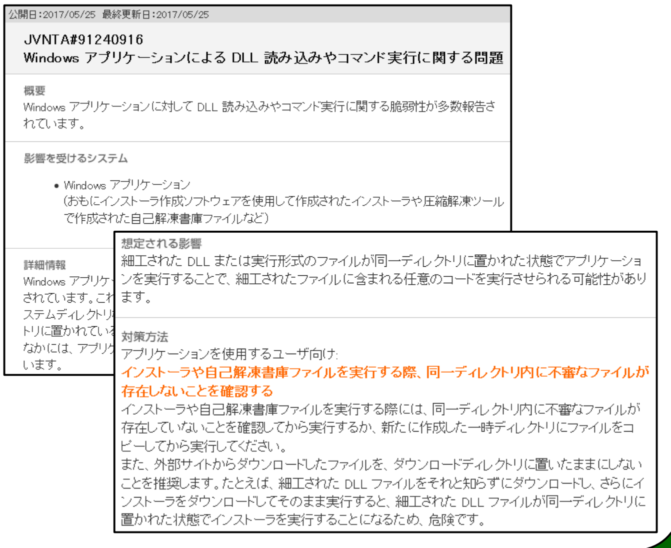
目次一覧

シェア 158

DLLファイルはシステムフォルダーなどに置き、さまざまなプログラムがそのシステムフォルダーからDLLファイルを読み込む。

ところがWindowsは、プログラムの実行ファイルと同じフォルダー（カレント）に、読み込もうとするDLLファイルと同名のファイルがあると、そのファイルを優先して読み込む仕様になっている。攻撃者が用意した不正なDLLファイルが実行ファイルと同じフォルダーに置かれると、その不正DLLファイルを読み込んでしまう可能性がある。

JVNの注意喚起によると、この脆弱性を持つインストーラープログラムが複数見つかっているという。インターネットからダウンロードしたファイルは、通常ダウンロードフォルダーに保存されるため、細工されたDLLファイルが紛れ込みやすい。インストーラーと同じフォルダーに不審なファイルがないかをプログラム実行前に確認するか、新規でフォルダーを作成してその中でプログラムを実行する、などの対策が必要だとしている。



公開日：2017/05/25　最終更新日：2017/05/25

JVNTA#91240916
Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題

概要
Windows アプリケーションに対して DLL 読み込みやコマンド実行に関する脆弱性が多数報告されています。

影響を受けるシステム
- Windows アプリケーション
（おもにインストーラ作成ソフトウェアを使用して作成されたインストーラや圧縮解凍ツールで作成された自己解凍書庫ファイルなど）

詳細情報

想定される影響
細工された DLL または実行形式のファイルが同一ディレクトリに置かれた状態でアプリケーションを実行することで、細工されたファイルに含まれる任意のコードを実行させられる可能性があります。

対策方法
アプリケーションを使用するユーザ向け:
インストーラや自己解凍書庫ファイルを実行する際、同一ディレクトリ内に不審なファイルが存在しないことを確認する
インストーラや自己解凍書庫ファイルを実行する際には、同一ディレクトリ内に不審なファイルが存在していないことを確認してから実行するか、新たに作成した一時ディレクトリにファイルをコピーしてから実行してください。
また、外部サイトからダウンロードしたファイルを、ダウンロードディレクトリに置いたままにしないことを推奨します。たとえば、細工された DLL ファイルをそれと知らずにダウンロードし、さらにインストーラをダウンロードしてそのまま実行すると、細工された DLL ファイルが同一ディレクトリに置かれた状態でインストーラを実行することになるため、危険です。

●不正なリンク指定でWindowsをクラッシュ可能な脆弱性

https://japan.zdnet.com/article/35101928/

このニュースをザックリ言うと・・・

- 5月22日（現地時間）、ロシアのセキュリティ研究者により、Windows 8.1以前にOSのクラッシュに繋がる脆弱性が存在することが発表されました。

- 発表によれば、脆弱性はWindowsで通常利用されるNTFSファイルシステムに存在するもので、ディスク上の特定の場所を不正な形式で指定することにより、OSの動作が遅くなる、プログラムが実行できなくなる、さらにはブルースクリーンが発生する等の症状が発生する模様です。

- この脆弱性を悪用した攻撃はWeb上からでも可能で、ローカル上のファイルを指定する不正なimgタグ等を含むHTMLファイルを開くだけで影響を受けるとされています。

- 影響を受けるOSはWindows Vista・7・8.1とされており、一方で、Windows10では影響は受けないとされています。


ZDNet Japan

旧「Windows」をクラッシュさせるNTFSのバグが発覚

Steven J. Vaughan-Nichols (Special to ZDNet.com) 翻訳校正：編集部 2017年05月30日 10時10分

いいね！ 241　ツイート　G+1 20　B! 35　Pocket 119

印刷　メール　ダウンロード　クリップ

ロシアのある研究者が、過去の「Windows」製品に潜んでいた脆弱性を発見した。NTFSファイルシステムを実装した際に生じたこの単純なバグにより、「Windows Vista」から
なるのだという。

NTFSではファイルシス
「$MFT」という名称のフ
この$MFTをディレクトリ
のファイルアクセスがブロ
には「死のブルースクリー
ステムがクラッシュしたり

ただ、「Google Chrome」ブラウザの場合、不正な形式のディレクトリパスによる画像のロードは抑止されるため、こうした攻撃は無効化される。

残念ながら「Internet Explorer」と「Firefox」は、このようなファイルのロードを許すため、こうした攻撃の影響を受けるとみられている。

ただ、悪い話ばかりではない。まず、「Windows 10」はこの攻撃の影響を受けない。また、（手放しで良い話とは言えないが）この攻撃ではシステムをクラッシュさせることしかできない。つまり、この脆弱性を悪用して、「WannaCry」のようなランサムウェアや、その他のマルウェアをWindowsシステムに持ち込むのは（現状では）不可能だ。

この問題に対処するパッチは現時点では提供されていない。

AUS便りからの所感等

- かつてWindows 9x系では「concon クラッシャー」等と呼ばれるOSをクラッシュさせるバグが存在し、これもimgタグ等から悪用することが可能だったもので、今回の脆弱性はその再来とも呼ばれています。

- この問題に対処するパッチは現時点では提供されておらず、早ければ月例のセキュリティパッチで修正されるとみられますが、WebページやHTMLメールからの攻撃を食い止めるために、Webブラウザやアンチウイルス・UTMにおいても対応されることを期待したいものです。

●偽「WannaCry」対策アプリがGoogle Playストアに

http://internet.watch.impress.co.jp/docs/news/1061779.html

このニュースをザックリ言うと・・・

- 5月26日（日本時間）、大手セキュリティベンダーのマカフィー社より、ランサムウェア「WannaCry（WannaCrypt）」の対策アプリと称する不審なAndroidアプリが確認されたとして注意喚起が出されています。

- 警告では、Android公式のアプリストア「Google Play」において確認されたアプリとして「WannaCry Ransomware Protection」および「Anti WannaCry Virus？Android」が挙げられておりますが、例えば前者は広告収入を得るための別のアプリのインストールを促すもので、総じてこれらには「悪質なコード」は含まれていないとのことです。

- 同社ではGoogleにこれらのアプリを削除するよう要請し、現在は削除されている模様ですが、同社ではこういった不審なアプリについて、トレンドに便乗してマルウェアを配布しようとするサイバー犯罪者の画策としています。

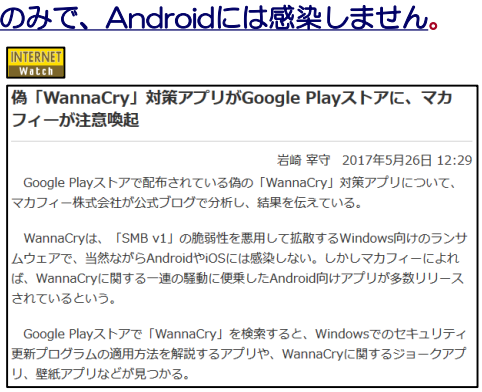
- なお、現在確認されている限り、WannaCryが感染するのはWindowsのみで、Androidには感染しません。

AUS便りからの所感等

- Google Playで「WannaCry」等で検索して出てくる結果としては、他にも「Windowsへのパッチの適用方法を解説するアプリ」やジョークアプリ、壁紙があるようですが、一見安全に見えるそういったアプリにもマルウェアが仕込まれることは十分に考えられます。

- インストールしたアプリが不自然に多くの権限を要求するようであれば十分に注意が必要ですが、そもそも、セキュリティ面から鑑みてもアプリのインストールは必要最低限とすべきです。

- 最低限、Google Play上のレビューのみならずネット上のあらゆる評判から判断しつつ、セキュリティベンダーが提供するアンチウイルスアプリ等を導入するのが良いでしょう。


INTERNET Watch

偽「WannaCry」対策アプリがGoogle Playストアに、マカフィーが注意喚起

岩崎 宰守　2017年5月26日 12:29

Google Playストアで配布されている偽の「WannaCry」対策アプリについて、マカフィー株式会社が公式ブログで分析し、結果を伝えている。

WannaCryは、「SMB v1」の脆弱性を悪用して拡散するWindows向けのランサムウェアで、当然ながらAndroidやiOSには感染しない。しかしマカフィーによれば、WannaCryに関する一連の騒動に便乗したAndroid向けアプリが多数リリースされているという。

Google Playストアで「WannaCry」を検索すると、Windowsでのセキュリティ更新プログラムの適用方法を解説するアプリや、WannaCryに関するジョークアプリ、壁紙アプリなどが見つかる。