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。

●実在する組織からの注文連絡を装ったマルウェア添付メール･･･IPA改めて警告

http://news.mynavi.jp/news/2015/12/02/199/
https://www.ipa.go.jp/security/txt/2015/12outline.html

このニュースをザックリ言うと･･･

- 12月1日（日本時間）、独立行政法人情報処理推進機構（IPA）が毎月行っている「今月の呼びかけ」の12月度が発表され、実在する組織からの注文連絡等を装った添付ファイル付きメールについて警告しています。

- 問題となったメールは10月8日・27日および30日の各日に送信が確認されていたもので、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、不正なマクロを含むWord文書が添付されていたのが特徴です。

- IPAでは発生当時も警告を行っていましたが、今回改めて当該メールの特徴をまとめた警告を出しており、この他、トレンドマイクロ社も11月30日に、使用されたマルウェア「SHIZ」の解析結果に関する記事を同社ブログに掲載しています。

- IPAでは従来通りの対策として、「不用意に添付ファイルを開かない」「リンクをクリックしない」こと、また今回の添付ファイルの特徴を鑑み、同様のWord文書を開く際は「マクロが自動で有効になるような設定は行わない」「安全性が不明なファイルではマクロを有効にするための『コンテンツの有効化』を絶対クリックしない」こと、を呼びかけています。

AUS便りからの所感等

- 前述したIPAのページでは、問題となったメールが標的型攻撃で使われるパターンと似通っていることを挙げており、そこからもリンクされている「標的型攻撃メールの例と見分け方（https://www.ipa.go.jp/security/technicalwatch/20150109.html）」をはじめとした文書は、攻撃者がどういった内容のメール・添付ファイルでマルウェアへの感染を誘導するかを知り、防御を行うために必ず役に立つことでしょう。

- アンチウイルスやUTMをはじめとするセキュリティプロダクトの導入は、マルウェアに感染しないこと以上に、感染してしまった際のマルウェアの行動を迅速に把握し、被害を最小限に抑える上で重要不可欠となります。

マイナビニュース

実在する組織からの注文連絡を装ったばらまき型メールに注意－IPA

[2015/12/02]

IPA（情報処理推進機構）は12月1日、2015年10月の8日、27日、30日の各日において、実在する組織からの注文連絡等を装った添付ファイル付きメールが不特定多数の宛先に届くという事象が確認されたとして、注意を呼びかけた。

このメールは、「実在する組織を装っており、本文に不自然な言い回しがないなど、その内容に不審な箇所を見い出しにくい」「添付ファイル（ウイルス）がセキュリティソフトで検知できない」点など、標的型攻撃の手口と似ているという。

IPAは確認した相談および情報提供の内容から、ばらまき型メールの特徴には「メールの内容（件名や本文）」と「添付ファイル」に特徴があるとしている。

「メールの内容（件名や本文）」は、実在の組織をかたったり、FAXや複合機の自動送信を装ったりしており、特に組織をかたったメールの場合、日本語に不自然な表現もなく、一見では、不審をいだきにくい内容となっていたという。

IPA Better Life with IT 情報処理推進機構

表21　標的型攻撃メールの着眼点

(ア)メールのテーマ	① 知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容 (例1) 新聞社や出版社からの取材申込や講演依頼 (例2) 就職活動に関する問い合わせや履歴書送付 (例3) 製品やサービスに関する問い合わせ、クレーム (例4) アンケート調査
	② 心当たりのないメールだが、興味をそそられる内容 (例1) 議事録、演説原稿などの内部文書送付 (例2) VIP訪問に関する情報
	③ これまで届いたことがない公的機関からのお知らせ (例1) 情報セキュリティに関する注意喚起 (例2) インフルエンザ等の感染症流行情報 (例3) 災害情報
	④ 組織全体への案内
	(例1) メールボックスの容量オーバーの警告 (例2) 銀行からの登録情報確認
(イ)差出人のメールアドレス	① フリーメールアドレスから送信されている
	② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
(ウ)メールの本文	① 日本語の言い回しが不自然である
	② 日本語では使用されない漢字（繁体字、簡体字）が使われている

●三菱東京UFJ銀行から電話番号14,000件流出

http://www.itmedia.co.jp/news/articles/1512/01/news098.html

このニュースをザックリ言うと・・・

- 11月30日（日本時間）、三菱東京UFJ銀行は、出会い系サイト等のサービス運営者の預金口座47口座の入出金明細、およびそれに含まれる振込依頼人の電話番号約14,000件が流出したことを発表しました。

- 同行の「残高照会ダイヤル」について本人確認に関する不備があり、第三者が他の口座の入出金明細を聞き出すことが可能だったことが流出の原因とされており、電話番号の情報が架空請求詐欺に利用されていたことから今回の流出が発覚したとのことです。

ITmedia ニュース

2015年12月01日 12時56分 更新

三菱東京UFJ銀行、出会い系サイト口座へ振り込んだ1万4000件の電話番号流出か

三菱東京UFJ銀行の一部の口座入出金明細が不正アクセスで漏えいし、出会い系サイトに振り込んだ人の電話番号約1万4000件が流出した可能性が高いという。

[ITmedia]

三菱UFJ銀行は11月30日、出会い系サイト運営者の預金口座入出金明細が不正アクセスで漏えいし、出会い系サイトに振り込んだ利用者の電話番号約1万4000件が流出した可能性が高いと発表した。流出番号が架空請求詐欺に悪用されたことで発覚したという。

平成27年11月30日

株式会社三菱東京UFJ銀行

会員制サイト等の利用者として入力された電話番号の漏えいについて

今般、弊行にて、会員制サイト等のサービス運営者の預金口座入出金明細が漏えいし、当該明細に記載された一部の振込依頼人（＝会員制サイト等の利用者）であるお客さまの電話番号が架空請求詐欺に利用されていたことが判明いたしました。
関係者の皆さまにご迷惑、ご心配をおかけすることとなり、誠に申し訳なく、深くお詫び申し上げます。

1. 漏えいの概要
・ 今般漏えいした振込依頼人であるお客さまの情報は、電話番号またはカナ氏名(※1)であり、住所や口座番号等の情報は含まれておりません。
・ 架空請求詐欺に利用されていたのは電話番号のみであり、弊行で調査をしたところ、約1万4千件の電話番号が漏えいしている可能性があります。

発表の一部

AUS便りからの所感等

- 流出が発覚した個人情報は電話番号のみのようですが、入手した電話番号を悪用してのなりすまし、あるいはSNS上で検索されることにより、本人のみならず知り合いのユーザを検索される等の可能性を指摘する声もあり、重大性は十分に高いとみられます。

- 今回のような音声サービスの不備はインターネットサービスのそれに比べ見つけられにくく、それに特化した診断等を行って検証する必要があると考えられます。

- 一方で、電話番号やマイナンバーのような個人情報に紐付けられ得る番号情報を保存しているサーバへのインターネット経由での侵入、および情報の流出であれば、UTMの設置はそれを食い止める一助となり得ます。

●攻撃者が悪用するWindowsコマンド・・・JPCERT/CCが警告

https://www.jpcert.or.jp/magazine/acreport-wincommand.html

このニュースをザックリ言うと・・・

- 12月2日（日本時間）、セキュリティ専門機関JPCERT/CCより、PCへ不正アクセスする攻撃者が侵入したWindows PC上で使用するコマンドについての調査結果が発表されました。

- 発表では、攻撃者の攻撃フェーズを「(1)初期調査：感染した端末の情報を収集する」「(2)探索活動：感染した端末に保存された情報や、ネットワーク内のリモート端末を探索する」「(3)感染拡大：感染した端末を別のマルウエアにも感染させる、または別の端末にアクセスを試みる」の3段階に分け、それぞれでどういったコマンドが使用されるかについて示しています。

- また、これに対する対策として、AppLocker（マイクロソフトのWindows7、Server2008 R2から導入された、特定のアプリケーションの実行の許可/拒否を管理するセキュリティ機能）やソフトウエア制限ポリシーを用いた、一部コマンドの実行を制限する方法を解説しています。

JPCERT CC

表1：初期調査(上位10コマンド)

順位	コマンド	実行数
1	tasklist	155
2	ver	95
3	ipconfig	76
4	systeminfo	40
5	net time	31
6	netstat	27
7	whoami	22
8	net start	16
9	qprocess	15
10	query	14

表2:探索活動(上位10コマンド)

順位	コマンド	実行数
1	dir	976
2	net view	236
3	ping	200
4	net use	194
5	type	120
6	net user	95
7	net localgroup	39
8	net group	20
9	net config	16
10	net share	11

AUS便りからの所感等

- Windowsのバージョンが進むごとにセキュリティに関する機能も増えていますので、そういった追加されたセキュリティ機能の存在を把握し、設定を行うことにより、PCのセキュリティを高度にすることを強く推奨します。

- また、組織内の多数のPCに対してそういったセキュリティ機能を一括して設定するためにも、家庭向けエディションではなくProエディション（Windows7 Professional、Windows8.1 Pro）の導入を行うべきでしょう。

- 今回の調査結果の活用次第では、アンチウイルスやUTMにおけるマルウェアの振る舞いを分析して検知する機能に役立てられ、検知率が向上することも期待されます。