— AUS（アルテミス・ユーザ・サポート）便り 2017/09/25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。

●Amazonから身に覚えのない「注文通知」→注文をキャンセルさせて偽サイトに誘い込む偽メールが出回る

http://internet.watch.impress.co.jp/docs/news/1082187.html
https://www.antiphishing.jp/news/alert/amazon_20170922.html

このニュースをザックリ言うと・・・

- 9月22日（日本時間）、フィッシング対策協議会より、Amazonをかたる新たなフィッシングメールが確認されたとして警告が出されています。

- メールは、件名「注文通知：Launchpad Pro 2017年9月21日」、本文は架空の注文に関する請求書となっており、更にはキャンセル用ページとして、アカウント情報・個人情報およびクレジットカード番号を入力させる下記のURLのフィッシングサイトへ誘導するものとなっています。

  - http://●●●●.co/amzauthlog
  - https://www.annazon.com.service.customer.jp-●●●●.care/en/ap/英数字/signin.php?パラメータ

- 同協議会では、同日11時30分現在フィッシングサイトがまだ生きているとしており、絶対にこのようなサイトで情報を入力しないよう呼び掛けています。

AUS便りからの所感等

- Amazonでは、以前から同様のフィッシングに対する注意喚起を行っており（https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=201304810）、フィッシングメールでよく見られる内容の傾向として、今回のような「注文していない商品の注文確認を促すもの」「アカウントに登録した個人情報や支払い情報の更新を求めるもの」等を挙げています。

- Webブラウザやアンチウイルスソフト・UTMが提供する、フィッシングサイトへのアクセスを警告あるいは遮断する機能を可能な限り有効にすること、他にも通常使用するサービスのログインページはブックマークに登録してそこからアクセスするよう心がけること、などによりフィッシングに騙される可能性を低減できるでしょう。

- この他、PCに感染したマルウェアが「本物のログインページの表示時に偽のログインフォーム等を表示する」恐れもある点にも注意が必要です。

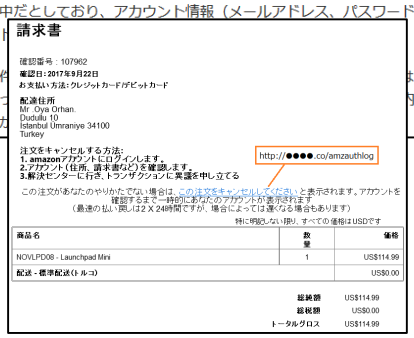
INTERNET Watch

Amazonから身に覚えのない「注文通知」→注文をキャンセルさせて偽サイトに誘い込む偽メールが出回る

磯谷 智仁　2017年9月22日 13:38

ツイート　リスト　いいね！ 1,021　シェア　B! 46　Pocket 144

Amazonをかたるフィッシングメールが出回っているとして、フィッシング対策協議会が22日、緊急情報を出した。誘導先のフィッシングサイトは同日11時30分現在も稼動中だとしており、アカウント情報（メールアドレス、パスワードなど）やクレジッ


請求書

確認番号：107962
確認日：2017年9月22日
お支払い方法：クレジットカードデビットカード

配達住所
Mr. Oya Orhan.
Dudullu 10
Istanbul Umraniye 34100
Turkey

注文をキャンセルする方法：
1. amazonアカウントにログインします。
2. アカウント（住所、請求書など）を確認します。
3. 解決センターに行き、トランザクションに異議を申し立てる

http://●●●●.co/amzauthlog

この注文があなたのやりかたでない場合は、注文をキャンセルしてください と表示されます。アカウントを確認するまで一時的にあなたのアカウントが表示されます
（最速の払い戻しは2 X 24時間ですが、場合によっては遅くなる場合もあります）

特に明記しない限り、すべての価格はUSDです

商品名	数量	価格
NOVLPD08 - Launchpad Mini	1	US$114.99
配送 - 標準配送（トルコ）		US$0.00

総納額 US$114.99
総税額 US$0.00
トータルグロス US$114.99

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 (2017/09/22)

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

注文通知：Launchpad Pro 2017年9月21日

詳細内容

Amazon をかたるフィッシングサイトに関して、以下の報告を受けています。

1. 2017/09/22 11:30 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アカウント情報 (Email または phone for mobile accounts, Password)、請求先情報 (Full name, Address line, City, State/Province/Region, Zip Code, Country, Date of Birth, Phone number)、クレジットカード情報 (Name on card, Card number, Card Security Code, Expiration date, SecureCode 3D/VBV) 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。

●ビックカメラ・楽天でポイント不正利用

https://www.jiji.com/jc/article?k=2017091900546&g=soc

このニュースをザックリ言うと・・・

- 9月19日（日本時間）、警視庁サイバー犯罪対策課より、不正アクセス禁止法違反と詐欺の疑いで中国人留学生ら3人を逮捕したと発表されました。

- 2016年10月に「ビックカメラ」で、スマホアプリに他のユーザのID・パスワードを入力して表示されたバーコードで約7万円の商品を不正に購入した疑いが持たれています。

- 同時期に同社サイトでは不正ログイン4000件が発生、計約133万円分のポイントが不正利用されており、容疑者グループの犯行とみられています。

- この他、「楽天」のポイントも約4万円分が不正利用された疑いがあるとのことです。

AUS便りからの所感等

- ビックカメラのサイトへの不正ログインにあたっては、他のWebサイトから流出したアカウント情報をもとにした、いわゆる「リスト型攻撃」が発生していたとされています。

- かつて、アカウントのパスワードは定期的に変更することがルールとされていましたが、これが複数のサイトで同じパスワードを使い回す傾向を強め、リスト型攻撃で連鎖的にログインされてしまう原因を作ったとの指摘もあります。

- 今日では、完全にランダムな文字列でないにしても、同じパスワードを使い回さず、可能であればパスワード管理ツール等で管理することも推奨されており、セキュリティに関する常識は年々変化していく場合もあると心得ましょう。

JIJI.COM

他人のポイントで商品購入＝不正アクセス容疑、中国人逮捕－警視庁

不正アクセスで他人のポイントを利用し、家電量販店「ビックカメラ」で商品を購入したとして、警視庁サイバー犯罪対策課は１９日までに、不正アクセス禁止法違反と詐欺の疑いで中国人留学生の于冰冰容疑者（２４）＝川崎市川崎区下並木＝ら２人を逮捕した。于容疑者は「友人に買ってくるよう頼まれただけだ」と否認しているという。

同課は同じグループの中国人で無職魏星容疑者（２３）＝埼玉県川口市芝園町＝も詐欺容疑で逮捕。このグループが少なくとも約２００万円分のポイントを不正に使ったとみて裏付けを進めている。

于容疑者の逮捕容疑は２０１６年１０月、同社のスマートフォンアプリに他人のＩＤとパスワードを入力し、ポイントを使えるバーコードを表示。東京都内の店舗で示し、デジタルカメラ１台（約７万円）を購入した疑い。

同課によると、ビックカメラには同月１～４日、流出したＩＤとパスワードの組み合わせによる不正アクセスをさまざまなサイトで試みる「リスト型攻撃」が４７万回あった。このうち不正にログインされた痕跡が約４０００件あり、同年１０～１１月に計約１３３万円分のポイントが使われたという。

魏容疑者は他人の楽天ポイントを使ってドラッグストアで医薬品７２点（約４万円相当）を購入した疑いが持たれている。（2017/09/19-12:31） 関連ニュース

●定番のシステムクリーナーソフト「CCleaner」にマルウェア混入

http://www.itmedia.co.jp/enterprise/articles/1709/19/news051.html

このニュースをザックリ言うと・・・

- 9月18日（現地時間）、Cisco社のセキュリティ部門Talosより、Windows用の定番システムクリーナーソフト「CCleaner」が8月15日から9月12日までの間、マルウェアが混入した状態で配布されていたとブログで発表されました。

- マルウェアが混入していたのは「CCleaner 5.33.6162」および「CCleaner Cloud 1.07.3191」で、それぞれバイナリが改ざんされ、外部サーバから指令を受け取るバックドアが仕込まれた状態だったとのことです。

- 同日、CCleanerを提供するPiriform社からも混入を認める発表があり、CCleaner 5.34以降（現在最新は5.35）にアップデートするよう呼び掛けています（CCleaner Cloudは自動的に更新されるとのことです）。

AUS便りからの所感等

- マルウェアは「コンピューター名」「インストールされているソフト一覧」「実行中のプロセス一覧」「IPアドレスとMACアドレス」等のデータを収集して外部に送信するものとされ、またTalosによる続報では、複数の大企業をターゲットとした標的型攻撃を狙っていた可能性が指摘されています。

- マルウェアが混入したインストーラーが正規の署名がされ、正規のダウンロードサーバから配布されていたことから、Talosでは「サプライチェーン攻撃」、即ちソフトウェアの開発過程での攻撃（開発者アカウントの乗っ取り、悪意のある開発者の仕込み等）によりマルウェアが混入した恐れがあるとしており、各種ウイルススキャンにおいても、事件が公表される以前はマルウェアが検出されにくい状況だった模様です。

- 同様のケースが今後どれだけ発生するかは分かりませんが、可能な限りマルウェアの混入やPCからの情報の流出を防ぐため、最低限アンチウイルスの導入、パターンファイルを常に最新に保つ、そしてUTMによる不正な外部への通信を遮断する設定とすることを推奨致します。

ITmedia エンタープライズ

2017年09月19日 08時15分 公開

Avast傘下の「CCleaner」にマルウェア混入、正規ルートで配信

システムクリーナーソフト「CCleaner」の正規版が改ざんされてマルウェアを仕込まれ、正規のダウンロードサーバを通じて配布されていたことが分かった。

[鈴木聖子，ITmedia]

ウイルス対策ソフトウェアメーカーAvast Software傘下のシステムクリーナーソフト「CCleaner」が何者かに改ざんされた。マルウェアを仕込まれ、正規のダウンロードサーバを通じて配布されていたことが分かった。Ciscoのセキュリティ部門Talosが2017年9月18日のブログで明らかにした。