— AUS（アルテミス・ユーザ・サポート）便り 2016/02/22号 —
http://www.artemis-jp.com

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。

●日本郵政かたる不審メール急増･･･問合せ1日300件に

http://www.itmedia.co.jp/news/articles/1602/17/news147.html
http://www.japanpost.jp/information/2016/20160216115665.html

このニュースをザックリ言うと･･･

- 2月16日（日本時間）、日本郵政株式会社より、同社およびグループ会社の日本郵便株式会社をかたる不審なメールが送りつけられるケースが急増しているとして、警告が発表されました。

- 不審メールの事例には、「商品を配達するため電話で連絡したが、入力された電話番号に誤りがあったためつながらなかった」として、メールに添付されている「委託運送状」を印刷し、最寄りの「JAPANPOST取り扱い郵便局」まで問合せるように、といったものが挙げられています。

- 不審なメールに関する同社への問合せは15日から増え、1日300件を超えているとのことで、同社では、日本郵政および日本郵便からこのようなメールを送ることはないとして、安易にリンク先をクリックしたり、添付ファイルを開いたりしないよう注意を呼びかけています。

AUS便りからの所感等

- 同様の内容の不審メールについては、昨年12月18日にも同社が注意喚起を行っている他、委託運送状としている添付ファイルを開くことにより、オンラインバンキングの認証情報を奪取するマルウェア「Rovnix」(※)に感染する可能性が指摘されています。

- マルウェア添付メールについては、昨年は請求書やFAX受信通知に偽装したものも確認されており、マルウェアへの感染を誘導するための手口が日々洗練させている様子が伺えます。

- うっかりメールの内容に興味を持って添付ファイルを開いてしまうケースを未然に防ぐよう、メールの添付ファイル等を確実にアンチウイルスやUTMによってチェックする体制を整えることが肝要です。

ITmedia ニュース

速報　2016年02月17日 18時40分 更新

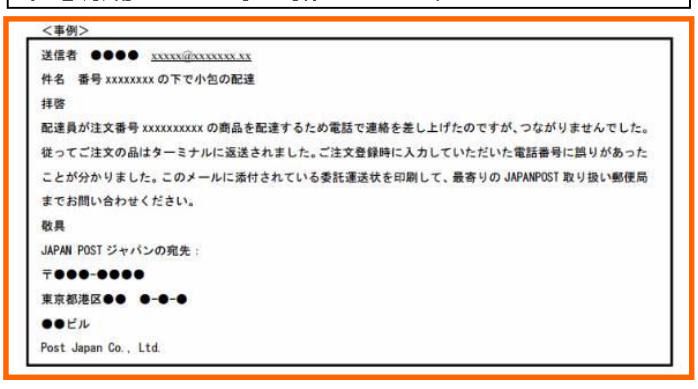
日本郵政かたる不審メール急増　注意を

日本郵政グループをかたる不審なメールが送りつけられるケースが急増しているとして、日本郵政が注意を呼び掛けている。

[ITmedia]

日本郵政グループをかたる不審なメールが送りつけられるケースが急増しているとして、日本郵政が注意を呼び掛けている。問い合わせが2月15日から増え、1日300件を超えているという。

不審メールの例は、「商品を配達するために電話で連絡したが、つながらなかった。最寄りのJAPANPOST 取り扱い郵便局まで問い合わせを」などとして連絡を求める内容。送信者欄に部分的に「日本郵政」「JAPAN POST」などと表示されているという。



＜事例＞

送信者　●●●●　xxxxx@xxxxxxx.xx
件名　番号 xxxxxxxx の下で小包の配達
拝啓
配達員が注文番号 xxxxxxxxxx の商品を配達するため電話で連絡を差し上げたのですが、つながりませんでした。
従ってご注文の品はターミナルに返送されました。ご注文登録時に入力していただいた電話番号に誤りがあったことが分かりました。このメールに添付されている委託運送状を印刷して、最寄りの JAPANPOST 取り扱い郵便局までお問い合わせください。
敬具
JAPAN POST ジャパンの宛先：
〒●●●-●●●●
東京都港区●●　●-●-●
●●ビル
Post Japan Co., Ltd.

不審メールの例＝ニュースリリースより

日本郵政 JP HOLDINGS

発表日：2016年2月16日
タイトル：日本郵政を騙った不審メールが急増していますのでご注意ください

日本郵政株式会社
日本郵便株式会社

2015年12月18日にも「日本郵政を装った迷惑メールについて」で日本郵政グループの名前を騙った不審メールについて注意喚起をさせていただいたところですが、再び不審メールが届いたというお問い合わせが急増しているため、再度ご注意いただきたく、お知らせいたします。

詳しくはこちらをご覧ください。
⇒日本郵政を騙った不審メールが急増していますのでご注意ください[PDF:48kバイト]
⇒日本郵政を装った迷惑メールについて（2015年12月18日）[PDF:47kバイト]

(※)「Rovnix」（不正送金マルウェア）
http://www.itmedia.co.jp/enterprise/articles/1512/17/news082.html

ITmedia ニュース

2015年12月17日 12時19分 更新

不正送金マルウェア「Rovnix」に新手口、偽画面で追加情報を盗む

国内の金融機関を狙うために攻撃手法がカスタマイズされているという。

[ITmedia]

セキュリティ企業のセキュアブレインは12月17日、インターネットバンキングの不正送金犯罪に使われるマルウェア「Rovnix」に、新たな攻撃機能が加わっていることを確認したとして注意を呼び掛けた。金融機関の通知に見せかけた画面を表示させ、その間にさまざまな情報を盗み取るという。

Rovnixはバックドア型のトロイの木馬の一種で、無数の亜種が存在するとみられる。セキュアブレインが解析したRovnixの検体は、国内の金融機関を標的にするようカスタマイズされていた。

●IPA「情報セキュリティ10大脅威 2016」発表、「ランサムウェア」はランク外から第3位に

https://www.ipa.go.jp/security/vuln/10threats2016.html

このニュースをザックリ言うと･･･

- 2月15日（日本時間）、独立行政法人情報処理推進機構（IPA）より、2015年に発生したセキュリティ事故・事件に関するもののうち、特に社会的に影響が大きかったと考えられるものを選定した「情報セキュリティ10大脅威 2016」が発表されました。

- 総合順位の1位は昨年と同様「インターネットバンキングやクレジットカード情報の不正利用」、2位は「標的型攻撃による情報流出」が昨年3位から上昇、さらに3位は昨年のランキング外から「ランサムウェアを使った詐欺・恐喝」が入りました。

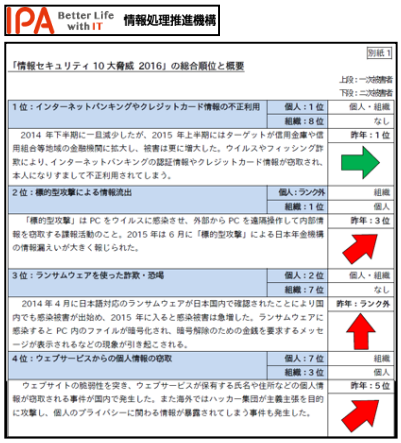
- いずれも日本国内で発生し、大きな話題となったものとなります。

AUS便りからの所感等

- ランサムウェアは、単にPC上のファイルを暗号化してしまうこと以上に、感染したPCから直接アクセス可能なUSBドライブ等のファイルにも被害をもたらす挙動が、これまで注目されていなかった対策が求められるようになるきっかけになったと言えます。

- 世の中でどういったセキュリティ上の事件が発生しているか随時情報収集を行い、さらにはどういった攻撃が注目されているかの知見を十分に得て、行うべき対策についても折に触れて追加や見直しを行うことが重要です。

- その一方で、アンチウイルスやUTM等のこれまで言われてきた防御策について確実に実行しているか、また攻撃に対して効果的な防御体制となっているかについてもまた、適宜確認は欠かせません。



IPA Better Life with IT 情報処理推進機構

別紙 1

「情報セキュリティ 10 大脅威 2016」の総合順位と概要

上段：一次被害者
下段：二次被害者

1 位：インターネットバンキングやクレジットカード情報の不正利用	個人：1 位	個人・組織
	組織：8 位	なし
2014 年下半期に一旦減少したが、2015 年上半期にはターゲットが信用金庫や信用組合等地域の金融機関に拡大し、被害は更に増大した。ウイルスやフィッシング詐欺により、インターネットバンキングの認証情報やクレジットカード情報が窃取され、本人になりすまして不正利用されてしまう。		昨年：1 位
2 位：標的型攻撃による情報流出	個人：ランク外	組織
	組織：1 位	個人
「標的型攻撃」は PC をウイルスに感染させ、外部から PC を遠隔操作して内部情報を窃取する諜報活動のこと。2015 年は 6 月に「標的型攻撃」による日本年金機構の情報漏えいが大きく報じられた。		昨年：3 位
3 位：ランサムウェアを使った詐欺・恐喝	個人：2 位	個人・組織
	組織：7 位	なし
2014 年 4 月に日本語対応のランサムウェアが日本国内で確認されたことにより国内でも感染被害が出始め、2015 年に入ると感染被害は急増した。ランサムウェアに感染すると PC 内のファイルが暗号化され、暗号解除のための金銭を要求するメッセージが表示されるなどの現象が引き起こされる。		昨年：ランク外
4 位：ウェブサービスからの個人情報の窃取	個人：7 位	組織
	組織：3 位	個人
ウェブサイトの脆弱性を突き、ウェブサービスが保有する氏名や住所などの個人情報が窃取される事件が国内で発生した。また海外ではハッカー集団が主義主張を目的に攻撃し、個人のプライバシーに関わる情報が暴露されてしまう事件も発生した。		昨年：5 位

●Androidに新手のマルウェア･･･10万台以上のデバイスに感染、遠隔操作される恐れ

http://www.itmedia.co.jp/enterprise/articles/1602/16/news059.html

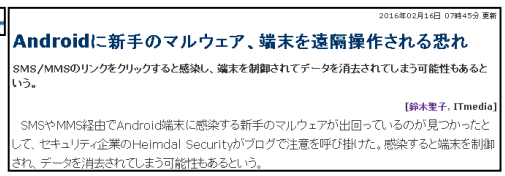
このニュースをザックリ言うと･･･

- 2月12日（現地時間）、デンマークのHeimdal Security社より、OSにAndroidを使用するスマートフォン等のデバイスにSMS（ショートメッセージサービス）やMMS（マルチメディアメッセージングサービス）経由で感染するマルウェア「Mazar BOT」について警告が発表されました。

- 不審なSMS等に記載されたリンクをクリックすることにより、Mazarが含まれたアプリがダウンロード・インストールされ、デバイスが完全に乗っ取られるようになっています。

- 同社によれば、デンマーク国内だけでも既に10万台以上のデバイスが感染しているとのことで、「SMSやMMS内のリンクをむやみに開かない」「アンチウイルスアプリをインストールしておく」「不審なWi-Fiスポットに接続しない」「VPN接続を使用する」等を呼びかけています。

AUS便りからの所感等



ITmedia エンタープライズ

2016年02月16日 07時45分 更新

Androidに新手のマルウェア、端末を遠隔操作される恐れ

SMS/MMSのリンクをクリックすると感染し、端末を制御されてデータを消去されてしまう可能性もあるという。

[鈴木聖子, ITmedia]

SMSやMMS経由でAndroid端末に感染する新手のマルウェアが出回っているのが見つかったとして、セキュリティ企業のHeimdal Securityがブログで注意を呼び掛けた。感染すると端末を制御され、データを消去されてしまう可能性もあるという。

- スマートフォンは今やPC以上に普及しており、既にマルウェアにとっては新たなる格好のターゲットとなりつつあります。

- Webサービス利用時に本人であることを厳密に確認する「二段階認証」では通常のネット回線とは異なる電話回線を通して送受信されるSMSが度々使われますが、マルウェアにこれを読み取られることにより、二段階認証さえも破られる恐れも指摘されています。

- デバイス上のデータやキー入力が傍受されたりすることのないよう、アンチウイルスアプリの導入等、とにかくマルウェアに侵入されないための対策をとることが肝心です。

- VPN接続は公衆Wi-Fiの使用時等に有効であり、特にUTMにおけるVPN機能を使用することにより、不審な通信の検知・遮断等に有用となるでしょう。