— AUS（アルテミス・ユーザ・サポート）便り 2019/01/15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。

●2020年はWindows 7とOffice 2010がサポート終了、IPAが注意喚起

https://www.ipa.go.jp/security/announce/win7_eos.html
https://www.microsoft.com/ja-jp/business/windows/endofsupport.aspx

このニュースをザックリ言うと・・・

- 1月10日（日本時間）、情報処理推進機構（IPA）より、2020年に複数のMicrosoft社ソフトウェアのサポートが終了することを受けて注意喚起が出されています。

- 2020年1月14日にWindows 7（およびWindows Server 2008、Windows Server 2008 R2）が、同10月13日にOffice 2010が、それぞれ一般的なサポートを終了する予定となっています。

- サポート終了後に新たな脆弱性が発見されても、一般にベンダによる修正は行われず、脆弱性を悪用した攻撃による被害を受ける可能性が高くなるとして、IPAでは、WindowsやOffice以外のサードパーティー製ソフトウェアも含めて速やかな最新版への移行等の実施を推奨しています。

AUS便りからの所感等

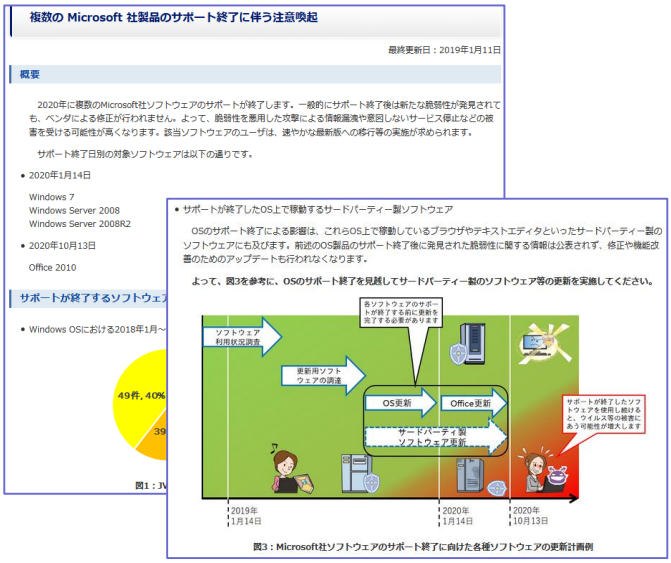
- Windows 7については、2018年9月に企業ユーザ向け有償延長サポートを2023年まで提供することが発表されていますが、ボリュームライセンス契約かつ一部のエディションに限定される等、利用条件は厳しいものとなっています（AUS便り 2018/09/18号参照）。

- 2014年のWindows XPのサポート終了時、一部アンチウイルスソフトでは引き続き一定期間サポートを行っていましたが、今回も同様の措置がとられることを最初からあてにするのは適切ではないでしょう。

- ともあれ、あと1年と迫ったサポート終了までに、Windows 10およびOffice 2016（あるいはOffice365）への移行が完了することを目標に、今からでも十分な計画を立てることが肝要です。

- どうしても古いOS等を使い続けなければならない場合、そのPCを別のLANに隔離し、他のアプリケーションは可能な限り最新に保ち、アンチウイルス・UTMによる防御を適切に行うこと等、何らかの防衛策を検討する必要があるでしょう。

IPA Better Life with IT 情報処理推進機構



Microsoft

●ランサムウェアに感染させる顔文字や英文メールが横行

https://blog.trendmicro.co.jp/archives/20107

このニュースをザックリ言うと・・・

- 1月11日（日本時間）、トレンドマイクロ社より、ランサムウェア「GandCrab」や仮想通貨採掘マルウェアへの感染を狙ったメールが今年に入ってから拡散している、として警告が出されています。

- 同社によれば、1月1日～8日に全世界で約400万通のマルウェアメールが確認、うち日本で確認されたものは約388万通で、全体の98%に上っています。

- 同3～5日には件名と本文が「:)」「:D」といった顔文字のみのメールが拡散していましたが、以降は激減し、代わって「I love you」「This is my love letter to you」等の英語の件名のものが出回っている模様です。

AUS便りからの所感等

- GandCrabは2018年に入ってから活動が確認されているランサムウェアで、10月には宇陀市立病院において感染による電子カルテデータ暗号化の被害が発生しています（AUS便り 2018/10/29号参照）。

- 日本をターゲットとした攻撃にしては、英語圏で使われる顔文字を用いる等、現時点では比較的事前に回避しやすいものとなっていますが、日本人にとって違和感を抱きにくい内容に洗練されるまでそう時間はかからないでしょう。

- ウォッチガード社が2019年のセキュリティ動向予測の一つとして「公共機関や産業制御システムを標的としたランサムウェアによる都市機能の麻痺」を挙げる（AUS便り 2018/12/03号参照）等、今年もランサムウェアへの対策は不可欠なものとなると考えられ、アンチウイルス・UTMによる防御のみならず、PCやファイルサーバ等におけるデータバックアップを確実に行うことが重要です。


TREND MICRO トレンドマイクロ セキュリティブログ
POWERED BY TrendLabs
セキュリティ専門家による脅威情報・ニュースをお届けします。

新年にランサムウェアの「ばらまき攻撃」が「顔文字メール」で復活

投稿日: 2019年1月11日
脅威カテゴリ: スパムメール
執筆: セキュリティエバンジェリスト 岡本 勝之

トレンドマイクロでは日夜多くのサイバー攻撃を監視していますが、新年を迎えると共にメール経由でマルウェアを拡散させる新たな攻撃の発生を確認しました。この攻撃では、件名とメール本文が「:)」、「:D」などのいわゆる「顔文字」のみとなっている特徴的なメールが拡散されていますが、この「顔文字」メールを開いてしまうとどのような実害に繋がるものであったのかを解説します。

2019/01/03 (木) 17:51
.com>
:-)
宛先
メッセージ IMG026190480_2018-JPG.zip
:)

図：1月3日時点で確認された「顔文字」マルウェアスパムの例

■マルウェアを拡散させる「顔文字」メール
上回は1月3日に確認されたマルウェアスパムの実例です。この例では「:-)」と「:)」という顔文字が使用されています。トレンドマイクロが確認した範囲では、以下の6種の顔文字がメール件名に使用されていました。

●環境省のWebサイトが改ざん、通販サイトに偽装

https://www.nikkei.com/article/DGXMZO39427150X21C18A2000000/

このニュースをザックリ言うと・・・

- 昨年12月25日（日本時間）、環境省より、同省が実施していた洋上風力発電実証事業に関するWebサイトが不正アクセスを受け、改ざんされていたと発表されました。

- 被害を受けたサイトは同省と独立したgo.jpドメイン下で運営されていたもので、改ざんにより通販サイトを偽装したページが表示されるようになっていたとのことですが、同サイトでは機密情報を取り扱っておらず、情報漏洩の事実はないとしています。

- 同省では同21日に外部からの通報を受けてサイトを閉鎖しており、原因分析・対策の上でサイトを再公開する予定としています。

AUS便りからの所感等

- 改ざんの意図は不明ながらも、フィッシングサイトに利用しようとした可能性が指摘されています。

- 今回幸いにも被害は大きなものとはなりませんでしたが、サイト改ざんは場合によっては閲覧者へのマルウェア感染を引き起こすなどの二次被害をももたらし得ることに注意が必要です。

- 改ざんの経路は、Webサイトの管理画面から直接不正ログインするものから、サイト管理者のPCに侵入するものまで様々で、それぞれについてセキュリティを確保すること、加えて万が一の改ざん発生から復旧できるようデータバックアップを随時実施することが重要です。


日本経済新聞

環境省のウェブサイトが改ざん、通販サイトに偽装

科学&新技術 BP透報
2018/12/27 13:00

保存 共有 印刷 その他

日経 XTECH

環境省は2018年12月25日、同省が運営しているウェブサイトが改ざん被害にあったと発表した。現在、このウェブサイトは閉鎖している。同サイトでは機密情報を取り扱っていなかったため、「機密情報の漏洩の事実はない」という。

改ざんの被害にあったのは、環境省が実施していた洋上風力発電実証事業についてのウェブサイト。このウェブサイトのドメイン配下にあるファイルの一部が第三者によって書き換えられ、通販サイトを偽装したページが表示されるようになっていた。第三者がファイルを書き換えた理由は不明だが、フィッシングサイトに利用しようとした可能性がある。

環境省は18年12月21日、外部からの通報でウェブサイトが改ざんされていることを知り、同日に該当のウェブサイトを閉鎖した。今後は原因分析を進め、対策を講じた上でウェブサイトを再公開する予定だ。

（日経 xTECH　矢口竜太郎）