— AUS（アルテミス・ユーザ・サポート）便り 2018/07/09号 —
https://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。

●「あなたのアカウントは閉鎖されます」…Amazonをかたるフィッシングに注意喚起

http://www.itmedia.co.jp/news/articles/1806/29/news098.html
https://www.antiphishing.jp/news/alert/amazon_20180629.html
https://www.antiphishing.jp/news/alert/apple_amazon_20180604.html

このニュースをザックリ言うと･･･

- 6月28日（日本時間）に日本サイバー犯罪対策センター（JC3）より、同29日にフィッシング対策協議会より、Amazon.co.jpをかたるフィッシングメールが出回っているとして注意喚起が出されています。

- フィッシングメールは、件名が「アラート:あなたのアカウントは閉鎖されます。」、本文が「大変申し訳ございません、あなたのアカウントは閉鎖されます。あなたのアカウントAmazonを更新できませんでした…」等と書かれたHTMLメールで、「アカウント検証」と書かれたリンクから、Amazonのアカウント情報および住所・氏名・クレジットカード等の個人情報の入力を求める偽のページへ誘導するものとなっています。

- 7月4日にも全く同じ内容のフィッシングメールの拡散が確認されています。

AUS便りからの所感等

- フィッシング対策協議会が6月4日に注意喚起を出していた、Appleをかたり、なぜかAmazonの偽サイトに誘導するフィッシングメールと文面等が似通っており、同一の犯行グループによるとみられます。

- 7月には既に楽天やソフトバンクをかたるフィッシングメールが確認されている他、件名が「写真送付の件」「写真送付」「イメージ送付」「7月度発注書送付」「invoice／証明書」「注文書をお送りいたします」といった、マルウェアが添付されたメール等も拡散しています。

- 必ずPCのアンチウイルスソフトやWebブラウザのセキュリティ機能を有効にし、他にもUTMの設置、使用するサイトへはブックマーク登録してアクセスすること等、各種防衛策を複数実施することにより、フィッシングやマルウェアメールからの防御を徹底することが肝要です。


ITmedia NEWS

「あなたのアカウントは閉鎖されます」Amazonかたるフィッシングメール出回る

2018年06月29日 12時20分 公開 [ITmedia]

印刷 通知 349 185 B! 9

「あなたのアカウントは閉鎖されます」という件名で、Amazon.co.jpをかたるフィッシングメールが出回っているとし、日本サイバー犯罪対策センター（JC3）6月28日、注意を呼び掛けた。

フィッシングメールの文面（JC3のWebサイトより）

Amazonのロゴ入りHTMLメールで、本文には「大変申し訳ございません、あなたのアカウントは閉鎖されます。あなたのアカウントAmazonを更新できませんでした」などと書かれ、「アカウント検証」と書かれたリンクも添えられている。リンクをクリックすると、フィッシングサイトに誘導される。

リンクをクリックしたり、フィッシングサイトに個人情報やクレジットカード情報などを入力しないよう注意が必要だ。


フィッシング対策協議会 Council of Anti-Phishing Japan

Amazon をかたるフィッシング (2018/06/29)

概要
Amazon をかたるフィッシングメールが出回っています。
メールの件名
アラート:あなたのアカウントは閉鎖されます。
詳細内容
Amazon をかたるフィッシングの報告を受けています。
1. 2018/06/29 14:00 現在、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のため
です。類似のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。
2. このようなフィッシングサイトにて、ログイン情報 (E メールまたは携帯電話番号、パスワード)、
名、郵便番号、都道府県、住所、電話番号)、クレジットカード情報 (カード名義人、カード番号、セ
ド、月、年) 等を絶対に入力しないように注意してください。
3. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphish
絡ください。
サイトのURL
メール内の URL
http://securitymanagment-supprt-●●●●.com/
http://securityprotection-supprt-●●●●.com/ (2018/07/05 追記)
転送先の URL
http://securitymanagement-support-●●●●.com/rmid_vcs
http://securityprotection-support-●●●●.com/rmid_vcs (2018/07/05 追記)


フィッシング対策協議会 Council of Anti-Phishing Japan

Apple および Amazon をかたるフィッシング (2018/06/04)

概要
Apple をかたり Amazon のフィッシングサイトへ誘導するフィッシングメールが出回っています。
メールの件名
アラート:あなたのアカウントは閉鎖されます。
詳細内容
Apple をかたり Amazon のフィッシングサイトへ誘導するフィッシングメールの報告を受けています
1. 2018/06/04 13:00 現在、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。
2. このようなフィッシングサイトにてログイン情報 (E メールまたは携帯電話番号、パスワード)、個人情報 (氏名、住所、電話番号等)、クレジットカード情報等を絶対に入力しないように注意してください。
3. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。
サイトのURL
http://pdate-security-supprt-●●●●.com/
http://update-security-support-appleid-●●●●.com/

●日経新聞社、元社員を告訴…社員3000人分と読者のべ38万人分の情報持ち出し

https://www.nikkei.com/article/DGKKZO32582700T00C18A7CR8000/

このニュースをザックリ言うと・・・

- 7月3日（日本時間）、日経新聞社より、同社元社員が社内からデータを持ち出したとして不正競争防止法違反容疑で告訴したと発表されました。

- 発表によれば、元社員は2012年10月に別社員の業務用PCを分解してハードディスクから全社員約3000人分の賃金等のデータを抜き取り、2017年12月にそのデータを月刊紙を発行する団体に郵送したとされています。

- この他に日経電子版読者約34万人分および同社週刊紙「日経ヴェリタス」読者約36000人分の個人情報等も持ち出していたことが明らかになっていますが、こちらの第三者への流出は確認されていないとしています。

AUS便りからの所感等

- 内部犯行による個人情報・機密情報の持ち出し事件といえば、2004年のYahoo! BB登録者情報約450万件が流出した事件、あるいは最大3504万件が持ち出された2014年のベネッセの事件等が思い出されます。

- 内部の悪意を持った人間により、機密情報にアクセスされることを食い止めることはもちろん、入手された情報がオンラインあるいはオフライン（USBメモリ等）で外部に持ち出されないようにすることにも十分に注意を払い、いわゆる「出口対策」についてのソリューションの導入が重要となるでしょう。

- 今回はPCを分解してハードディスクからデータを取り出すという手口がとられており、こういった手口に対する機密情報の保護をさらに徹底するのであれば、データを「暗号化」して保存する、さらにはハードディスクのデータ領域ないし全体を暗号化することも検討に値すると言えます。


日本經濟新聞

元日経社員を告訴 社内情報漏洩の疑い

2018/7/4付

営業秘密にあたる社員約３千人分の賃金データなどを外部に漏洩させたとして、日本経済新聞社は３日までに、東京本社デジタル事業担当付の元社員（53）を不正競争防止法違反容疑で警視庁に告訴した。元社員が社内規定に反して日経の顧客情報を社外に持ち出していたことも判明した。日経は既に元社員を懲戒解雇している。

日経は元社員の不正行為について今年１月以降、弁護士、デジタルデータを解析・復元するデジタルフォレンジック専門会社と協力し、社内調査を進めてきた。元社員は大量のデータを持ち出していたが、顧客情報を第三者に漏洩させた形跡はなかった。

告訴状によると、元社員はデジタル販売局所属だった2012年10月、日経本社内で総務局員の業務用パソコンを分解してハードディスクを抜き取り、営業秘密にあたる社員約３千人分の生年月日、基準内賃金などを記録したデータを私用パソコンに転送。17年12月、同データなどを保存したＵＳＢメモリーを月刊紙を発行する団体に郵送した。同団体は18年１月、運営するブログに一部を掲載した。

社内調査では、元社員は17年１月から18年３月までの間、業務上アクセス可能だった日経サービス会員情報（日経ＩＤ情報）や約３万６千人分の日経ヴェリタス読者情報のデータファイルをコピー。業務用パソコンから私用のメールアドレスに送信したり、クラウド上に複製、保存したりしていたケースも確認した。

●拡張子「.SettingContent-ms」のファイル悪用によるマルウェア拡散…Malwarebytes発表

https://news.mynavi.jp/article/20180704-658672/

このニュースをザックリ言うと・・・

- 7月2日（現地時間）、アンチウイルスソフトベンダーの米Malwarebytes社より、Officeのドキュメントにおいて、マクロを悪用せずにマルウェアの感染を行う新たな攻撃手法が確認されたと同社ブログで発表されました。

- 発表によれば、「.SettingContent-ms」拡張子（註：参考記事で「.SettingContent.ms」とあるのは誤りです）のファイルに不正なコマンドを記述することにより、ファイルを開いた場合にコマンドが確認なしで実行される仕様を悪用するものとなっています。

- Microsoftではこの機能が悪用されないよう修正する予定は特にないとのことですが、Malwarebytes社の製品では不正なファイルによる挙動を遮断するよう対応しているとのことです。

AUS便りからの所感等

- 「.SettingContent-ms」拡張子のファイルは、「設定コンテンツ」と呼ばれる、Windowsのコントロールパネル内の特定の設定画面を呼び出すショートカットを作成するためのものです。

- Windowsでファイルの拡張子が表示される設定にした場合でも、「.SettingContent-ms」拡張子のファイルはその拡張子の部分が表示されないことがあるため、ドキュメント等のファイルに偽装した不正なファイルを作成してメールに添付する攻撃が行われる可能性が考えられる点には注意が必要です。

- 機能自体の修正はしないと言っているMicrosoftについても、同社のWindows Defenderでは不正なファイルが検出するようになっているとの情報もありますので、拡張子からの判断が困難なこともあり、アンチウイルスやUTM等による防御は必須と言えるでしょう。


マイナビニュース

2018/07/04 09:26:39

マクロを使わないでマルウェア感染を広める新しいテクニックが発見

後藤大地

関連キーワード：マルウェア、サイバー攻撃

Malwarebytesは7月2日(米国時間)、「New macro-less technique to distribute malware - Malwarebytes Labs | Malwarebytes Labs」において、米セキュリティベンダーのSpecterOpsのセキュリティリサーチャーであるMatt Nelson氏が、Microsoft Officeのドキュメントにおいて、マクロを悪用せずにマルウェアの感染を行える方法を発見したと伝えた。

Windows 10特有のファイルに拡張子が「.SettingContent.ms」というものがある。これはフォーマットとしてはXML形式のファイルで、コントロールパネルに対してショートカットを作成する目的で使われている。問題はこのファイルのDeepLink要素に任意のコードを書くことが可能という点にあり、ここに指定したコードがユーザーに許可なしで実行されてしまうという。Nelson氏によると、当面のところ、Microsoftはこの不具合を修正するつもりはないとのことだ。