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。

●「新型コロナウイルス」便乗の不審なメールに注意…Emotet感染の可能性

https://internet.watch.impress.co.jp/docs/news/1233046.html
https://www.ipa.go.jp/security/announce/20191202.html#L12

このニュースをザックリ言うと・・・

- 1月30日(日本時間)、情報処理推進機構(IPA)より、マルウェア「Emotet」への感染が目的とみられる新たな攻撃メールが確認されたとして注意喚起が出されています。

- 例として示された攻撃メールは、中国の武漢市を中心に感染が広がっている「新型コロナウイルス」に便乗したもので、保健所を騙り「管内 通所・施設系障害福祉サービス事業者 拝」「国内でも〇〇県で患者が報告されているところであり…」等と書かれており、添付されているWord文書を開くことにより、Emotetへの感染に至る不正なマクロが実行されるとのことです。

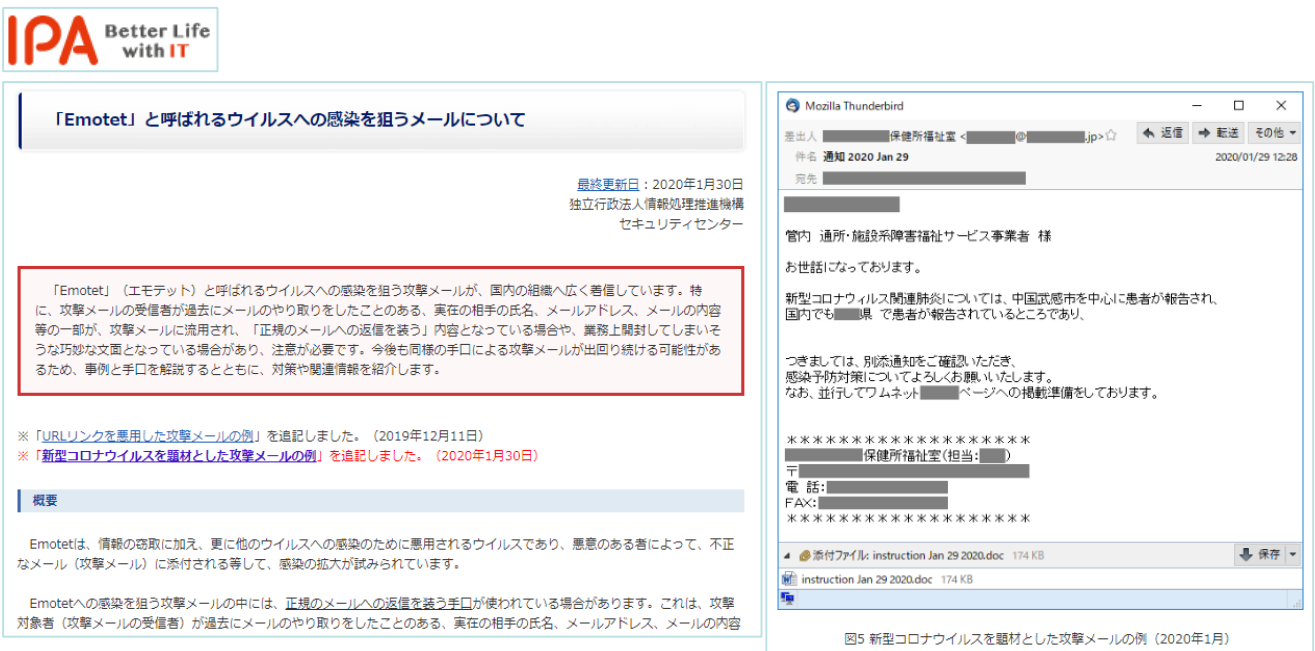
- IPAではEmotetに留まらない一般的なウイルス対策として「身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない」「自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない」「OSやアプリケーション、セキュリティソフトを常に最新の状態にする」「Word文書やExcelファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、『マクロを有効にする』『コンテンツの有効化』というボタンはクリックしない」等を挙げています。

AUS便りからの所感等

- 昨年末には賞与の支払いに関する通知を騙ったメールも出回る等、刻々と手口を変化させているEmotetについて、IPAでは昨年12月以降随時情報の追加更新を行っています。

- また、JPCERT/CCより、PCにEmotetが感染していないかチェックするツール「EmoCheck」が提供されており(https://internet.watch.impress.co.jp/docs/news/1233055.html)、例えば組織内の各PCで定期的に実行させる等も有用でしょう。

- マルウェアにも、また新型コロナウイルスにも当然言えることですが、とにかく最新の正しい情報を的確に収集し、慎重に行動することが肝心であり、またアンチウイルスやUTM等の役割を理解しつつ各種適切な対策をとることを推奨致します。


「Emotet」と呼ばれるウイルスへの感染を狙うメールについて

最終更新日：2020年1月30日
独立行政法人情報処理推進機構
セキュリティセンター

「Emotet」（エモテット）と呼ばれるウイルスへの感染を狙う攻撃メールが、国内の組織へ広く着信しています。特に、攻撃メールの受信者が過去にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容等の一部が、攻撃メールに流用され、「正規のメールへの返信を装う」内容となっている場合や、業務上開封してしまいそうな巧妙な文面となっている場合があり、注意が必要です。今後も同様の手口による攻撃メールが出回り続ける可能性があるため、事例と手口を解説するとともに、対策や関連情報を紹介します。

※「URLリンクを悪用した攻撃メールの例」を追記しました。（2019年12月11日）
※「新型コロナウイルスを題材とした攻撃メールの例」を追記しました。（2020年1月30日）

概要

Emotetは、情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大が試みられています。

Emotetへの感染を狙う攻撃メールの中には、正規のメールへの返信を装う手口が使われている場合があります。これは、攻撃対象者（攻撃メールの受信者）が過去にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容

図5 新型コロナウイルスを題材とした攻撃メールの例（2020年1月）

●pixivで脆弱なパスワードを登録不可に…流出パスワードデータベースと照合

https://www.itmedia.co.jp/news/articles/2001/28/news093.html
https://inside.pixiv.blog/2020/01/22/180000

このニュースをザックリ言うと・・・

- 1月22日(日本時間)、イラストコミュニケーションサービス「pixiv」より、同サービスで使用するパスワードとして、他のサービスで流出が確認された脆弱なパスワードを設定できないようにしたと発表されました。

- 流出したメールアドレス・パスワードのデータベースを運営するWebサイト「Have I Been Pwned」(以下HIBP)が、同サイトで保有しているパスワードをハッシュ化したデータを提供しており、アカウント登録時やパスワード変更時に入力されたパスワードをそのデータと照合しているとのことです。

- HIBPが提供するデータは5億5,000万件程度と膨大なものになっていることから、同サービスでは一定の回数以上流出が確認されたパスワードのみを用いているとのことです。

- pixivでは「FIDOや多要素認証といったパスワードに頼らない認証方法によるセキュリティ強化についても対応していく」としています。

図1: 脆弱なパスワードを入力した場合のエラー画面

AUS便りからの所感

- 攻撃者がブルートフォース攻撃を行うために用いる「パスワード辞書」と照合する手法に比べ、実際に流出の被害を受けたデータが揃っており効果的に「脆弱なパスワード」を検知できる利点があるとされています。

- 自社が運営するWebサービスあるいは社内向けミドルウェア等に対し「リスト型攻撃」による不正ログインが行われないために、適切なパスワードを設定するよう啓発するだけでなく、HIBPが提供するサービスやデータの活用等といった対策を採用しやすくなっていくことにも今後期待したいものです。

●東京五輪に向けたサイバーセキュリティ対策強化の緊急提言…総務省が発表

https://www.itmedia.co.jp/news/articles/2001/28/news120.html
https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00093.html

このニュースをザックリ言うと・・・

- 1月28日(日本時間)、総務省より、7月以降開催の東京オリンピック・パラリンピックを前に早急に取り組むべきサイバーセキュリティ対策について取りまとめた緊急提言「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項」が発表されました。

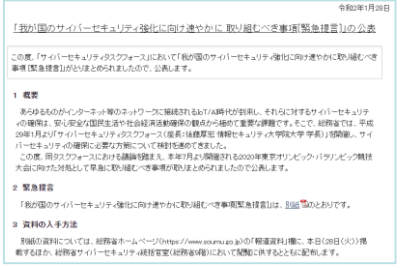
- 提言では、具体的施策として
「IoT機器のセキュリティ対策(機器が攻撃を受けやすくなっていないかの調査と所有者・運用者への注意喚起等)」
「地方公共団体向けサイバーセキュリティ演習(50%程度に留まっている受講率の引き上げ等)」
「情報共有体制の強化(個人情報等の流出が疑われる時点で速やかに情報の公表を検討する、等)」
「公衆無線LANのセキュリティ対策(リテラシー強化のための周知啓発を、特に多くの利用が見込まれるホテル・観光関係機関・病院・教育機関等で行う、等)」
「制度的枠組みの改善(法令・ガイドライン等策定)」
の5点が挙げられています。

AUS便りからの所感

- 提言の内容は真新しいものを含んでいるものではなく、むしろこれまで実施された施策についての見直し、あるいは「基本に立ち返るべき」という意味合いが濃いものと考えられます。

- 「オリンピック・パラリンピックが開催されるから」とか「大企業だから」とかの理由でサイバー攻撃のターゲットにされる頻度が上がるという因果関係は真っ向から否定できるものではありませんが、それでも実際にはそういったイベントと関係なく普段から攻撃は発生していますし、中小企業が運営するWebサイトでも個人情報の漏洩が度々発表されてニュースになっており、それはオリンピックが終了した後も変わらないでしょう。

- さらにはニュースにならない、ターゲットとなる組織が気付いていないような攻撃も陰では多く発生していることが予想され、攻撃の余地を与えない・発生に気付き遮断する・被害を最小限に抑える等のための各種対策をとって頂ければ幸いです。


令和2年1月28日
「我が国のサイバーセキュリティ強化に向け速やかに 取り組むべき事項[緊急提言]」の公表
この度、「サイバーセキュリティタスクフォース」において「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項(緊急提言)」がとりまとめられましたので、公表します。
1 概要
2 緊急提言
3 資料の入手方法