— AUS（アルテミス・ユーザ・サポート）便り 2023/03/22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。

●新たなEmotetはOneNoteファイルでも感染拡大か…EmoCheck最新バージョンでチェックを

https://www.ipa.go.jp/security/announce/20191202.html#L24
https://www.jpcert.or.jp/at/2022/at220006.html

このニュースをザックリ言うと・・・

- 3月16日(日本時間)にJPCERT/CC、同17日にIPAより、マルウェア「Emotet」の新たな感染拡大の手口に関する情報が発表されました。

- Emotetは3月7日に新たな拡散活動が確認されたとして両団体から注意喚起が出され、アンチウイルスのチェック回避のため、約550MBのWordファイル(.doc)を約655KBのzipファイルに圧縮する手口をとるとされていました(AUS便り 2023/03/14号参照)。

- 今回発表されたさらなる手口として、「Microsoft OneNote」のファイル(.one)を添付し、これを開いた際、文書を見るためにボタンをクリックするよう指示する偽のダイアログを表示し、クリックによってEmotetの感染に繋がり得る不正なスクリプトを実行される可能性があるとしています。

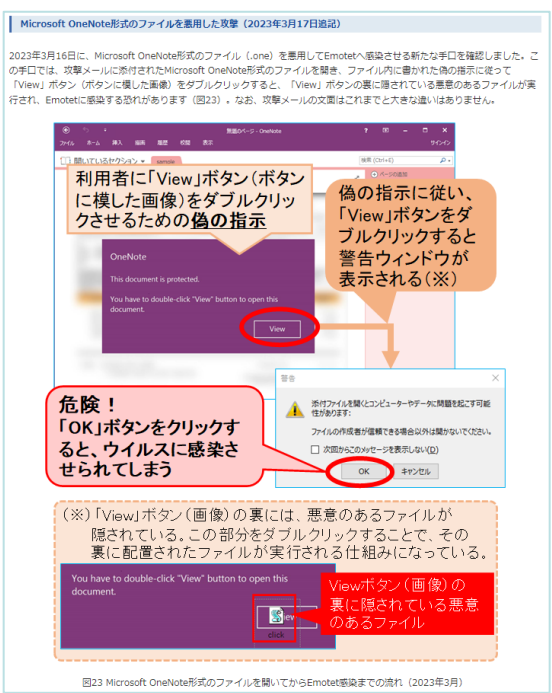
- また3月19日、JPCERT/CCが提供するPC上のEmotet検出ツール「EmoCheck」について、これらに対応したとする最新バージョン2.4.0がリリースされています。

AUS便りからの所感等

- 今回Emocheckについてはバージョン2.3.2以来10ヶ月ぶりの更新となり、メモリスキャン機能も追加されており、今後も更新のリリース毎に、過去のバージョンでチェックしたことがあっても改めてダウンロード、チェックを行うこと、またチェックにはさほど時間がかからないため、アップデートがなくても定期的に実行することが推奨されます。

- WordやExcelはともかく、OneNoteファイルをメールに添付して外部と情報のやり取りを行うという場面は通常考えにくく、それでも念の為「OneNoteファイルで情報をやりとりすることはありません」といった取り決めを顧客等との間で改めて行うことは、安全性の確保のために有用でしょう。

- IPAおよびJPCERT/CCによるEmotetの情報は過去数年間にわたり情報が追加されており、過去にもどういった手口が確認されたかを把握し、日々のメールの受信等において慎重に行動することが肝要です。



● Twitter、無料ユーザー向けのSMS認証を3月19日に終了

https://www.watch.impress.co.jp/docs/news/1479778.html
https://www.itmedia.co.jp/news/articles/2303/19/news042.html
https://gigazine.net/news/20230221-twitter-lost-60-million-dollars-2fa-sms/

このニュースをザックリ言うと･･･

- 2月15日(現地時間)、Twitter社より、Twitterログイン時の2要素認証のうち、SMS(テキストメッセージ)認証の無料ユーザーへの提供を3月19日に終了すると発表しました。

- 3月19日以後、SMS認証の提供は有料サービス「Twitter Blue」の契約ユーザーに限られるとのことで、3月22日時点では予定通り無料ユーザーによるSMS認証の指定はできなくなっています。

- 無料ユーザーに対しては、物理的なセキュリティーキー、あるいは各種認証アプリ(Google Authenticator、Authy、Duo Mobile、1Passwordあるいはi0Sの自動入力機能等)によるTOTP(ワンタイムパスワード)を用いての2要素認証が引き続き提供されます。

AUS便りからの所感

- SMS認証については、スマートフォン・携帯電話のSIMの不正な情報移行や再発行により、SMSを受信する電話番号の乗っ取り等を行う「SIMスワップ詐欺」に対し脆弱であることが指摘され、またTwitter社側の事情としても、ボットによるSMSの大量送信が行われ、年間6000万ドル(約80億円)の送信料がかかっていること等が要因に挙げられています。

- Twitterではログイン時に2要素認証を使用しない設定も可能ですが、今までSMS認証を設定していたユーザーについて、今回の措置により意図せず2要素認証が解除状態になっている可能性もあり、その場合第三者にパスワードのみで不正にログインされる恐れがあります。

- 2要素認証の設定状態は、設定とサポート→設定とプライバシー→セキュリティとアカウントアクセス→セキュリティ→2要素認証(もしくは https://twitter.com/settings/account/login_verification)にて確認可能ですので、SMS認証の解除、意図している設定かの確認とともに、TOTPによる2要素認証の導入をこの機会にご検討頂ければ幸いです。

ITmedia NEWS

Twitterの「SMS認証」3月19日に終了　まだ解除してない無料ユーザーは早めの変更を

2023年03月19日 14時00分 公開　[ITmedia]

米Twitterが2月に発表した、SMSを使った2要素認証をサブスクリプションサービス「Twitter Blue」ユーザー限定にする措置。同社は無料ユーザーに対し設定を削除するようにアプリ内で案内していたが、その期限が迫っている。

SMSを使った2要素認証を削除してください

SMSを使った2要素認証は、Twitter Blueサブスクライバーのみ利用できます。この方法は、ほんの数分で削除できます。認証アプリやセキュリティキーを使った方法は引き続き利用できます。2要素認証についての詳細はこちら。Twitterにアクセスできなくなることを防ぐため、SMSを使った2要素認証は2023/03/19までに削除してください。

● Zoomクライアントに脆弱性、最新バージョンにアップデートを

https://forest.watch.impress.co.jp/docs/news/1486483.html
https://explore.zoom.us/en/trust/security/security-bulletin/

このニュースをザックリ言うと･･･

- 3月14日(現地時間)、米Zoom社より、オンラインビデオ会議サービス「Zoom」のクライアントに計6件の脆弱性が存在すると発表されました。

- 脆弱性はZoomクライアント バージョン5.13.5より前に存在し、PCの乗っ取りやサービス拒否につながるとされています。

- 1月16日にリリースされたバージョン5.13.5で修正済みとされています(3月22日現在の最新は5.14.0です)。

AUS便りからの所感

- ZoomクライアントはChrome等と同様に自動更新機構がありますが、しばらく実行されていなかったり、更新の通知があっても適用されていないケースもあり得るため、必ずクライアントを実行し「更新を確認」するようにしてください。

- この日はMicrosoftからも月例のセキュリティアップデートがリリースされましたが、既に適用が可能であるところを一週間も放置するようなことがくれぐれもないよう、管理下のあらゆるPC・機器とOS・ソフトウェアについて最新バージョンに保つよう心掛けましょう。

Impress Watch

「Zoom」に複数の脆弱性 ～特権昇格やサービス拒否、情報漏洩の欠陥

対策済みバージョンへのアップデートを

樽井 秀人　2023年3月16日 19:05

米Zoom Video Communicationsは3月14日（現地時間）、オンラインビデオ会議サービス「Zoom」のクライアントに複数の脆弱性があることを明らかにした。