— AUS（アルテミス・ユーザ・サポート）便り 2016/10/24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。

●ネットバンキングで他人の口座から180万円不正送金･･･パスワード乱数表を闇サイトで購入

http://www.nikkei.com/article/DGXLZO08536030Z11C16A0CC0000/
http://www.antiphishing.jp/report/pdf/internetbanking_guideline.pdf

このニュースをザックリ言うと･･･

- 10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電子計算機使用詐欺の疑いで、岐阜市の自営業者の男を追送検したことが発表されました。
- 発表によれば、男は昨年6月にネットバンキングサイトに不正アクセスし、大阪府の男性の口座から約180万を自分が管理する他人名義の口座に送金した疑いがもたれています。
- また、送金の際には「乱数表」に書かれたパスワードが必要でしたが、男はそれを闇サイトで入手していたとのことです。
- なお、男はこうしたID・パスワード情報を第三者にも販売した等の容疑で、今年7月に逮捕されていました。

AUS便りからの所感等

- ネットバンキングサイトをかたるフィッシングサイトの特徴として、ログインのためのID・パスワードだけでなく、送金のために必要な「乱数表」に書かれた番号を全て入力するよう求めることが挙げられますが、通常はこれらの番号の一部しか求めません。
- こういったフィッシングサイトに誘導されて入力してしまったものが闇サイトで流通し、誰かに悪用されることになります。
- 銀行をはじめとする各金融機関はフィッシングサイトに騙されないよう頻繁に警告を行っていますし、自分が利用しているサイトの正式な情報にあたり、サイトがどういった挙動をとるのかについて把握しておき、不審な様子に遭遇した場合や万が一そこで情報を入力してしまった場合は速やかに金融機関や警察に連絡することを推奨致します。
- メール等からフィッシングサイトへ誘導するだけでなく、マルウェアの感染により不正な入力フォームが表示される可能性もありますので、それを抑止するためにアンチウイルス・UTMによる十分な防御を事前に行うことも重要です。

日本経済新聞

速報＞社会＞記事

闇サイト購入の口座で不正送金　容疑の男を追送検

2016/10/19 13:53

保存　印刷　その他

他人名義のインターネットバンキングの口座から現金180万円を不正に送金したとして、警視庁サイバー犯罪対策課は19日、岐阜市長良、自営業、中村明博被告(29)＝窃盗罪などで起訴＝を電子計算機使用詐欺などの疑いで追送検した。

同課によると、中村被告は検索サイト経由ではたどり着けない「ダークウェブ」にあるサイトで他人名義の口座を大量に購入。口座は不正送金に悪用するほか、ネット上で販売して代金を仮想通貨「ビットコイン」で受け取っていた。

送検容疑は昨年6月、大阪府の40代男性のネットバンキング口座に不正に接続し、180万円を中村被告が管理する口座に送金した疑い。

保存　印刷　その他

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

インターネットバンキング不正送金被害、もしもの時の相談先

フィッシング詐欺やオンライン銀行不正送金、ウイルス感染、不正アクセスなどのサイバー犯罪の不安がある場合、巻き込まれた場合には、速やかに下記の窓口に相談しましょう。

1）金融機関への連絡
ご利用のサービスの相談窓口へ連絡し、銀行からの案内を踏まえて必要な手続きを取りましょう。また、相談窓口では、犯罪手口の解明のために、手掛かりとなる情報を聞かれることがありますので、できるかぎり協力するようにしましょう。
連絡先：各金融機関の相談窓口
※ご利用のインターネットバンキングの問い合わせ先・連絡先を、あらかじめ確認しておきましょう。

2）警察への相談、通報など
インターネットバンキング不正利用にあったり、あいそうになったときは、事実関係を整理し、警察のサイバー犯罪相談窓口に相談、通報しましょう。
連絡先：都道府県警察本部 サイバー犯罪相談窓口
http://www.npa.go.jp/cyber/soudan.htm

3）コンピューターウイルス感染に関する相談

●富山大学の研究施設にてサイバー攻撃、PCがマルウェア感染

http://www.asahi.com/articles/ASJBB4QN2JBBPUZB002.html

このニュースをザックリ言うと・・・

- 10月10日（日本時間）、富山大学より、同大学水素同位体科学研究センターが外部から攻撃を受け、個人情報等のデータが外部に流出した可能性があると発表されました。

- 発表によれば、昨年11月24日に同大学の職員あてに標的型攻撃メールが送信され、添付ファイルを開いたことによりPCがマルウェアに感染、以後マルウェアによる外部への通信等の不審な行動が行われていたとされており、今年6月14日に外部からの連絡により発覚し、以後10月までの間調査・分析を行っていたとのことです。

- 当該PCには学内外の1492名分の個人情報や研究に関する情報が含まれており、またPC上で不審な圧縮ファイルが作成されていた痕跡があったことから、これらの情報の一部ないし全部が外部に流出した可能性があるとされています。

AUS便りからの所感等

- 大学を標的とした攻撃は、関西学院大学等複数の大学がフィッシング攻撃を受け、個人情報が流出する事件が直近にも発生していますが（「AUS便り 2016/10/17号」参照）、その例とは手口が異なり、攻撃が発生した時期も異なるため、同一の攻撃者によるものであるかは不明です。

- 大学では、今回の事件を受けて今後の課題をまとめるとともに、システム面・ユーザリテラシー面の両方から各種対策を行う模様です。

朝日新聞 DIGITAL

富山大にサイバー攻撃　放射性物質研究などの情報流出か

江向彩也夏　2016年10月10日21時33分

シェア 35　ツイート list　ブックマーク 15　スクラップ　メール　印刷

放射性物質 トリチウム（三重水素）などを研究する富山大（富山市）の水素同位体科学研究センターが サイバー攻撃 を受け、研究成果や共同研究者ら1492人分の個人情報が流出した可能性のあることが分かった。富山大が10日発表した。情報の悪用は確認されていないとした。

富山大によると、サイバー攻撃 を受けたのは、トリチウム 理工学が専門の同センター 非常勤職員 が管理していたパソコン1台。昨年11月に職員とセンター教授の2人にメールが届き、メールを開いた職員のパソコンがウイルスに感染した。教授はメールを開かず、ウイルスに感染しなかった。

感染したパソコンは遠隔操作され、昨年11月～今年6月に4カ所の外部サーバーと通信していた。

- ユーザのリテラシーの強化は行うに越したことはないですが、どれだけ強化してもうっかりは発生するものと心得たうえで、アンチウイルス・UTMの採用やネットワーク構成の見直しを中心としたシステム面での防御こそが肝心です。

●BINDにおいて新たな？脆弱点・・・2013年に修正済み

https://jprs.jp/tech/security/2016-10-21-bind9-vuln-malformed-options.html

このニュースをザックリ言うと・・・

- 10月21日（日本時間）、DNSサーバソフト「BIND」の開発元である米ISCより、古いバージョンに修正済みの脆弱性（CVE-2016-2848）が存在していたことが発表されました。

- 脆弱性は細工されたDNSパケットを受信することにより、DNSサーバプロセス（named）を落とされる可能性があるもので、2013年にBIND 9.9.3にて修正済みとされています。

- ISCやJPRS、JPCERT/CCおよびJPNIC等からは、使用しているBINDにおいて脆弱性が存在しないか確認し、最新バージョン（BIND 9.11.0/9.10.4-P3/9.9.9-P3）にアップデートすること等が警告されています。

AUS便りからの所感等

- 現時点でISCからリリースされているBINDの最新バージョンは、9月27日に別の脆弱性が確認された際に出た修正バージョンであり（「AUS便り 2016/10/03号」「AUS便り 2016/10/11号」参照）、今回は新しいバージョンは出ていませんので、この時に最新バージョンを入手し、コンパイルしてインストールしたのであれば問題はありません。

- ただし、Linuxディストリビューションにおいて提供されるコンパイル済みのパッケージでは、通常、ある古いバージョンを元に、より新しいバージョンからセキュリティに関する修正のみを抜き出して適用するという形をとっていますので、今回初めてセキュリティに関する修正と認識され、改めてセキュリティアップデートがリリースされているケースがあります。

JPRS

■（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2848）
- フルリゾルバ（キャッシュDNSサーバ）／権威DNSサーバの双方が対象。対象となるディストリビューション・バージョンに要注意 -

株式会社日本レジストリサービス（JPRS）
初版作成 2016/10/21（Fri）

▼概要

BIND 9.xにおける実装上の不具合により、namedに対する外部からのサービス不能（DoS）攻撃が可能となる脆弱性が、開発元のISCから発表されました。本脆弱性により、提供者が意図しないサービスの停止が発生する可能性があります。

本脆弱性は、2013年5月にバグ修正済の項目が外部から攻撃可能であったと判明したことによるものであり、ISCからリリースされている最新版のBIND 9は対象となりません。ただし、各ディストリビューションベンダーからパッケージとしてリリースされているBIND 9が本脆弱性の対象となるバージョンをベースとしていた場合、対応が必要になる可能性があります（※1）。

（※1）バージョン情報については、本注意喚起の「対象となるバージョン」をご参照ください。

- この他、ルータやUTM等のアプライアンスにBINDが含まれているケース等、周辺の環境でBINDが存在するのか、どのような形で導入されているかを事前に把握しておき、それぞれにおいて適切な対応をとることが重要となってきます。