— AUS（アルテミス・ユーザ・サポート）便り 2017/04/17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。

●件名「の陳述書」はウイルスメール、警視庁等が警告

http://itpro.nikkeibp.co.jp/atcl/news/17/041301129/
https://www.jc3.or.jp/topics/virusmail.html

このニュースをザックリ言うと･･･

- 4月12日（日本時間）、警視庁と日本サイバー犯罪対策センター（JC3）より、陳述書やFAX等を装った、ウイルスが添付されたメールが同日から拡散しているとして警告が出されています。

- JC3によれば、確認されたメールは以下の3種類で、いずれもPDFやWord文書を装ったウイルスがzip形式で添付されています。

① 件名が「の陳述書」、本文が「PDFですが、がひっくり返っていますので見難いかと思いますが」で始まるもの

② 件名が「From ″0462{数字}0″(Fax Message NO.{数字})」、本文が「このメールは『RNP00{数字}』（MP C{数字}A JPN）から送信されたものです。」で始まるもの

③ 件名が「[日本郵便]集荷依頼申込み完了のお知らせ」「送り状の用意：用意済み」「集荷希望日」のいずれか、本文が「この度は日本郵便のWeb集荷サービスをご利用頂きありがとうございます。」で始まるもの

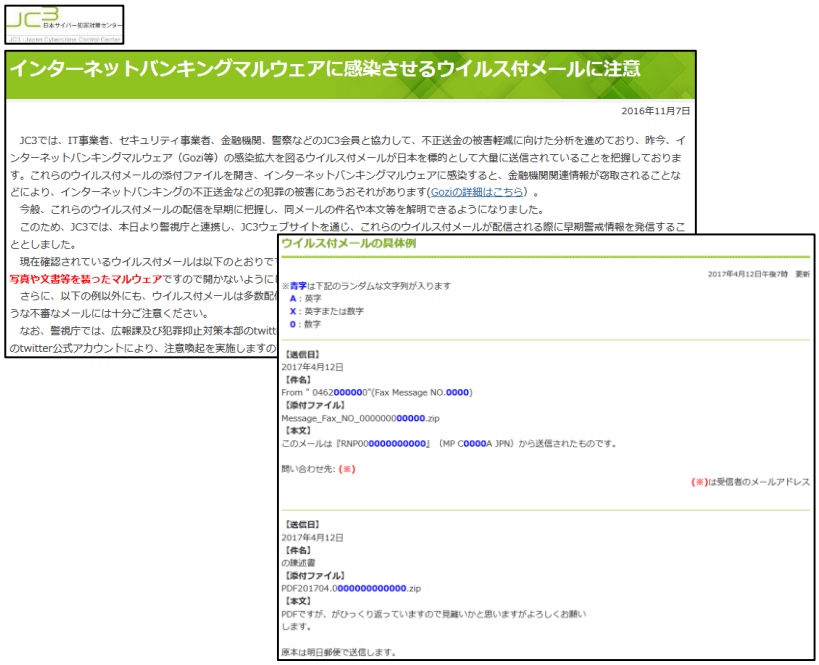
AUS便りからの所感等

- 挙げられている3種類のメールは、例えば、①については2月22日にも拡散が確認されて警告が出されている等、いずれも今回初めて確認された文面ではありません。

- 一方で、添付されるウイルスが新しいものとなっているためか、UTMのチェックを通過してしまうケースも稀にあることから、アンチウイルスとの二重でのチェックがマルウェアに対する防御のためには有効となります。

- 前述したJC3のページやTwitterといったSNSでの言及等、ウイルスメールの拡散についての情報収集を常に行っておくこともマルウェアへの感染の可能性を最小限に抑える一助となることでしょう。


速報
「の陳述書」メールはウイルス付き、警視庁が警告
斉藤 貴之＝日経NETWORK　2017/04/13　日経NETWORK
目次一覧
警視庁と日本サイバー犯罪対策センター（JC3）は2017年4月12日、件名が「の陳述書」だったり、ファックスを装ったりした、ウイルスが添付されたメールが同日から拡散していると注意を呼び掛けた。
警視庁は、犯罪抑止対策本部のTwitterアカウントを使って告知。件名が「の陳述書」のメールはPDF文書を装ったウイルスが添付され、件名が「From"0462｛数字｝0"（Fax Message NO.｛数字｝）」のメールはファックスのように見えるが、Wordファイルを装ったウイルスが添付されていると注意している。
警視庁犯罪抑止対策本部 @MPD_yokushi　フォローする
【サイバー犯罪対策課】
ウイルス付メールが拡散中！件名は「の陳述書」。メール本文は、添付ファイルの確認を求める内容となっていますが、添付ファイルはPDF文書を装ったウイルスです。ご注意ください！
114 リツイート　55 いいね
17:57 - 2017年4月12日
警視庁犯罪抑止対策本部のTwitter。
[画像のクリックで拡大表示]


インターネットバンキングマルウェアに感染させるウイルス付メールに注意
2016年11月7日
JC3では、IT事業者、セキュリティ事業者、金融機関、警察などのJC3会員と協力して、不正送金の被害軽減に向けた分析を進めており、昨今、インターネットバンキングマルウェア（Gozi等）の感染拡大を図るウイルス付メールが日本を横断として大量に送信されていることを把握しております。これらのウイルス付メールの添付ファイルを開き、インターネットバンキングマルウェアに感染すると、金融機関関連情報が窃取されることなどにより、インターネットバンキングの不正送金などの犯罪の被害にあうおそれがあります(Goziの詳細はこちら)。
今般、これらのウイルス付メールの配信を早期に把握し、同メールの件名や本文等を解明できるようになりました。
このため、JC3では、本日より警視庁と連携し、JC3ウェブサイトを通じ、これらのウイルス付メールが配信される際に早期警戒情報を発信することとしました。
現在確認されているウイルス付メールは以下のとおりで
写真や文書等を装ったマルウェアですので開かないように
さらに、以下の例以外にも、ウイルス付メールは多数配
うな不審なメールには十分ご注意ください。
なお、警視庁では、広報課及び犯罪抑止対策本部のtwitt
のtwitter公式アカウントにより、注意喚起を実施します
ウイルス付メールの具体例
2017年4月12日午後7時　更新
○青字は下記のランダムな文字列が入ります
A：英字
X：英字または数字
0：数字
【送信日】
2017年4月12日
【件名】
From " 0462000000"(Fax Message NO.0000)
【添付ファイル】
Message_Fax_NO_0000000000000.zip
【本文】
このメールは『RNP000000000000』（MP C0000A JPN）から送信されたものです。
問い合わせ先：(※)
(※)は受信者のメールアドレス
【送信日】
2017年4月12日
【件名】
の陳述書
【添付ファイル】
PDF201704.0000000000000.zip
【本文】
PDFですが、がひっくり返っていますので見難いかと思いますがよろしくお願いします。
原本は明日郵便で送信します。

●Windows・Officeにおけるゼロデイ脆弱性確認、パッチ適用を

http://blog.trendmicro.co.jp/archives/14694

このニュースをザックリ言うと・・・

- 4月7日（現地時間）、セキュリティベンダーのマカフィー社およびファイア・アイ社より、Microsoft Officeの全てのバージョンに未対策の脆弱性が存在し、これを悪用するゼロデイ攻撃が確認されたと相次いで発表されました。

- この発表の時点では、脆弱性はOfficeアプリケーションのうちWordに存在するものとされ、メールに添付された不正な文書ファイルを開くことにより、密かにマルウェアをダウンロードして実行するケースが挙げられていました。

- しかし、4月12日（日本時間）、Microsoftからの月例のセキュリティパッチリリースにより、Officeの他にWindowsのワードパッドについても脆弱性の対策が行われており、IPA等からも至急アップデートを行うよう呼び掛けられています。

AUS便りからの所感等

- 脆弱性はRTF（リッチテキストフォーマット）と呼ばれる形式の文書ファイルの処理において存在するもので、RTF文書では拡張子として、.rtfの他、古いWord形式と同じ.docが用いられる場合もあります。

- マカフィーによれば、この脆弱性を悪用したファイルによる攻撃は、Officeの「保護ビュー」で開いた場合は機能しないとのことですが、メーラーやzipファイル等の展開ツールによっては、ファイルを保護ビューで開くよう指定する情報が付加されないケースがある模様で、この他、攻撃者が巧みに保護ビューを解除するよう誘導する可能性もありますので、これに依存することは得策ではありません。

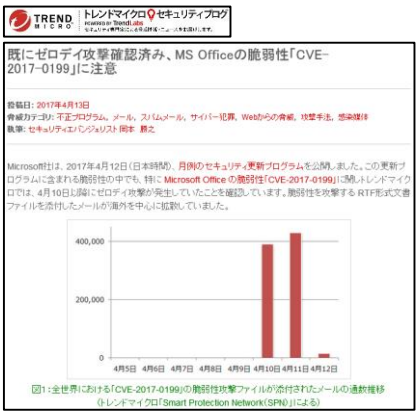


図1：全世界における「CVE-2017-0199」の脆弱性攻撃ファイルが添付されたメールの通数推移（トレンドマイクロ「Smart Protection Network(SPN)」による）

- トレンドマイクロ社の情報では、4月10日から11日にかけてゼロデイ攻撃が確認されたものの、パッチがリリースされた12日には沈静化したとされていますが、いつ攻撃が再度活発化するか、油断は禁物であり、各種セキュリティパッチを必ず適用し、加えてアンチウイルスとUTMによる防御が確実に行うことが重要です。

●BINDに3件の脆弱性、アプライアンスについても注意を

http://www.jpcert.or.jp/at/2017/at170016.html

このニュースをザックリ言うと・・・

- 4月13日（日本時間）、DNSサーバソフト「BIND」について3件の脆弱性が発表され、開発元の米ISCより修正バージョン（BIND 9.11.0-P5/9.10.4-P8/9.9.9-P8）がリリースされたことを受けてJPCERT/CC等から警告が出されています。

- 脆弱性のうち最も危険な1件（CVE-2017-3137）では、攻撃者が用意したDNSサーバに問合せを送信するよう誘導され、細工されたDNS応答を受信することにより、DNSサーバプロセス（named）を不正に落とされる可能性があるため、BINDをDNSキャッシュサーバとして利用しているあらゆる組織について早急なアップデートが推奨されています。

AUS便りからの所感等

- BINDは今年に入ってからだけでも1月・2月にセキュリティアップデートがリリースされる等、アップデートの頻度が比較的高いソフトウェアですので、ISCやLinuxディストリビューションのベンダーからアップデートがリリースされ次第、可能な限り速やかに適用できる体制を整えておくことは重要でしょう。

- 社内ネットワークに設置しているDNSキャッシュサーバの前面にUTMを設置することにより、不正なDNSサーバとの通信を遮断できる可能性がある一方、UTMを含めたアプライアンスにおいてBINDを利用している場合、逆に脆弱性の影響を受ける恐れがありますので、こういった機器でアップデートが必要かどうかの確認もまた、必要不可欠です。