— AUS（アルテミス・ユーザ・サポート）便り 2018/03/12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「2月請求書」「Re：ご注文ありがとうございます。」のウイルスメール拡散、Appleをかたるフィッシングにも注意

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

このニュースをザックリ言うと・・・

- 3月6日（日本時間）以降、ウイルスが添付されたメールが拡散しており、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）より警告が出されています。

- 警告による、メールの特徴は以下のとおりです。

◆ 3月6日に送信されたメール：
件名「2月請求書」、本文が「いつも大変お世話になっております。1月～2月分請求書送付させて頂きます。」で始まり、ファイル名「000000-([ユーザー名])-00.xls」等のExcelファイルが添付。

◆ 3月8日に送信されたメール：
件名「Re: ご注文ありがとうございます。」、本文が「新しい請求書が本日アップロードされました。どうぞよろしくお願い申し上げます。」、ファイル名「00000-2018 年 3 月 8 日.xls」等のExcelファイルが添付。

- JC3ではこの他に、2017年10月以降、Appleをかたり継続的に送信されているフィッシングメールについても警告しており、以下の特徴があります。

◆ 件名「あなたのApple IDのセキュリティ質問を再設定してください。」、本文が「お客様のApple ID が、ウェブブラウザからiCloudへのサインインに使用されました。」で始まるHTMLメールで、Apple IDを詐取しようとするフィッシングサイトへのリンクが張られている。

AUS便りからの所感等

- 2016年11月以降、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、JC3のサイトではその情報が随時更新されています。

- 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、そこで見たことがあるような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ましょう。

- 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、さらにUTMの設置による不審なメールの遮断といった多層防御を行う他、ウイルスメールで用いられるような件名・文面を避ける等のアプローチも検討に値するでしょう。

●企業PCのOS移行、Windows 7終了後も「半分ほどしか進まない」

http://www.itmedia.co.jp/news/articles/1803/08/news116.html

このニュースをザックリ言うと・・・

- 3月8日（日本時間）、IT専門調査会社のIDC Japan社より、国内法人PC市場のOS移行状況に関する2017年9月の調査の結果が発表されました。

- 発表によれば、2020年1月にサポートが終了するWindows 7について、サポート終了を「認識している」企業・団体は76.7%との結果が出ており、これは即ち23.3%が「認識していない」ことになります。

- またWindows 10に「移行済み」との回答は全体の14.6%、「(明確な)移行計画がある」のは40.6%であり、その他「以降計画はあるが詳細不明」24.0%、「移行計画がない」10.6%等となっています。

- 2016年に行った調査より進展はあるものの、「Windows 10に切り替え予定がある企業のPC台数」の比率でみると、サポート終了後の2020年上半期時点で51.5%程度と予想されています。

AUS便りからの所感等


ITmedia NEWS

企業PCのOS移行、Windows 7終了後も「半分ほどしか進まない」 IDC Japanの予測

2018年03月08日 16時24分 公開 [村田朱梨, ITmedia]

印刷 通知 146 70 B! 18

IDC Japanは3月8日、国内法人PC市場のOS移行状況に関する調査結果を発表した。Windows 7の延長サポートは2020年1月14日に終了するが、調査ではサポート終了時点で企業PCの「半分ほどしかWindows 10に移行していない」と予測。同社の浅野浩寿さん（PC、携帯端末＆クライアントソリューション シニアマーケットアナリスト）は「非常にまずい状況だ」と警鐘を鳴らす。

- 中堅中小企業に限定すると「サポート終了を認識している」「Windows 10に移行済み～移行計画がある」のは約70%と低くなっており、中でも建築・土木業等は特に認識が低いとのことです。

- あらゆるOSやその特定のバージョンにはサポート期限があり、Windows10も2025年10月には全てのサポートが終了しますが、半年おきにリリースされる10の各バージョン（1607・1703・1709等）に至ってはサポート期間が1年半しかありません。

- 今後新たに導入されるPCについては、特殊な事情がない限りWindows 10あるいは8.1が選ばれると思われますが、その特殊な事情の多くは業務で使用するWindowsアプリケーションが利用可能かといったところでしょうし、それらのアプリケーションの更新やそれを前提としたより新しいOSでの検証も早い段階で実施することが最終的にはコストの軽減につながることでしょう。

●NEM不正流出、社員PCのウイルス感染が原因と想定

https://www.asahi.com/articles/ASL386K55L38ULZU00D.html

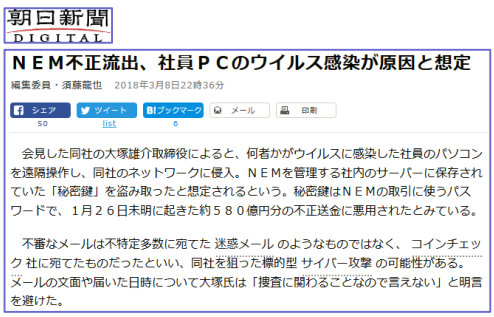
このニュースをザックリ言うと・・・

- 3月8日（日本時間）、仮想通貨取引サイト「Coincheck」を運営するコインチェック社より、1月に発生した仮想通貨「NEM」の流出事件についての調査結果等が報告されました。

- 報告によれば、複数名の同社社員のPCがマルウェアに感染し、攻撃者がPCを経由して同社ネットワークに侵入、NEMのサーバ上で通信傍受を行ってNEMの秘密鍵を奪取し、外部へ不正送金を行ったものと想定しています。

- 同社ではサービス再開に向け、「ネットワークの再構築」「サーバの再設計及び再構築」「業務PCのセキュリティ強化(認証・アクセス制限等)」「セキュリティ監視の実施」「仮想通貨入出金の安全性検証」といった取組みを行うとしています。

AUS便りからの所感等


朝日新聞 DIGITAL

ＮＥＭ不正流出、社員ＰＣのウイルス感染が原因と想定

編集委員・須藤龍也 2018年3月8日22時36分

シェア 50 ツイート list B!ブックマーク 6 メール 印刷

会見した同社の大塚雄介取締役によると、何者かがウイルスに感染した社員のパソコンを遠隔操作し、同社のネットワークに侵入。ＮＥＭを管理する社内のサーバーに保存されていた「秘密鍵」を盗み取ったと想定されるという。秘密鍵はＮＥＭの取引に使うパスワードで、１月２６日未明に起きた約５８０億円分の不正送金に悪用されたとみている。

不審なメールは不特定多数に宛てた 迷惑メール のようなものではなく、コインチェック 社に宛てたものだったといい、同社を狙った標的型 サイバー攻撃 の可能性がある。メールの文面や届いた日時について大塚氏は「捜査に関わることなので言えない」と明言を避けた。

- 特に中小企業においては、外部ネットワークから内部ネットワークへの侵入に対する対策を重視する一方、内部ネットワーク上のPCからサーバへのアクセス、あるいはそこから外部へのアクセスについては十分な防御がされていないケースも未だ少なくはないと思われ、そういったネットワーク構成では、たとえマルウェア感染への対策が万全であっても、ひとたび侵入された際の被害を最小限に抑えることは困難でしょう。

- コインチェック社では「ネットワークの再構築」の一例として、社内ネットワークから外部ネットワークへの接続に対する出口対策においても多層防御を行うとしており、UTMを用いる等によるネットワーク構成の見直しをはじめ、とり得る対策を可能な限り検討・採用することがシステム全体のセキュリティを大幅に高めることに繋がります。