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。

●日本もマクロ攻撃のブーム再来、企業は要注意！マクロウイルス(※)を知らない世代の社員が狙われる？

http://www.itmedia.co.jp/enterprise/articles/1601/29/news124.html
http://internet.watch.impress.co.jp/docs/news/20160129_741451.html

このニュースをザックリ言うと･･･

- 1月28日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、不正なマクロを含むOfficeファイルが添付されたメールによる攻撃について警告が発表されました。

- 同社によれば、2015年の全世界での攻撃検出数は530,594件と、2014年の103,804件から5倍以上に急増しており、その8割が企業を狙ったものとされる他、日本での検出も2015年10月～12月に大きく増加した模様です。

- 同社では近年のマクロウイルスについて、「過去の流行とマクロ無効化設定の背景を知らない利用者をだまして、攻撃の成功率を高める手法」がとられていると分析しており、「メールの添付ファイルを安易に開かない」「不用意にマクロを実行できるようにしない」「更新プログラムを速やかに適用する」「セキュリティ製品の利用」といった、基本に立ち返った対策を呼びかけています。

AUS便りからの所感等

- マクロ機能を悪用するいわゆる「マクロウイルス」は1995年以降様々なものが大流行し、Office2007以降ではデフォルトでマクロ実行を無効化する措置がとられたことにより下火にはなったものの、手動でマクロを有効化するよう仕向けるために様々な巧妙な手口がとられるようになっています。

- 記憶に新しいところでは、2015年10月、実在する組織からの注文確認や、複合機からの自動送信通知に偽装したマクロウイルスが確認されています。

- なぜマクロ実行がデフォルトで無効化されているのかといった背景を含め、マクロウイルスが如何にしてPCに感染しようとするかについて啓発を行い、ユーザに慎重な行動を促すとともに、不審なメール・添付ファイルがユーザのもとに届かないようアンチウイルス・UTMによる防御を固めることが重要です。

ITmedia エンタープライズ

2016年01月29日 16時50分 更新

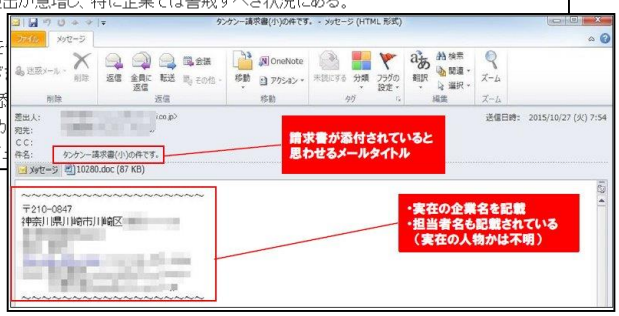
日本もマクロ攻撃のブーム再来、企業は要注意

不正なマクロを埋め込んだOfficeファイルを添付してメールで送り付ける攻撃が2015年10～12月期に急増。特に企業は注意すべきだという。

[ITmedia]

トレンドマイクロは1月28日、不正なマクロを埋め込んだOfficeファイルを添付してメールで送り付ける攻撃への注意を呼び掛けた。攻撃は2015年初めから観測されていたが、2015年10～12月期に日本での検出が急増し、特に企業では警戒すべき状況にある。

不正なマクロを
知といったさまざ
んだファイルが添
を開くと、マクロ
染すると、コンピ



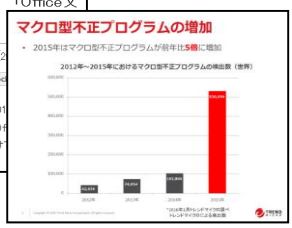
実在企業の請求になりすましたメール。
添付ファイルに不正マクロが埋め込まれていた（トレンドマイクロより）

INTERNET Watch

ニュース

マクロウイルスを知らない世代の社員が狙われる？ 「Office文書を開いて感染」攻撃が再び増加

かつて猛威を振るった“マクロ型不正プログラム（マクロウイルス）”が201
しつつあるという。トレンドマイクロ株式会社の統計によると、Microsoft Of
クロ機能を悪用した不正プログラムの検出数が2014年から2015年にかけ
いたことが分かった。



IT用語辞典 e-Words

（※）マクロウイルス【 macro virus 】マクロ感染型ウイルス

マクロウイルスとは、ワープロ文書などに埋め込まれて実行される「マクロ」と呼ばれる簡易プログラムの仕組みを悪用したコンピュータウイルス。

ワープロソフトや表計算ソフトなどは、簡単な作業を自動化するために「マクロ」と呼ばれるコンピュータプログラムの実行機能を持っており、文書ファイルに内蔵することができるようになっている。この仕組みを悪用し、利用者に気づかれないようにこっそりと文書ファイルに「感染」して、自己増殖や破壊活動を行うよう設計されたマクロがマクロウイルスである。

マクロは構造上、元のプログラム（ソースコード）がそのままファイル内に記録されるため、興味本位で「改造」して再配布することも多く、「亜種」が発生しやすいという特徴も持つ。マクロを実行できる環境があればOSの種類を問わずに感染できるため、アプリケーションソフトが複数のOSに移植されるようになった今日では、複数のOSにまたがって大量感染するケースも見られる。

●Amazon.co.jpをかたるフィッシングサイトに注意

http://internet.watch.impress.co.jp/docs/news/20160201_741724.html

このニュースをザックリ言うと・・・

- 2月1日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、Amazon.co.jpを騙るフィッシングサイトが確認されたとして警告が発表されました。

- 問題のサイトはAmazon.co.jpのサインイン画面になりすましたもので、同協議会では「.co」ドメインの「http://www.am●●●●●.co/ 」というURLのものを確認している他、類似のフィッシングサイトが開設される可能性もあるとしており、アカウント情報（Eメールアドレス・パスワードなど）を絶対に入力しないよう呼びかけています。

- この他、今回を受けてというわけではありませんが、Amazonも「Amazon.co.jp からのEメールかどうかの識別について」というページにおいて、フィッシングメールか否か確認するよう解説しています。

AUS便りからの所感等

Amazon.co.jpをかたるフィッシングサイト（フィッシング対策協議会の緊急情報より画像転載）

- フィッシングサイトは、本物と同じロゴを使用し、デザイン的には本物と見分けがつきにくいものとなっており、一部テレビ報道では、細かい文言の差異から注意するよう呼びかけるものもあったようですが、あまりに違和感のある日本語でない限り、こういった点で見分けをつけるのは困難です。

- ブラウザのアドレスバーに表示されているURLやSSL証明書での確認はこれに比べれば有効ですが、残念なことに本物のAmazon.co.jpのSSL証明書は、より厳密に組織の証明を行うEV-SSL証明書ではない点には注意すべきです。

- メールにあるURLを安易にクリックせず、ブラウザのブックマークから正規のサイトへアクセスするよう心がけるのが安全であり、この他、ブラウザ・アンチウイルスソフトあるいはUTM等のアンチフィッシング機能を活用することにより、より確実にフィッシングからの防御を行うことができるでしょう。

●DNSプロトコルを介して指令を受ける遠隔操作ウイルス

http://www.atmarkit.co.jp/ait/articles/1602/01/news109.html

このニュースをザックリ言うと・・・

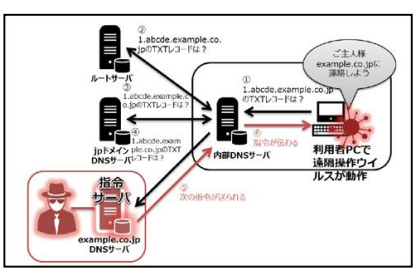
- 2月1日（日本時間）、国内大手セキュリティベンダーのラック社より、「遠隔操作ウイルスへの指令伝達手段としてDNSプロトコルが利用されるケース」が2015年後半より複数の大手企業等で確認されたとして警告が発表されました。

- これまでの遠隔操作ウイルスは、HTTP/HTTPSプロトコルで指令サーバと通信するケースが大半とされていましたが、今回のケースではDNSサーバが指令サーバとなり、ウイルスはDNSサーバにTXTレコードを問合せることで指令を受信する仕組みになっているとのことです。

- 同社は、DNSリクエストログを保持している企業は多くなく、また、一見しただけでは正常なDNS問合せにしか見えないためにファイアウォールやIDSでの検知は困難であること等から、今回発見された遠隔操作ウイルスを「深刻な脅威」としています。

- また、対策として、「ログを用いて不審なDNSアクセス記録を確認し、不正なリクエストがあれば指令サーバとのDNS通信を拒否する」「企業内の名前解決では社外のDNSサーバにフォワードしない設定とし、インターネットアクセスはプロキシサーバ経由に制限する」等が挙げられています。

AUS便りからの所感等



DNSプロトコルを悪用する遠隔操作ウイルスの動作イメージ（ラック発表資料より）

- TXTレコードは、指定されたドメイン名に対するテキストデータを収納する汎用的なDNSレコードで、主な用途としてはSPF（Sender Policy Framework、メール送信者ドメインの認証を行う）等が挙げられます。

- ラック社の発表では、ウイルスが指令サーバに対し大量のTXTレコードの問合せを行っている様子が伺えますが、アンチウイルスやUTMのIDS機能等において、こういった通信を不審なものと判断し自動的に遮断できるようになるか、今後の展開に期待したいものです。