— AUS（アルテミス・ユーザ・サポート）便り 2018/03/19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。

●件名「■【重要】」「Re: 」「Re: 発注書」等のウイルスメール拡散

https://twitter.com/nisc_forecast/status/971188928731475969
https://www.jc3.or.jp/topics/vm_index.html

このニュースをザックリ言うと・・・

- 3月13日から15日（日本時間）にかけて、警視庁や内閣サイバーセキュリティセンターおよび日本サイバー犯罪対策センター（JC3）より、Excelファイルに偽装したウイルスが添付されたメールの拡散について警告が出されています。

- 今回様々なメールが確認されており、一例を以下に挙げます。

◆3月13日に送信されたメール：
件名「■【重要】」、本文が「※【注】請求書の画面表示をされましたら必ず印刷もしくはデータ保存をお願い致します。」で始まり、添付ファイル名「0000_2018_000.xls」等。

◆3月13日に送信されたメール：
件名が「Fwd:」「Re:」「Fw:」等、本文が「お支払明細を添付致しましたので漏れ等ないかご確認下さい。」または「請求書です。」、添付ファイル名「00000.[ユーザー名].0.xls」等。

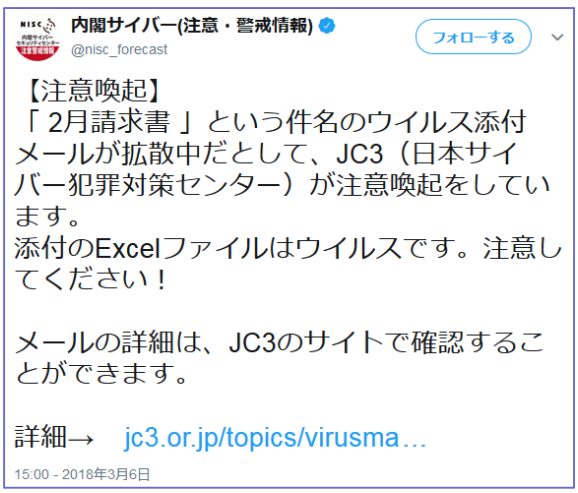
◆3月13・14日に送信されたメール：
件名に「Re: 2月度発注書送付」を含み、本文が「いつも大変お世話になっております。3月度の発注書を添付資料にてお送りさせていただきます。」で始まり、添付ファイル名「00000.[ユーザー名].0.xls」等。

◆3月15日に送信されたメール：
件名が「Re: 発注書」「Fwd: 発注書」「発注書」等、本文が「お世話になっております。発注書をお送り致します。」で始まり、添付ファイル名「発注書_(ユーザー名).xls」「000_発注書_(ユーザー名).xls」等。

AUS便りからの所感等

- 先週に引き続き、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、さまざまな件名や文面でのメールが拡散しており、また、Apple IDを詐取しようとするフィッシングメールも確認されています。

- JC3のサイトではこういった情報が随時更新されていますので、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備えるとともに、OS・各種ソフトウェア・アンチウイルスのパターンファイルを最新に保つ、UTMを設置する等の多層防御を確実に行うようにしましょう。



●仮想通貨の採掘を秘密裏に行うツールをバンドルした「oCam」を窓の杜で収録中止

https://forest.watch.impress.co.jp/docs/news/1111067.html

このニュースをザックリ言うと・・・

- 3月12日（日本時間）、Windows向けソフトウェアライブラリ等を提供する「窓の杜」より、ライブラリに収録していた動画キャプチャーソフト「oCam」が仮想通貨を密かに採掘するツール「BRTSvc」をバンドルしていたとして収録を中止したと発表されました。

- oCam バージョン430のインストール時にBRTSvcを同時にインストールするチェックボックスが表示され、チェックを外さないとそのままインストールされる仕組みになっており、またoCamをアンインストールしてもBRTSvcは同時にアンインストールされない（別途指定してのアンインストールが必要）とのことです。

- 窓の杜では、ユーザが意図せずインストールしてしまった後にその存在を認識することが困難であり、CPUパワーの占有、スリープへの移行の妨害、バッテリー等のリソースを消費し続けることを理由に、BRTSvcを悪質なツールだと判断し、これをバンドルしていたoCamの収録も1月26日に中止しています。

AUS便りからの所感等

- 名の知れたソフトウェアにおいても、アドウェア（広告ウェア）がバンドルされ、同時にインストールされる仕組みになっているものは昔から珍しくありませんし、アドウェアの種類もリスクの高低は様々です。

- そういったアドウェアのインストールを回避し、本来のソフトウェアのみを安全にインストールする方法もネット上で解説されていることが多いので、事前に調査することは重要でしょう。

- また今後、バンドルされたソフトウェアがアンチウイルスやUTMのスキャンでマルウェアと扱われれば、元のソフトウェアもインストールできなくなるでしょう。


窓の杜
WINDOWS FOREST

仮想通貨の採掘を秘密裏に行うツールをバンドルした「oCam」を窓の杜で収録中止

ユーザーインターフェイスを一切表示せずマイニングを実行し、CPUパワーを占有

長谷川 正太郎　2018年3月12日 16:06

ツイート リスト いいね！187 シェア B!140 Pocket 132

窓の杜ライブラリに収録していた動画キャプチャーソフト「oCam」をインストールすると、仮想通貨を採掘（マイニング）するツール「BRTSvc」も併せてインストールされます。窓の杜では1月26日に「oCam」のライブラリ収録を中止すると同時に、開発元であるOhsoftに対して事実の確認と影響の調査を実施しておりました。その結果、「BRTSvc」はユーザーにとって悪影響を与えると判断しました。

「oCam」

●ViX等、開発者に連絡が取れないソフトウェアの脆弱性、JVN発表

https://forest.watch.impress.co.jp/docs/news/1111312.html
http://jvn.jp/report/index.html

このニュースをザックリ言うと・・・

- 3月13日（日本時間）、情報処理推進機構（IPA）およびJPCERT/CCが運営する脆弱性情報ポータルサイト「JVN」より、開発が停止し、開発者に連絡が取れないソフトウェア6種類の脆弱性として計9件が発表されました。

- 一例として、画像ビューワー「ViX」には画像ファイルと同じフォルダに存在する特定のDLLを誤って読み込んでしまう脆弱性があり、PC上で任意のコードを実行される可能性があるとされています。

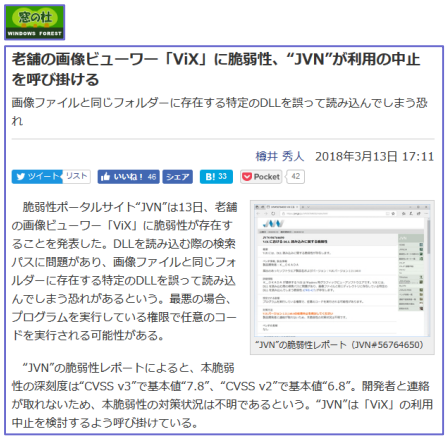
- JVNでは、こういったソフトウェアについて使用を停止するよう呼びかけています。

AUS便りからの所感等

- 不正なDLL読み込みに関する脆弱性は、2017年にJVNが注意喚起を行っており（AUS便り 2017/06/05号参照）、以後も多くのソフトウェアで発見・対策されてきました。

- 一般的にはインストーラー実行時に同じフォルダにDLLがある場合が想定されていた一方で、ViXについてはより広い範囲での危険性が考えられる模様です。

- アンチウイルスやUTMにより、古いソフトウェアに対し攻撃を仕掛けるようなマルウェアや不正なDLLを可能な限り遮断するとともに、アップデートがあるソフトウェアは必ず最新に保ち、そうでなく脆弱性が確認されているようなソフトウェアについては、もし使用し続けるにしても慎重に取り扱うようにしましょう。


窓の杜
WINDOWS FOREST

老舗の画像ビューワー「ViX」に脆弱性、“JVN”が利用の中止を呼び掛ける

画像ファイルと同じフォルダーに存在する特定のDLLを誤って読み込んでしまう恐れ

楢井 秀人　2018年3月13日 17:11

ツイート リスト いいね！46 シェア B!33 Pocket 42

脆弱性ポータルサイト“JVN”は13日、老舗の画像ビューワー「ViX」に脆弱性が存在することを発表した。DLLを読み込む際の検索パスに問題があり、画像ファイルと同じフォルダーに存在する特定のDLLを誤って読み込んでしまう恐れがあるという。最悪の場合、プログラムを実行している権限で任意のコードを実行される可能性がある。

“JVN”の脆弱性レポート（JVN#56764650）

“JVN”の脆弱性レポートによると、本脆弱性の深刻度は“CVSS v3”で基本値“7.8”、“CVSS v2”で基本値“6.8”。開発者と連絡が取れないため、本脆弱性の対策状況は不明であるという。“JVN”は「ViX」の利用中止を検討するよう呼び掛けている。