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。

●Emotetの感染、2月第1週から急速に拡大か…JPCERT/CCが注意喚起

https://www.jpcert.or.jp/at/2022/at220006.html
https://www.ipa.go.jp/security/announce/20191202.html#L18
https://xtech.nikkei.com/atcl/nxt/column/18/00598/121500151/
https://scan.netsecurity.ne.jp/article/2022/02/14/47125.html

このニュースをザックリ言うと･･･

- 2月10日(日本時間)、JPCERT/CCより、マルウェア「Emotet」への感染が2月第1週に急速に拡大したとして注意喚起が出されています。

- Emotetは昨年11月に活動再開の兆しがみられた(AUS便り 2021/11/24号)とされ、「Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数」が、以前感染が大幅に拡大した2020年に迫る勢いとなっているとのことです。

- 主に確認されている手口として、実行で感染するような不正なマクロ付きWord・Excelファイルがメールに暗号化ZIPファイルで添付される、メールのリンクから同様に不審なWord・Excelファイルがダウンロードされる、あるいはアプリケーションのインストールを騙って感染する、といったものが挙げられており、JPCERT/CCでは各種対策・対応を行うよう促しています。

- IPAにおいても感染に関する報告が多数寄せられているとして、Emotet関連の注意喚起ページを更新しています。

AUS便りからの所感等

- 直前となる1月末に、積水ハウスと和歌山県より、内部のPCがEmotetに感染してなりすましメールが外部に送信されたとする発表があり、2月に入ってからは北海道新聞社やクラシエホールディングス等、多数の企業・組織で感染報告が相次いでいます。

- Emotetが送信するメールは、感染したPC上のアドレス帳や送受信されたメール等をもとに、相手がうっかり開封しやすいような文言が記載されており、特に暗号化ZIPファイル(+パスワードを別メールで送信)を用いることにより、アンチウイルスやUTMで検出されにくくする効果があるとされています。

- Officeの将来のアップデートにおいても、マクロの実行をデフォルトでブロックするよう仕様変更するとの発表があり、感染の歯止めとなるかが注目されますが、とにかくEmotetの手口を把握し、自組織・相手それぞれの感染リスクを抑制できるよう、Emotetが悪用するようなメール・データのやりとりを可能な限り避け、場合によってはビジネスチャットやオンラインストレージの活用も検討するといった、安全な連絡手段のルール化等を行うことを推奨致します。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

【図1： Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移 (外部からの提供観測情報)】

● Windows 10 20H2、5月パッチをもってサポート終了…21H2へのアップグレードを

https://forest.watch.impress.co.jp/docs/news/1388040.html
https://docs.microsoft.com/en-US/lifecycle/announcements/windows-10-20h2-end-of-servicing

このニュースをザックリ言うと･･･

- 2月10日(現地時間)、マイクロソフト(以下・MS)より、Windows 10 バージョン 20H2のサポートが5月をもって終了するにあたっての告知ページが設置されています。

- 当該バージョンでは5月10日リリース予定の月例セキュリティパッチが最後となり、以後はパッチが配信されなくなります。

- 現在20H2より後のバージョンとして21H1および21H2がリリースされていますが、5月のサポート終了までに可能な限り21H2へのアップグレードを行うことが推奨されます。

AUS便りからの所感

- Windows 10の各バージョン(大型アップデート)におけるサポート期間は基本的に18ヶ月間とされており、常時セキュリティアップデートを受け取るには段階的なアップグレードの実施は必要不可欠です。

- アップグレードの準備ができ次第、Windows Updateや通知においてアップグレードを促す表示がされる一方、PCによってはすぐにアップグレードしたい場合でもなかなか通知が表示されないケースも珍しくありませんが、手動でのアップグレードのインストールは稀に相性の問題から(特に機種の古いノートPC等)不具合が生じる恐れがあるため、むしろPCの買い替えの方を視野に入れる方が有用な場合があります。

- また、これまでWindows 10は半年に1度新しいバージョンがリリースされていましたが、昨年末に年1度、秋頃のリリースへの変更が発表されており(AUS便り 2021/11/24号)、今年前半の大型アップデートは行われない見通しであること、21H1についても12月をもってサポートが終了することから、現時点では21H1に拘るより21H2(こちらのサポート期限は2023年6月となります)へ一気にアップグレードする方が賢明と思われます。

Impress Watch

「Windows 10 バージョン 20H2」のサービス終了まであと3カ月 ～Microsoftが注意喚起

企業向けエディションなどで残る「バージョン 1909」も終了。後継バージョンへの移行を

樽井 秀人　2022年2月14日 12:54

「バージョン 20H2」の「Windows 10」は、今年5月10日（米国時間、以下同）にサービス終了を迎える。米Microsoftは2月11日、公式ドキュメントサイトに告知ページを設置した。

「Windows 10 バージョン 20H2」（October 2020 Update）は、2020年10月にリリースされたバージョン。Windows 10の各バージョンはリリースされてから18カ月サポートされるのが基本で、以下のバージョンは今年5月にサービス終了となる。

- Windows 10 Home バージョン 20H2
- Windows 10 Pro バージョン 20H2
- Windows 10 Pro Education バージョン 20H2
- Windows 10 Pro for Workstations バージョン 20H2

● iPhone・iPad・Mac等セキュリティアップデート、Web閲覧で影響を受ける「ゼロデイ」脆弱性の修正

https://www.itmedia.co.jp/mobile/articles/2202/11/news038.html
https://support.apple.com/ja-jp/HT201222

このニュースをザックリ言うと･･･

- 2月10日(現地時間)、Apple社より、同社各製品に存在する脆弱性に対応するセキュリティアップデートがリリースされています。

- リリースされたのは「iOS 15.3.1」「iPad OS 15.3.1」「watchOS 8.4.2」「macOS Monterey 12.2.1」およびMacOSの「Safari 15.3(v.16612.4.9.1.8および15612.4.9.1.8)」となり、いずれもWeb閲覧用コンポーネント「WebKit」の脆弱性(CVE-2022-22620)を修正するものとなります。

- 当該脆弱性は悪意のあるWebサイトの閲覧だけで機器の乗っ取りが可能となる恐れがあり、既に攻撃が確認されている「ゼロデイ」脆弱性とされていることから、アップデートが強く推奨されています。

AUS便りからの所感

- iOS/iPadOS 13および14については前述のようなセキュリティアップデートはリリースされておらず、一方で今回の脆弱性の影響を受ける可能性が十分に考えられるため、必ずバージョン15へアップデートを行い、最新バージョンとなっているか確認するようにしましょう(バージョン13・14が動作する機種は全て15にアップデート可能です)。

- iOS/iPadOS 13以降でのサポート対象外となっている古い機種、例えばiPhone 5s・6・6 Plus、iPad(第4世代)・mini 3・Air(第1世代)およびそれ以前の機種については、iOS 12においてもセキュリティパッチがリリースされない限りは可能な限り使用を停止し、新しい機種への変更を強く推奨致します。

- 余談ですが、WebKitから枝分かれして開発されているエンジンを用いるGoogle Chromeにおいても8件の脆弱性を修正したバージョン98.0.4758.102がリリースされており(https://forest.watch.impress.co.jp/docs/news/1388304.html)、前述のCVE-2022-22620に相当する脆弱性が含まれているかはまだ不明ですが、こちらについても最新バージョンとなっているか確認してください。

ITmedia NEWS

「iOS」と「iPadOS」の「15.3.1」配信開始　悪用された可能性のある脆弱性の対処など

2022年02月11日 06時22分 公開　[佐藤由紀子, ITmedia]

米Appleは2月10日（現地時間）、「iOS 15.3.1」「iPad OS 15.3.1」「watchOS 8.4.2」「macOS Monterey 12.2.1」、MacOSの「Safari 15.3（v.16612.4.9.1.8および15612.4.9.1.8）」をリリースした。watchOS以外はいずれも、「悪用された可能性があるという報告」のあるWebKit関連のゼロデイ脆弱性の修正を含む。

本稿ではiOSのアップデートについて紹介する。

15
iOS 15.3.1
Apple Inc.
176.3 MB

iOS 15.3.1ではiPhoneの重要なセキュリティアップデートが提供され、点字ディスプレイが応答しなくなることがある問題が修正されています。

Appleソフトウェア・アップデートのセキュリティコンテンツについては、以下のWebサイトをご覧ください:
https://support.apple.com/kb/HT201222