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。

●複合機スキャンデータを装ったマルウェア付メール――トレンドマイクロが警告

http://www.asahi.com/articles/ASH6T5WCHH6TULFA03G.html
http://blog.trendmicro.co.jp/archives/11776

このニュースをザックリ言うと･･･

- 6月24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、複合機からの通知に偽装したメールによる攻撃を確認したとして、同社ブログにて警告が出されています。

- ブログによれば、攻撃メールは「scanner@(受信者のドメイン)」といったFrom: アドレスを持っており、複合機でスキャンされた文書データに偽装した、不正なマクロを含むWordファイルが添付されていることが特徴とのことです。

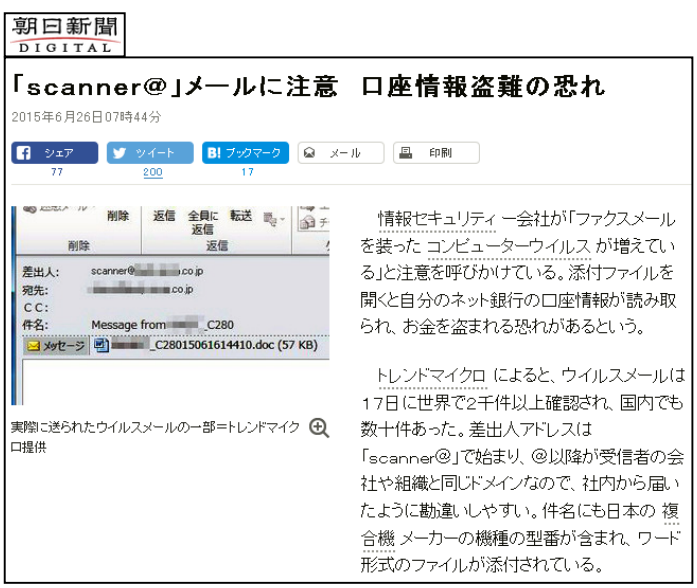
- 同社では、このWordファイルを開くことにより、最終的にネットバンキングの情報を奪取される可能性があること、6月17日前後に2,000件以上の攻撃メールがあったことなどを確認しており、また国内企業からも数十件の問合せがあったことを明らかにしています。

AUS便りからの所感等

- 今回の攻撃メールで使われた添付ファイルはWordファイル形式でしたが、複合機のスキャンデータとしてよりよく使用されるPDF形式の不正なファイルを用いた攻撃も以前は確認されていた模様です。

- 複合機のスキャン機能の詳細（どういったファイル形式で生成されるのか？ メールが送信されるとしたらどういった形でされるのか？ 等）を社内に周知し、通知を装った不審なメールへの注意を促すことはある程度有効かと思われますが、使用している複合機の情報を攻撃者が収集したうえで、より巧妙な偽装を行う可能性もあることには注意が必要です。

- 上記の他、「マルウェアが添付された偽通知メールをアンチウイルス・UTMで防御すること」「スキャンデータのメール送信機能を無効化して複合機上に保存されたデータを直接取り出すルールにすること」さらには「スキャン機能が利用されていなければ無効にすること」等、それぞれの各種対策や運用ルールの設定にはメリット・デメリットがありますので、慎重な取捨選択および組合せの検討が求められることでしょう。



朝日新聞 DIGITAL

「scanner@」メールに注意　口座情報盗難の恐れ

2015年6月26日07時44分

シェア 77　ツイート 200　ブックマーク 17　メール　印刷

削除　返信　全員に返信　転送

差出人：scanner@[redacted].co.jp
宛先：[redacted].co.jp
CC：
件名：Message from[redacted]_C280
メッセージ [redacted]_C28015061614410.doc (57 KB)

実際に送られたウイルスメールの一部＝トレンドマイクロ提供

情報セキュリティ一会社が「ファクスメールを装ったコンピューターウイルスが増えている」と注意を呼びかけている。添付ファイルを開くと自分のネット銀行の口座情報が読み取られ、お金を盗まれる恐れがあるという。

トレンドマイクロによると、ウイルスメールは17日に世界で2千件以上確認され、国内でも数十件あった。差出人アドレスは「scanner@」で始まり、@以降が受信者の会社や組織と同じドメインなので、社内から届いたように勘違いしやすい。件名にも日本の複合機メーカーの機種の型番が含まれ、ワード形式のファイルが添付されている。

TREND MICRO

複合機の通知を偽装したメールがマクロ型不正プログラムを頒布、日本でも被害

投稿日：2015年6月24日
脅威カテゴリ：不正プログラム，スパムメール，サイバー犯罪
執筆：セキュリティエバンジェリスト 岡本 勝之

トレンドマイクロではこの 6月17日前後に、複合機からの通知を偽装したメールによる不正プログラム頒布の攻撃を、世界的に確認しました。これは複合機からのスキャンデータ送信を偽装したマクロ型不正プログラムを含むWord文書ファイルが添付された攻撃メールが広まっているものです。トレンドマイクロのクラウド型セキュリティ技術基盤である「Trend Micro Smart Protection Network（SPN）」の統計データによれば、6月17日に 2000件以上の攻撃メールを集中して確認しています。その攻撃対象は海外が中心ですが、日本でも法人利用者から数十件の問い合わせを受けています。今後も同様の手口の攻撃が発生する可能性がありますので、対策のためにも攻撃について情報共有いたします。

●早稲田大学が標的型攻撃により3,308人分の個人情報が流出

http://itpro.nikkeibp.co.jp/atcl/news/15/062202090/
https://www.waseda.jp/top/information/28714

このニュースをザックリ言うと・・・

- 6月22日（日本時間）、早稲田大学は事務職員のPC数台が標的型攻撃によってマルウェアに感染し、教職員や学生のべ3,308人分の個人情報が流出していたことを発表しました。

- 発表では、PCがマルウェアに感染したのは昨年2014年12月11日で、医療費通知を装う攻撃メールの添付ファイルが開封されたことが感染のきっかけとされており、不審なアクセスに関する連絡を外部機関から受けて発覚したのは半年後の今年6月5日とのことです。

AUS便りからの所感等

- 個人情報流出が確認されなかったケースを含め、依然として企業・大学・自治体等における標的型攻撃によるマルウェア感染が連日報じられており、その多くが外部からの連絡によって感染が発覚しています。

- 高度化していく標的型攻撃に対し誰一人引っ掛からないことを期待することは困難となりつつあり、内部からの不審な通信を検知・遮断するシステムが構築されていない限りは、誰も気付くことなく長期間マルウェアが活動する状況になる可能性を見過ごすことはできません。

- アンチウイルスやパーソナルファイアウォールによる各PCの防衛も大事ですが、それ以上にUTMによる不審な通信の出入りを検知・遮断するシステムの構築が標的型攻撃へ対抗するための対策として必要不可欠となるでしょう。


ニュース 日経コンピュータ

早稲田大学から3308人分の個人情報が流出、「医療費通知メール」が発端

2015/06/22
清嶋 直樹＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

176 おすすめ シェア　3 共有　31 ブックマーク　40 Pocket　83 ツイート

早稲田大学は2015年6月22日、事務職員用のPCがマルウエア（ウイルス）に感染し、学生や教職員らの個人情報延べ3308人分の流出が判明したと発表した（画面）。

二次被害を防ぐために6月19日以降、事務職員用のネットワークで外部のWebサイトへの通信を遮断する措置をとっている。現時点では、学生向けや教員向けのネットワークには影響はないという。

画面● 個人情報流出を知らせる早稲田大学のWebサイト
［画像のクリックで拡大表示］

●標的型攻撃の対策は、従来のウイルス対策と全く逆

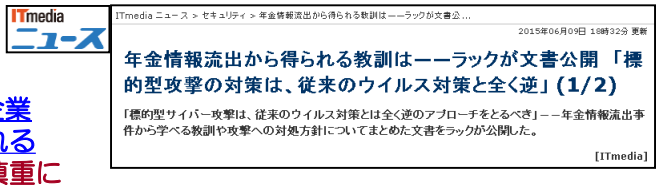
http://www.itmedia.co.jp/news/articles/1506/09/news150.html
http://www.lac.co.jp/news/2015/06/09_news_01.html

このニュースをザックリ言うと・・・

- 今月発覚した日本年金機構からの個人情報流出事件を受けて、6月9日（日本時間）国内セキュリティベンダーのラック社が「日本年金機構の情報漏えい事件から得られる教訓」と題した文書を発表しました。

- 当該文書では、「システム設計に起因する使いにくさ」をシステムそのものの改善ではなく、運用上の「工夫」によってカバーしたことが結果的にセキュリティ侵害を手助けしたものとしており、実際の業務を十分把握せず設計してしまったこと等により生じるシステム上のリスクであるとしています。

- また、標的型サイバー攻撃の対応としては「従来のウイルス対策とは全く逆のアプローチを取るべき」との見解を示しており、有効な対処法として「事件・事故前提の組織体制構築」「社員や職員の意識改革と教育」「事故対応チームの組織化」「セキュリティ監視と不正通信の洗い出し」「事件発生を見越した演習」の5つを挙げています。


ITmedia ニュース

ITmedia ニュース > セキュリティ > 年金情報流出から得られる教訓は――ラックが文書公...

2015年06月09日 18時32分 更新

年金情報流出から得られる教訓は――ラックが文書公開 「標的型攻撃の対策は、従来のウイルス対策と全く逆」(1/2)

「標的型サイバー攻撃は、従来のウイルス対策とは全く逆のアプローチをとるべき」――年金情報流出事件から学べる教訓や攻撃への対処方針についてまとめた文書をラックが公開した。

[ITmedia]

AUS便りからの所感等

- 折に触れて注意すべきなのは、官公庁・教育機関や大企業のみならず、中小企業でも標的型攻撃のターゲットとされる可能性は決して低くはないこと、また大多数のユーザが慎重に行動してマルウェアに感染しなかったとしても、ほんの数名のユーザのマルウェア感染によって標的型攻撃は成功することですが、しかしながら、そういった攻撃を認知した時点で十分な情報共有を行い、適切な対策をとれば、被害を最小限に食い止められることも不可能ではないことを当該文書は示しています。

- 標的型攻撃に対してとるべき対策法は多いですが、当該文書をはじめとした情報収集によってそれぞれ採用を検討すること、また例えば、単にUTMを設置するのみならず、不正な外部への通信を捕捉する等、標的型攻撃の検知を素早く行えるようにするための設定を確実に行うことが重要となるでしょう。