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。

●「注文確認」や「複合機の通知」のウイルスメールに注意！1万3000通以上を確認

http://itpro.nikkeibp.co.jp/atcl/news/15/100903331/
http://blog.trendmicro.co.jp/archives/12343

このニュースをザックリ言うと･･･

- 10月9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、同8日朝から合計1万3000通以上のウイルスメールの送信が確認されたとして警告が発表されました。

- ウイルスメールは同時に2種類が確認されており、

◆1つ目は件名に「ご注文ありがとうございました―添付ファイル「出荷のご案内」を必ずご確認ください」といった文言を含んだ通販サイトからの連絡を装ったメール

◆2つ目は本文の最後に「西東京複合機より送信」と書かれた複合機からの通知を装ったメール

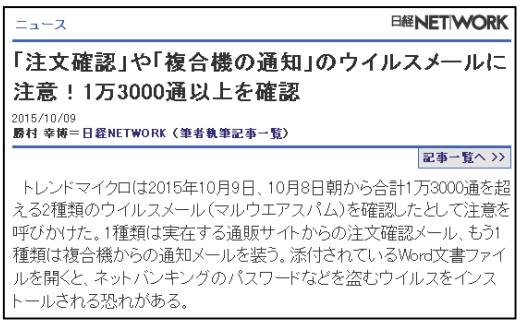
となっています。

- いずれのメールも不正なマクロを含むWordファイルが添付されており、ネットバンキングのパスワードを奪取するようなマルウェアをダウンロードする仕組みになっているとのことです。

AUS便りからの所感等

- 通販サイトに偽装したメールは今年9月に、複合機からの通知に偽装したメールは6月にも確認されていましたが、トレンドマイクロ社によれば、2種類のメールが同時に同じマルウェアを拡散させるケースは初めてとのことです。

- マルウェアや不正なマクロを含む文書が添付されるようなメールを防御するためには、通常利用しているサイトや機器等には有り得ない形でメールが送信されてきた際に十分に警戒することも一助になるでしょうが、標的型攻撃においては、ターゲットとなる組織で利用される機器やユーザがよく利用するサイトについて攻撃者が入念に調査し、文面を似せたメールを作成することも考えられるため、結局はアンチウイルスやUTMの導入が不可欠となるでしょう。

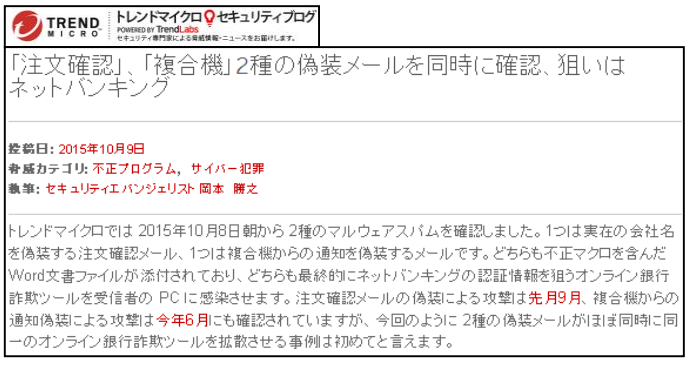

ニュース　日経NETWORK

「注文確認」や「複合機の通知」のウイルスメールに注意！1万3000通以上を確認

2015/10/09
勝村 幸博＝日経NETWORK（筆者執筆記事一覧）

記事一覧へ >>

トレンドマイクロは2015年10月9日、10月8日朝から合計1万3000通を超える2種類のウイルスメール（マルウエアスパム）を確認したとして注意を呼びかけた。1種類は実在する通販サイトからの注文確認メール、もう1種類は複合機からの通知メールを装う。添付されているWord文書ファイルを開くと、ネットバンキングのパスワードなどを盗むウイルスをインストールされる恐れがある。


TREND MICRO　トレンドマイクロ セキュリティブログ
POWERED BY TrendLabs

「注文確認」、「複合機」2種の偽装メールを同時に確認、狙いはネットバンキング

投稿日: 2015年10月9日
脅威カテゴリ: 不正プログラム, 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 2015年10月8日朝から 2種のマルウェアスパムを確認しました。1つは実在の会社名を偽装する注文確認メール、1つは複合機からの通知を偽装するメールです。どちらも不正マクロを含んだWord文書ファイルが添付されており、どちらも最終的にネットバンキングの認証情報を狙うオンライン銀行詐欺ツールを受信者の PC に感染させます。注文確認メールの偽装による攻撃は先月9月、複合機からの通知偽装による攻撃は今年6月にも確認されていますが、今回のように 2種の偽装メールがほぼ同時に同一のオンライン銀行詐欺ツールを拡散させる事例は初めてと言えます。


2015/10/08 (木) 6:06
R OrderConfirm JP <OrderConfirm.JP@[redacted].com>
[redacted]様]ご注文ありがとうございました－添付ファイル「出荷のご案内」を必ずご確認ください
宛先 [redacted]
メッセージ 1312061102_132339395E.doc (89 KB)

カスタマーナンバー:17374973-00001
オーダーNo.:132339395E

この度は [redacted] へご注文をいただき、誠に有難うございます。

「出荷のご案内」では、在庫不足や取扱終了、代替品のご案内をしています。
出荷となった商品は配送伝票番号と出荷日が、受注当日お届け出来なかった商品はその理由と出荷予定日を案内しています。
必ず添付の「出荷のご案内(.pdf ファイル)」をご確認ください。

◆◆[redacted] からご注文いただきましたお客様へ
注文直後に送信される「ご注文内容確認」メールの内容と実際の受注状況とは異なることがあります。必ず「出荷のご案内」で内容をご確認ください。

○本メールは送信専用です。必ず下記リンクからご返信ください。
◆出荷のご案内の配信方法をFAXに変更したい方(本文に必ずFAX番号をご記入ください)
mailto:[redacted]

図1●出回っているウイルスメールの例（トレンドマイクロの情報から引用。企業名などは修整されている）


2015/10/08 (木) 8:08
[redacted]0026738E40D2@[redacted].co.jp
Message from "[redacted]0026738E40D2"
宛先 [redacted]
メッセージ 20151007112034511.doc (89 KB)

このメールは（[redacted]0026738E40D2 (IP [redacted] JPN）から送信されたものです。

読み取り日時: 2015.10.08 7:20:34 (+0900)
問い合わせ先: [redacted]

西東京複合機より送信

図2●出回っているウイルスメールの例（トレンドマイクロの情報から引用。一部修整されている）

●2015年度第2四半期のインシデント報告件数は4,128件、前期より減少もサイト改ざん続く･･･JPCERT/CC

http://news.mynavi.jp/news/2015/10/12/030/

このニュースをザックリ言うと･･･

- 10月8日（日本時間）、一般社団法人JPCERT/CC（※）より、2015年度第2四半期（7月1日～9月30日）の「インシデント報告対応レポート」が公開されました。

- この期間のインシデント報告件数は計4,128件で、内訳は7月が1,543件、8月が1,215件、9月が1,370件となっており、2,981件が報告された1月に比べて月ベースでは半分まで減少しています。

- インシデントにおける各カテゴリの割合としては、システムの弱点を探索するスキャン系が過半数の53.0%、続いてWebサイト改ざん関連が15.8%、フィッシングサイト関連が13.9%となっており、Webサイト改ざんについては592件が確認されたとのことです。

IT用語辞典 e-Words

（※）JPCERT/CC（ジェーピーサートシーシー）（JPCERTコーディネーションセンター）【 Japan Computer Emergency Response Team/Coordination Center 】

JPCERT/CCとは、インターネットを介して発生するコンピューターセキュリティに関連する事象の情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信などを行う組織。日本の代表的なCSIRT（Computer Security Incident Respose Team）で、国内外の情報セキュリティ対策活動のコーディネートを行っている。

インターネット定点観測システム「ISDAS」の運用や、日本国内におけるインシデント報告の受付対応、インシデント情報の国内外のネットワーク管理者への情報連携も行う。さらに、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づいて報告されたソフトウェア等製品の脆弱性情報に関する日本国内の製品開発者との調整活動では、海外のCSIRTからの脆弱性情報の国内製品開発者への展開も行っている。日本国内の製品開発者の脆弱性対応状況を公開するサイト「JVN」の運営を情報処理推進機構（IPA）と共同で行っている。

また、日本で初めて、国際的なCSIRTが集まるフォーラムである「FIRST」に加盟、アジア太平洋地域におけるCSIRTが集まる「APCERT」の事務局もつとめている。

AUS便りからの所感等

- 2013年度以降の月間のインシデント報告件数は、2013年5月～9月と2014年12月～2015年1月に3,000件前後以上に急上昇したことを除けば、1,000件台を推移し続けている模様で、またWebサイト改ざんについてもこの1年間は月間200件前後で推移しており、なかなか減少する気配がありません。

- この状況を劇的に改善するような技術や製品がそう簡単に登場する可能性は低く、アンチウイルス・UTMの設置やメンテナンスをはじめとする地道なセキュリティ対策の実施と維持を油断することなく続けていくことが肝心でしょう。

●Flash Player最新版リリースも未修正の脆弱性

http://internet.watch.impress.co.jp/docs/news/20151014_725579.html

このニュースをザックリ言うと･･･

- 10月13日（米国時間）にFlash Player（※）のセキュリティアップデート19.0.0.207（Windows版・以下同様）がリリースされましたが、当該バージョンでも未修正の脆弱性「CVE-2015-7645」が存在することがAdobe社およびトレンドマイクロ社より発表されました。

- トレンドマイクロ社によれば、以前から同社が警告していた標的型サイバー攻撃「Pawn Storm」において、今回前述の脆弱性を突くゼロデイ攻撃が確認されており、既に各国の外務省に対し標的型メールによる攻撃が発生しているとのことです。

- Adobe社はさらなるアップデートを10月19日の週にリリースすることを予告しています（※10月16日、19.0.0.226がリリースされました）。

IT用語辞典 e-Words

（※）Flash Player【 フラッシュプレーヤー 】Flashプレーヤー / Adobe Flash Player

Flash Playerとは、「Adobe Flash」で作成したコンテンツをWebブラウザなどで再生するためのプラグインソフト。Adobe社のWebサイトから無償でダウンロードできる。同社によると世界で8億台以上のコンピュータにFlash Playerが組み込まれているという。

（※）プラグイン【 plug-in 】

プラグインとは、差し込む、差込口などの意味を持つ英単語。ITの分野では、ソフトウェアに機能を追加する小さなプログラムのことを指す場合が多い。

多くのソフトウェアには外部のプログラムを追加することで機能を拡張できるような機構を備えており、追加するソフトウェアのことをプラグイン（プラグインソフトウェア）という。ほとんどのプラグインは単体では動作せず、本体のソフトウェアに追加しなければ機能しない。プラグインはソフトウェア製作者が提供する場合もあるが、仕様が公開され、第三者が自由にプラグインを開発・公開できるようになっていることも多い。

AUS便りからの所感等

- Flash Playerについては、7月にもセキュリティアップデートで修正されなかった脆弱性がゼロデイ攻撃に悪用されるケースが発生しており、つい先週には、悪意のある広告によって誘導し、Flash Playerの脆弱性を突く攻撃についても話題になったばかりです。

- こういった脆弱性に対しては、アンチウイルス・UTMを導入することは、最新のセキュリティアップデートを適用するまでのタイムラグにおける防御策として非常に重要です。

- また、Flashコンテンツを含む等プラグイン（※）が必要となるサイト以外では、プラグインを無効にする設定もブラウザによっては可能ですので、一時的ないし常時の回避策として十分検討に値することでしょう。