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、9月から再び急増…JPCERT/CCが注意喚起

https://twitter.com/jpcert_ac/status/1301414900820975616
https://www.jpcert.or.jp/newsflash/2020090401.html

このニュースをザックリ言うと・・・

- 9月3日(日本時間)、JPCERT/CCより、マルウェアEmotetの感染被害および問合せが急増しているとして注意喚起が出されています。

- 注意喚起によれば、Emotetによってメール送信に悪用されている .jpドメインアドレス数がこれまで1日あたり1000件前後以内だったものが8月31日以降1500件以上に急増する等、活動が活発化しているとのことです。

- また、感染を広げるための新たな手口として、「パスワード付きzipファイルを添付し、パスワードはメール本文中に記載されている」ケースが確認されているとしています。

AUS便りからの所感等

- Emotetについては2019年以降断続的に日本国内をターゲットとした攻撃が確認されており、JPCERT/CCでは7月にも活動の再開がみられたとして注意喚起が出されていました(https://www.jpcert.or.jp/newsflash/2020072001.html)。

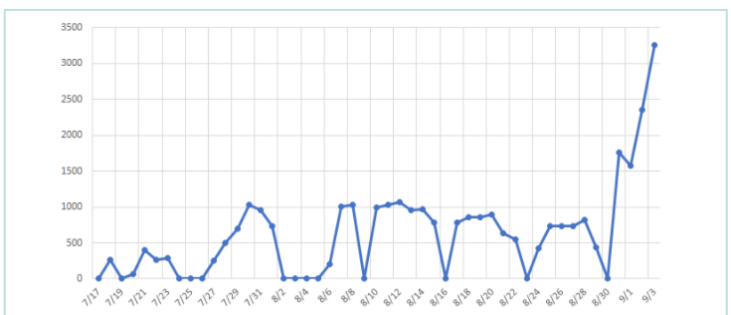
- IPAでも9月1日～2日に約40件の相談があったとし、不審なメールを開かない、不審なWordファイル等の「コンテンツの有効化」ボタンをクリックしない、不審なメール本文中のURLをクリックしないよう呼び掛けています(https://www.ipa.go.jp/security/announce/20191202.html#L13)。

- 暗号化zipファイルはアンチウイルスによるマルウェアの検出を回避する方法として既に何年も前から悪用されており、Emotetが従来から行っている「感染したPC上の実際に送受信されたメールをもとになりすましメールを作成する」手法との組合せにより、より効率的な感染を狙っていることは容易に予想されます。

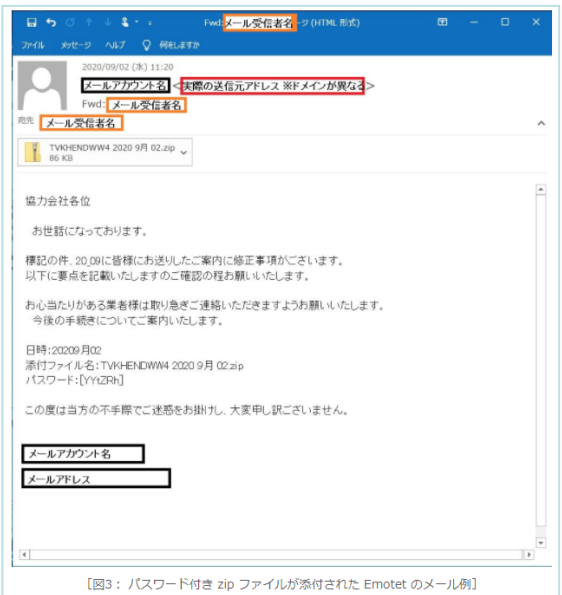
- このようなEmotetの流行と注意喚起を機会として、外部との安全なメール・文書ファイルのやりとりにあたっては、可能な限り暗号化zipファイル以外の手段を用いるよう依頼する等、相互にルールの策定が行われることに期待したいものです。

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

マルウェア Emotet の感染拡大および新たな攻撃手法について



[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 アドレスの推移 (外部からの提供観測情報)]



[図3： パスワード付き zip ファイルが添付された Emotet のメール例]

●新型コロナ関連の脅威が3カ月で8倍超に…トレンドマイクロ調査

https://www.itmedia.co.jp/news/articles/2009/01/news143.html
https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20200831-01.html
https://blog.trendmicro.co.jp/archives/25979

このニュースをザックリ言うと･･･

- 8月31日(日本時間)、トレンドマイクロ社より、2020年上半期(1～6月)における国内外での脅威動向についての分析結果をまとめた「2020年上半期セキュリティラウンドアップ」が公開されました。

- 新型コロナウイルスに便乗してのサイバー犯罪がやはり大きなトピックとなり、例えば2020年上半期において、国内の同社製品ユーザーのうち約297万人がフィッシングサイトへ誘導されたとのことです。

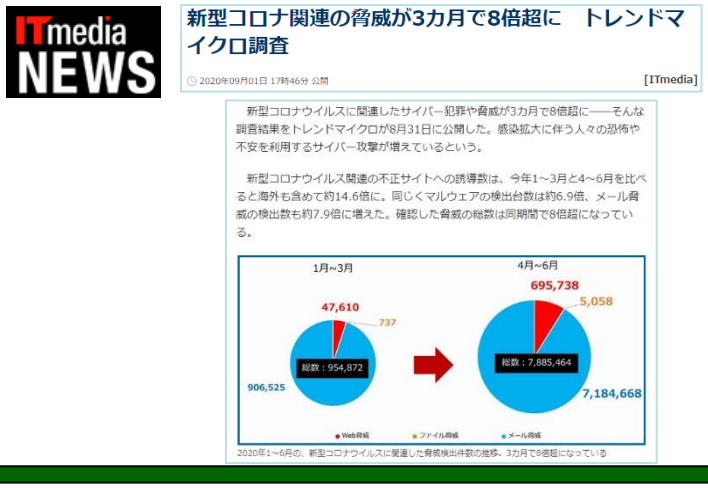
- また、同上半期を1～3月と4～6月に分けた場合の脅威検出数は、前者に比べ後者はその約8.26倍に上るとされています(うちフィッシングサイトなど不正サイトへの誘導数は約14.6倍、マルウェア検出数は約6.9倍、等)。

- 具体的な脅威の例としては、マスク販売や特別定額給付金に関する詐欺等のメール、テレワーク用ツールやVPNシステムに対する攻撃等が挙げられています。

AUS便りからの所感

- オリンピック等の一過性のスポーツイベントと異なり、社会の形を不可逆的に変えかねない出来事であり、それによって新たに導入された様々なものに対し攻撃者が目をつけることに注意を払わなければなりません。

- 一方で、テレワークで注目を集めている電子会議システムやVPN等といったものはこれまでにも存在していたものであり、防御すべきポイントは多くが既に挙げられているものと思われますので、慎重に情報収集を行いつつ要所を抑えたシステム構築を行うこと、たとえ拙速に導入していたとしても必ず安全でない箇所がないか確認することが肝要です。



●ネット接続製品の安全な選定・利用ガイド、IPA発表

https://www.ipa.go.jp/about/press/20200827.html

このニュースをザックリ言うと･･･

- 8月27日(日本時間)、IPAより、インターネット接続機器の脆弱性対処を促進するためのガイド文書が公開されました。

- ガイドは一般消費者と製品開発者向けの二種類で、特に一般消費者向けガイドは「ネット接続製品の安全な選定ガイド」と「ネット接続製品の安全な利用ガイド」の二つからなっています。

- IPAでは、テレワーク・ステイホームの推奨により、ネットワークに接続する機器の利用がますます増えていることを鑑み、「一般消費者と製品開発者のそれぞれが脆弱性に対する理解を深め、消費者が脆弱性に対処した製品を選ぶようになることで、企業における製品への対策が進むことを目指し」てガイドを公開したとしています。

AUS便りからの所感

- スマートフォンやPCのみならず、ルーター・ゲーム機・家電等あらゆる機器がネットワークに接続する機会が増えることは、その脆弱性や設定の不備を狙われる機会も増えることであり、それはいわゆるIoTが定着した頃から言われてきたこともあります。

- 「ネット接続製品の安全な選定ガイド」では選定の際のポイントとして「(ファームウェア等の)アップデート機能」「(脆弱点等の)セキュリティ情報」および「問合せ窓口の提供」を行っていること等を、「ネット接続製品の安全な利用ガイド」では利用の際のポイントとして「購入後すぐにパスワードの変更等を実施する」「メーカーのWebサイトを定期的に確認する」「サポートが終了した製品は利用をやめるか買い替える」こと等を挙げています。

- 挙げられているポイントの多くはこれまでにも度々IPAや各組織が取り上げているものであり、可能な限り全てのユーザーが目を通し、現在利用している機器についても問題がないか点検する等、改めてセキュリティを意識した機器の利用に努めて頂ければ幸いです。