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。

●拡張子「.iqy」の添付ファイルによるマルウェア拡散メール、一日で29万件…トレンドマイクロ警告

http://www.itmedia.co.jp/news/articles/1808/08/news061.html
https://japan.zdnet.com/article/35123751/

このニュースをザックリ言うと・・・

- 8月8日（日本時間）、トレンドマイクロ社より、日本語のマルウェア拡散メールにおいて拡張子「.iqy」のファイルが添付されたものが確認されたとして注意を呼び掛けています。

- 同社や日本サイバー犯罪対策センター（JC3）によれば、問題のメールは、
◆件名が「お世話になります」「ご確認ください」「写真添付」「写真送付の件」等
◆本文が「お世話になります。解約に関する書類です。」や「XLS版にて送付致します。」といったもの
◆「8月(数字).iqy」「(ユーザー名)(数字).iqy」という名前のファイルが添付されている
とのことです。

- トレンドマイクロ社では5月下旬から海外で.iqyファイル添付のメールによる攻撃を確認していましたが、今回8月6日だけで29万通もの日本向けメールが確認されたとしています。

AUS便りからの所感等

- .iqy拡張子のファイルはExcelの「Webクエリ」機能で使用されるものですが、これを悪用してExcelに不正なファイルをダウンロードさせ、最終的にオンラインバンキングを狙うマルウェア「URSNIF」へ感染させる意図があるとされています。

- .iqyファイルを開いた際にはExcelのセキュリティ機能により実行を確認するメッセージが表示されるため、誤ってファイルを開いた場合には決して「有効にする」を選択しないでください。

- トレンドマイクロ社ではこのような.iqyファイルが添付されたメールを受信しないようメールサーバで設定すること等を推奨していますが、いずれにしろ、アンチウイルスやUTMによる防御を確実に行うとともに、こういった方法でマルウェアに感染させる動きがあるということを情報収集し、組織内への啓発を行うことが肝要です。

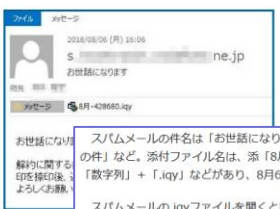
ITmedia NEWS

「.iqy」ファイル付きウイルスメール、日本語で初確認　1日で29万通、トレンドマイクロが注意喚起

2018年08月08日 12時01分 公開　[ITmedia]

印刷　通知　463　308　B! 25

トレンドマイクロは、拡張子「.iqy」ファイル付きの日本語ウイルスメールを8月に入って初めて確認したと、ブログで明らかにした。ファイルを開くとExcelが起動して不正スクリプトファイルをダウンロードさせられ、最終的にオンライン銀行詐欺ツールに感染させられるという。



.iqyは、Excelで直接インター
張子付きファイルが添付された
日本向けの日本語マルウェアス

スパムメールの件名は「お世話になります」「ご確認ください」「写真添付」「写真送付の件」など。添付ファイル名は、添「8月」＋「数字列」＋「.iqy」や、「受信者名」＋「数字列」＋「.iqy」などがあり、8月6日の1日だけで29万件以上を確認しているという。

スパムメールの.iqyファイルを開くとExcelが起動。不正スクリプトファイルをダウンロードさせ、最終的にオンライン銀行詐欺ツール「URSNIF」（アースニフ）に感染させられるという。ファイルを開いた際、Excelのセキュリティ機能により実行を確認するメッセージが2回にわたって表示され、「無効にする」か「いいえ」を選べばマルウェアの侵入を防げると解説している。

被害を防ぐためには、.iqyファイルを日常的に使っていない場合は、Excelの「セキュリティセンター」から「ファイル制限機能の設定」で、「Microsoft Officeクエリファイル」を開かない設定にすることをすすめている。また、法人ネットワークでは、.iqyファイルのメール受信を制限する対策も有効だとしている。

ZDNet Japan

拡張子「iqy」のファイルを使う攻撃に注意 --Excelを悪用

ZDNet Japan Staff 2018年08月08日 15時03分

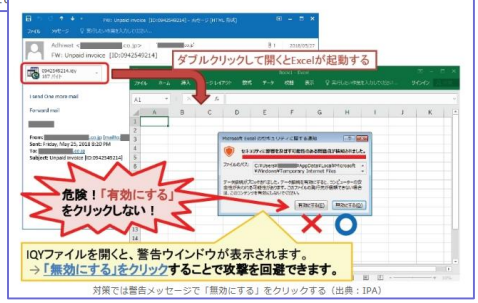
いいね！ 40　ツイート　B! 7　Pocket 47

印刷　メール　ダウンロード　クリップ

「.iqy」という拡張子のファイルを使う攻撃が急増しているとしてトレンドマイクロが8月8日、ブログを通じて注意を呼び掛けた。ファイルを開くとMicrosoft Excelが起動するが、その際に表示される警告メッセージで「無効にする」ボタンを選択すれば、被害を防止できるとして

この攻撃は5月に海外で報告
この拡張子を持つファイルを添
真添付」「写真送付の件」など
日には29万件以上を検知した。

Excelを悪用する攻撃は、これまで不正なマクロを使う手口などが知られる。マクロ機能の無効化や「保護ビュー」でファイルを開くことが基本的な対策となるが、情報処理推進機構（IPA）は「.iqy」ファイルを使う攻撃では保護ビューを有効にしていてもマルウェアに感染すると解説。警告メッセージで必ず「無効にする」を選択するようアドバイスしている。



対策では警告メッセージで「無効にする」をクリックする（出典：IPA）

●ドコモのユーザアカウントに不正ログイン…iPhone X等不正購入

http://www.itmedia.co.jp/mobile/articles/1808/17/news067.html

このニュースをザックリ言うと・・・

- 8月14日（日本時間）、NTTドコモより、同社ユーザ向けアカウント「dアカウント」が不正にログインされ、ドコモオンラインショップで不正に端末を購入・詐取される被害が発生していることが発表されました。

- 発表によれば、7月下旬までに約1800件の不正ログインが発生し、うち約1000件において端末の詐取が行われたとのことで、「iPhone X」など10万円超のスマートフォンを購入させられたケースもあるとされています。

- 同社ではdアカウントに2段階認証を設定するよう呼び掛けるとともに、ドコモオンラインショップの利用時に2段階認証を必須とする措置を行っています。

AUS便りからの所感等

- 今回NTTドコモが2段階認証を推奨あるいは義務付けている理由として、いわゆる「パスワードリスト型攻撃」による不正ログインが行われ、被害を受けたアカウントがいずれも2段階認証を設定していなかったことを挙げています。

- dアカウントのみならずあらゆるサービスにおいて、他のサービスで利用しているパスワードを使い回さないこと、そして各サービスが提供するアカウント保護機能について調べ、活用することを改めて意識しましょう。

ITmedia Mobile

ドコモオンラインショップが購入時の「2段階認証」を必須に
不正ログイン対策で

2018年08月17日 12時30分 公開　[井上翔, ITmedia]

印刷　通知　32　8　B! 2

NTTドコモは8月15日から、同社のWeb直販サイト「ドコモオンラインショップ」における商品購入手続き時、または申し込み履歴確認時の「2段階認証」を必須化した。同サイトにおいて不正ログインによる端末の詐取が行われたことに伴う措置だ。

端末詐取は約1000件　「2段階認証」未設定ユーザーが狙われた

ドコモオンラインショップで商品を購入する場合、「dアカウント」が必須となる。

ドコモ広報部によると、同サイトでは7月下旬からdアカウントでの不正ログインが約1800件発生し、そのうちの約1000件において端末の詐取が行われたという。詐取された端末には「iPhone X」など10万円超の高額なスマートフォンも含まれる。

不正ログインはいわゆる「パスワードリスト型攻撃」で行われたと見られ、被害にあったアカウント（ユーザー）はいずれも「2段階認証を設定していなかった」（広報部）。

●JPCERT/CCがランサムウェア被害の実態調査結果発表

https://japan.zdnet.com/article/35123248/

このニュースをザックリ言うと・・・

- 7月30日（日本時間）、JPCERT/CCより、2017年9月19日～10月17日に国内組織でのランサムウェア被害の実態を調査した報告書が発表され、重要インフラを手掛ける184組織からの回答のうち、35%にあたる64組織がランサムウェアの被害を受けたことがあるとしています。

- 感染原因としては「メールの添付ファイル」(66%)および「WebサイトまたはWebアプリケーション」(41%)が多かった一方、11%が「不明」等と回答しています。

- 被害の内容は、「データの暗号化」(89%)、「業務端末の使用不可」(56%)、「社内システムの停止」(11%)等が挙げられ、影響を受けた機器の数は多くが「1台(感染した端末のみに留まった)」(36%)や「2台以上～5台未満」(36%)程度でしたが、「20台以上」という回答も11%あったとのことです。

- また被害にあった際に行った対処としては、「業務端末を入れ替えた」(80%)、「データをバックアップから戻した」(58%)という回答があった一方、「バックアップしていなかったためデータを戻せなかった」という回答も16%あったとされています。

AUS便りからの所感等

- 上記の他にも多岐にわたる質問への回答は、現在もランサムウェアが少なからず猛威をふるっていることと、一方で「感染しないようにする対策」「万が一感染した場合に備えての対策」それぞれについて多くの組織が的確な対処を行っていたことがうかがい知れます。

- 調査報告書は「ランサムウェアがどんな被害を及ぼすか」から「どういった対策が適切か」までよくまとまった内容となっており、現在どれだけの対策をとっているかに関わらず、改めてランサムウェアについて学び直し、啓発し、さらなる安全の確保を行うための資料として有用なものとなり得るでしょう。

ZDNet Japan

国内組織の35%がランサムウェアで被害
--JPCERT/CCが実態調査

ZDNet Japan Staff 2018年07月30日 13時44分

いいね！40　ツイート　G+　B! 3　Pocket 22

印刷　メール　ダウンロード　クリップ

JPCERT コーディネーションセンター（JPCERT/CC）は7月30日、国内組織でのランサムウェア被害の実態を調査した初の報告書を発表した。回答組織の35%が被害を経験し、97%が身代金を支払わなかったといった状況が判明した。

調査は2017年9月19日～10月17日に、重要インフラを手掛ける組織にアンケートしたもの。184の組織が回答している。ランサムウェア被害を経験したのは全回答の35%に当たる64組織で、被害実態は64組織の回答内容が中心となる。