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。

●ランサムウェアに感染させる4種の日本語スパムメール、共通のサイバー犯罪者によるものか･･･トレンドマイクロ

http://internet.watch.impress.co.jp/docs/news/1031371.html
http://blog.trendmicro.co.jp/archives/14066

このニュースをザックリ言うと･･･

- 11月10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、ランサムウェア「STAMPADO」「MISCHA」への感染を目的とする日本語スパムメールが10月31日以降確認されているとして注意喚起が出されおり、また、11月21日には、4種類の日本語スパムメールの分析結果について発表されました。

- 対象となったのは、件名に「システム改修のお知らせとご協力のお願い」や「【受任のお知らせ】」を含むもの、それに、「【重要】総務省共同プロジェクト」で始まるマルウェア感染者への注意喚起、および除去ツールの配布をかたるものです（後半の2件については、一般社団法人ICT-ISACあるいはNTTコミュニケーションズをかたって送信されているとのことです）。

- 分析結果によれば、これらはいずれも同じ海外の匿名フリーメールサービス「SIGAINT」を使用、同じオンラインストレージサービス「MEGA」からマルウェアをダウンロードさせる点で共通しており、またマルウェア除去ツールをかたる2件に添付されたPDF文書はいずれも「Windows Difender」という誤字を含んでいたとのことです。

- 以上の点から、同社は4種類のスパムメールは全て共通のサイバー犯罪者がいると推測しています。

AUS便りからの所感等

- 今回分析されたスパムメールは、同社においてそれぞれ数十通が検出されている程度と、また大規模な拡散はない模様ですが、ランサムウェアによる攻撃が日本を本格的にターゲットとした兆候の一つととられており、今後本格的に活動を開始することも、また今回の発表を受けて攻撃者側が対策をとってくることも十分に考えられます。

- ランサムウェアの登場は、とるべきセキュリティ対策の見直しが迫られてきており、アンチウイルスやUTMを採用する最低限の対策の上で、万が一検出できず感染してしまった際に被害を最小限に抑えられるよう、ネットワーク構成の見直しの検討、PC毎の確実なデータ等バックアップ体制の確立が重要となってくるでしょう。

INTERNET Watch

ニュース

ランサムウェアに感染させる4種の日本語スパムメールの特徴まとめ、共通のサイバー犯罪者によるものか～トレンドマイクロ

岩崎 宰守　2016年11月22日 18:43

トレンドマイクロ株式会社は、10月以降に確認されているランサムウェアを頒布する4種類の日本語のスパムメールについて、詳細をブログで報告している。

4種類の日本語スパムメールは、いずれも海外の匿名フリーメールサービス「SIGAINT」が送信元となる。現時点で確認されているのは、1）10月2日以降に確認されている、件名に「システム改修のお知らせとご協力のお願い」の文字列を含むもの、2）10月27日以降に確認されている、件名に「【受任のお知らせ】」の文字列を含むもの。いずれもファイルは添付されていないが、1つ目は修正パッチの名目で、2つ目は法律事務所からの文書をうたい、メール本文に記載されたURLから、海外のクラウドストレージサービス「MEGA」より、前者はランサムウェア「STAMPADO」、後者は「MISCHA」をダウンロードさせる。

TREND MICRO トレンドマイクロ セキュリティブログ

2016年10月から継続して確認される巧妙な日本語メールと頒布されるランサムウェアを解析

投稿日: 2016年11月21日
脅威カテゴリ: 不正プログラム，統括，日本発
執筆: セキュリティエバンジェリスト 岡本 勝之

2016年10月以降、トレンドマイクロではランサムウェアの頒布を目的とした日本語マルウェアスパムの流布を継続して確認していることは、11月10日の記事でお伝えしました。このサイバー犯罪者が新たに日本を標的とし始めたことを示す事例について、今回は続報として確認された日本語メールのまとめと頒布されるランサムウェア自体についての解析をお伝えします。

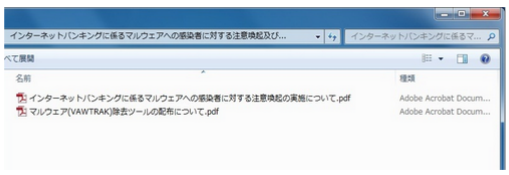


図1:マルウェアスパムの添付PDFファイルの例

●あらゆるPCから情報を抜き取れるUSBデバイス「PoisonTap」

http://pc.watch.impress.co.jp/docs/news/1030533.html

このニュースをザックリ言うと・・・

- 11月16日（現地時間）、ハッカーのSamy Kamkar氏より、小型コンピュータ「Raspberry Pi Zero」による強力なハッキングデバイス「PoisonTap」が発表されています。

- PoisonTapはUSB接続のネットワークデバイスとして動作し、接続したPCにDHCPでIPアドレスを付与することにより、PCが外部への通信にPoisonTapを通るよう仕向ける他、GoogleやYouTube、Facebook等へのHTTP通信を横取りし、ブラウザからCookieを奪取するといった挙動を取るとのことです。

- PoisonTapは5ドルで製作可能で、ソースコードは公開されており、作者のKamkar氏は、こういうデバイスへの対抗手段として、WebサイトにHTTPSを使用すること等を推奨しています。

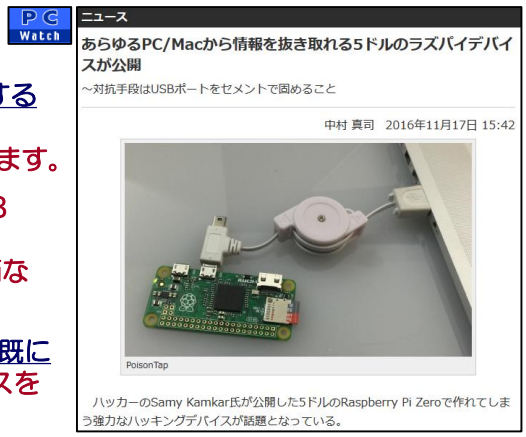
AUS便りからの所感等

- 今回発表されたPoisonTapはあくまでUSBデバイスを安易に接続することの危険性等を説くコンセプトのためのものとみられますが、別の攻撃者がより見つかりにくい外見のデバイスを作成する可能性もあります。

- Kamkar氏はこういったUSBデバイスを接続されないよう、「USBポートをセメントで塞ぐこと」といった冗談めいた回避策も推奨していますが、こういう強引な手段ではなくとも、USBポートを塞ぐ安価なセキュリティ製品は既にいくつか発売されています。

- 出所が不明なUSBデバイスがマルウェア感染の経路となるケースは既に珍しくなく（AUS便り 2016/10/03号参照）、そういったデバイスを安易に接続しない等、ユーザ側で各種対策をとることは重要です。

- しかし、さらなる安全なUSBデバイスの利用のため、OS側でのセキュリティ機構が確立されることに期待したいものです。


PC Watch
ニュース
あらゆるPC/Macから情報を抜き取れる5ドルのラズパイデバイスが公開
～対抗手段はUSBポートをセメントで固めること
中村 真司　2016年11月17日 15:42
PoisonTap
ハッカーのSamy Kamkar氏が公開した5ドルのRaspberry Pi Zeroで作れてしまう強力なハッキングデバイスが話題となっている。

●Googleではない謎のサイト「google.com」が出現

http://gigazine.net/news/20161122-google-is-not-google/

このニュースをザックリ言うと・・・

- 11月21日（現地時間）、Googleアナリティクス等の分析ツール「Analytics Edge」の開発者より、Googleとは関係ない「google.com」というドメイン名を持つサイトが確認されたと発表されました。

- 1文字目が通常のアルファベットではなくラテン文字のスモールキャピタルのいわゆる「国際化ドメイン名（IDN）」となっており、アクセスすると別の長いサイト名を持つスパムサイトに誘導されるようになっています。

- Webサイトのアクセス解析結果にこのドメイン名をアクセス元とする記録が大量に残され、サイトのオーナーがこのスパムサイトにアクセスするよう誘導するのが狙いとみられます。

- 当該開発者は、コンピュータに損害を与える恐れもあるとして、このドメイン名のサイトにアクセスしないよう呼び掛けています。

AUS便りからの所感等

- ドメイン名にアルファベット・数字以外の文字（漢字、ギリシャ文字、キリル文字等）を使えるようにするIDNは、内部ではPunycode（「xn--」で始まるASCII文字のみの形式）に変換して用いられます。

- IDNは当初からフィッシング等への対策が検討され、例えばブラウザ側では、特定の条件外の文字を含むドメイン名をそのままの表記ではなく、Punycode形式で表示するようになっていますが、Webアプリケーション側でも同様の対応がされているとは限らないこともあり、誘導されてしまうケースは皆無とは言えません。

- 今回の「google.com」のようなIDNを登録するのはフィッシング目的以外には到底考えられず、このようなドメインのサイトについて、今後UTM等各種セキュリティ製品やブラウザのアンチフィッシング機能において順次対象に登録されていくことに期待したいものです。


GIGAZINE
2016年11月22日 20時00分00秒
GoogleのようでGoogleではない謎のサイト「google.com」が出現
“G”oogle
Google Analyticsはスパマーのターゲットとなっていて、ユーザーがどこからやってきたのかチェックしている人をアクセス元であるかのように見せかけてスパムサイトへ誘導するという手口が存在します。そのアクセス元が「google.com」となっていると「google」で何かの検索フレーズが引っかかったのだろうか」などと思ってしまいそうですが、この「google.com」は「Google.com」ではないスパムサイトなので絶対にアクセスしないようにしてください。「G」が違います。