— AUS（アルテミス・ユーザ・サポート）便り 2017/03/13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。

●クレカ情報約72万件流出か…都納税サイト等に不正アクセス

http://www.itmedia.co.jp/enterprise/articles/1703/10/news157.html
http://www.jhf.go.jp/topics/topics_20170310_im.html

このニュースをザックリ言うと･･･

- 3月10日（日本時間）、GMOペイメントゲートウェイ（以下GMO-PG）社より、同社が運営委託を受け、クレジットカード決済サービスを提供していた2つのWebサイトが不正アクセスを受け、クレジットカード情報延べ719,830件が流出した可能性があると発表されました。

- 被害を受けたのは、東京都の都税クレジットカード支払いサイト（流出の可能性のあるカード情報676,290件）と、住宅金融支援機構の団体信用生命保険特約料クレジットカード支払いサイト（同43,540件）で、カード番号・有効期限・メールアドレスの他、後者からはカードのセキュリティコード・住所・氏名・電話番号等も流出した模様です。

- GMO-PG社によれば、各サイトのWebアプリケーションで用いられている「Apache Struts2」の脆弱性が発表されたことを受けて9日夜に対策と調査を行ったところ、脆弱性を悪用して悪意のあるプログラムが仕込まれていたことが判明したとのことです。

AUS便りからの所感等

- Struts2は、JavaによるWebアプリケーション構築のためのフレームワークとしてよく使われる一方、重大なセキュリティホールが比較的頻繁に見つかることでも知られており、今回の脆弱性はWebサーバを乗っ取ることが可能となるレベルとされ、IPA（https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html）等からも注意喚起が出されていました。

- 自前で決済システムを構築し、自社サーバ上に保存していたカード情報が不正アクセスで流出してしまい、決済部分を外部サービスに委託したというケースも珍しくない中、今回委託を受ける側のシステムで流出が発生したこと、さらには「PCI DSS」で基本的に保存が禁止されているカードのセキュリティコードが保存され、それが流出したことは「痛恨」と言えます。

- GMO-PG社では、今回の脆弱性への対策の一環として、WAFによる脆弱性への攻撃の遮断等を行っており、Webアプリケーションに対する攻撃を検知・遮断するためには、アプリケーションやフレームワークのセキュリティホールを塞ぐのももちろんですが、サーバの前面にWAF機能を搭載したUTMを設置する等、多層防御を前提とすべきでしょう。

ITmedia エンタープライズ

2017年03月10日 22時24分 更新

GMOペイメントゲートウェイに不正アクセス　クレジットカード情報など約72万件が流出した可能性

GMOペイメントゲートウェイが提供する決済サービスに不正アクセスがあり、東京都の都税クレジットカードお支払いサイトと、住宅金融支援機構の団体信用生命保険特約料クレジットカード支払いサイトから、クレジットカードなどの情報約72万件が流出した可能性がある。

GMOペイメントゲート
カードの番号や有効期限
た。

不正アクセスがあった
援機構の団体信用生命保
脆弱性を悪用した不正ア
明した。調査の結果、ク
スなどの情報が流出した

不正アクセスされた可能性がある情報と件数は以下の通り。

東京都 都税クレジットカードお支払サイト（総件数 67万6290件）

情報の内容	件数
クレジットカード番号、クレジットカード有効期限	6万1661件
クレジットカード番号、クレジットカード有効期限、メールアドレス	61万4629件

住宅金融支援機構　団信特約料クレジットカード払い（4万3540件）

情報の内容	件数
クレジットカード番号、クレジットカード有効期限、セキュリティコード、カード払い申込日、住所、氏名、電話番号、生年月日	622件
クレジットカード番号、クレジットカード有効期限、セキュリティコード、カード払い申込日、住所、氏名、電話番号、生年月日、メールアドレス、加入月	2万7661件
クレジットカード番号、クレジットカード有効期限、セキュリティコード、カード払い申込日、住所、氏名、電話番号、生年月日、メールアドレス	5569件
クレジットカード番号、クレジットカード有効期限、セキュリティコード、カード払い申込日、住所、氏名、電話番号、生年月日、加入月	9688件

住宅金融支援機構 Japan Housing Finance Agency

事務委託先であるGMOペイメントゲートウェイ株式会社のシステムへの不正アクセス及び個人情報流出について

2017年3月10日現在

今般、当機構の団体信用生命保険特約制度のクレジットカード払いに係る事務を委託しているGMOペイメントゲートウェイ株式会社より、同社の機構団体信用生命保険特約料クレジットカード支払いサイトに対して不正なアクセスがあり、当機構のお客さまの個人情報が流出した可能性があるとの報告を受けました。お客さまにご心配とご迷惑をおかけしますことを深くお詫び申し上げます。

同社において、不正アクセスによる個人情報の流出の可能性があることを確認しておりますが、現在のところ、お客さまの個人情報を悪用された等の報告はございません。

当機構としては、機構団体信用生命保険特約制度の「クレジットカード払い」のお申し込み受付を一時休止しております。再開については、本事案の状況を確認し、改めてお知らせさせていただきます。
また、今回の事態を重く受け止め、同社に詳細な事実関係の調査及び報告を求めるとともに、委託先に情報セキュリティ体制の強化を要請してまいります。

流出の概要につきましては、GMOペイメントゲートウェイ株式会社のホームページに公表されております。
▸ 同社公表資料はこちらをご覧ください。

※GMOペイメントゲートウェイ株式会社（法人番号 6011001005411）
機構団体信用生命保険特約制度の特約料のお支払い方法で、「クレジットカード払い」を選択されているお客さまのクレジットカード払い関係データの処理及び管理等に係る事務を委託している事業者です。
機構団体信用生命保険特約制度とは、機構が民間金融機関と提携して提供する住宅ローン「フラット35」などをお借り入れされている方に万一のことがあった場合に、残りの債務が保険により全額弁済する保障制度です。

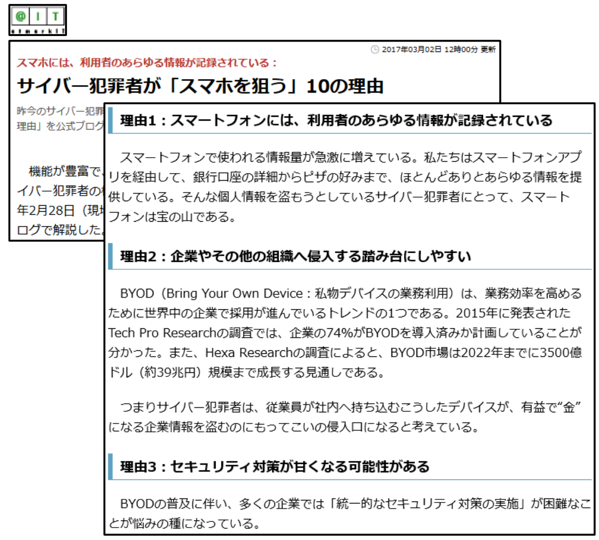
●サイバー犯罪者が「スマホを狙う」10の理由…ESETが解説

http://www.atmarkit.co.jp/ait/articles/1703/02/news104.html

このニュースをザックリ言うと・・・

- 2月28日（現地時間）、セキュリティベンダーのESET社より、「サイバー犯罪者がスマートフォンをターゲットにする10の理由」と題した記事が同社ブログで発表されました。

- その理由として、①利用者のあらゆる情報が記録されている、②企業やその他の組織へ侵入する踏み台にしやすい、③セキュリティ対策が甘くなる可能性がある、④自動入力機能が普及している、⑤財布に直結している、⑥利用者の現在位置や勤務先を知っている、⑦Bluetoothによる近接通信機能がある、⑧モバイル詐欺の手口が知られるようになった、⑨スパム送信にもうってつけである、そして最後に、⑩利用者がその危険を知らない、が挙げられています。



2017年03月02日 12時00分 更新

スマホには、利用者のあらゆる情報が記録されている：

サイバー犯罪者が「スマホを狙う」10の理由

理由1：スマートフォンには、利用者のあらゆる情報が記録されている

スマートフォンで使われる情報量が急激に増えている。私たちはスマートフォンアプリを経由して、銀行口座の詳細からピザの好みまで、ほとんどありとあらゆる情報を提供している。そんな個人情報を盗もうとしているサイバー犯罪者にとって、スマートフォンは宝の山である。

理由2：企業やその他の組織へ侵入する踏み台にしやすい

BYOD（Bring Your Own Device：私物デバイスの業務利用）は、業務効率を高めるために世界中の企業で採用が進んでいるトレンドの1つである。2015年に発表されたTech Pro Researchの調査では、企業の74%がBYODを導入済みか計画していることが分かった。また、Hexa Researchの調査によると、BYOD市場は2022年までに3500億ドル（約39兆円）規模まで成長する見通しである。

つまりサイバー犯罪者は、従業員が社内へ持ち込むこうしたデバイスが、有益で“金”になる企業情報を盗むのにもってこいの侵入口になると考えている。

理由3：セキュリティ対策が甘くなる可能性がある

BYODの普及に伴い、多くの企業では「統一的なセキュリティ対策の実施」が困難なことが悩みの種になっている。

AUS便りからの所感等

- PC（デスクトップおよびノート）においてどういったセキュリティ対策を行うべきかは概ねユーザの間で知られているところですが、そのPCと同等の処理能力を持つ一方、PCとは異なるOS、異なる使い勝手（だからこそ自動入力機能が良く使われる）、ほぼすべての通信が無線であること、PCに通常はない機能（電子マネー等）を多く備えている点、そして小さいゆえにより持ち運びしやすいこと等、スマートフォンやタブレットにおいて必要なセキュリティ対策はPCとまた異なってきます。

- 月並みな結論ですが、PCと共通したセキュリティ対策、スマートフォン等に特有のセキュリティ対策、両方について情報収集し、それを確実に適用することが重要です。

●リモートデスクトップへの不正ログインによるランサムウェア拡散攻撃

http://blog.trendmicro.co.jp/archives/14451

このニュースをザックリ言うと・・・

- 2月10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、リモートデスクトップ（RDP）からPCに不正にログインし、ランサムウェア「CRYSIS(クライシス)」に感染させようとする攻撃についての注意喚起が出されました。

- 攻撃者は、一般的に使用頻度の高いユーザ名とパスワードによるブルートフォース（アカウント総当り）攻撃を行ってRDPへのログインを試み、成功すると共有フォルダやクリップボード経由でCRYSISを送り込むとされています。

- 同社では2016年9月の時点でこの攻撃の存在について報告していますが、以後も攻撃は続いており、今年1月時点で攻撃数が倍増していることから、再度警告を出しています。

AUS便りからの所感等

トレンドマイクロ セキュリティブログ

RDP経由のブルートフォース攻撃を確認、暗号化型ランサムウェア「CRYSIS」を拡散

投稿日: 2017年2月10日
脅威カテゴリ: 不正プログラム, クライムウェア, サイバー犯罪, TrendLabs Report
執筆: Threats Analyst - Jay Yaneza

トレンドマイクロは、2016年9月、更新したランサムウェア「CRYSIS(クライシス)」(「RANSOM_CRYSIS」として検出)がオーストラリアとニュージーランドの企業を標的に、「リモート・デスクトップ・プロトコル(RDP)」を経由したブルートフォース(総当り)攻撃を仕掛けていたことについて報告しました。そして現在、RDP経由のブルートフォース攻撃は続行中であり、世界中の大企業や中小企業に影響を及ぼしています。事実、2017年1月には、2016年末に比べ攻撃数が倍増しています。さまざまな業界が影響を受けていますが、終始一貫して標的とされているのは、米国の医療業界です。

- RDPはWindowsに備わっている、PCのデスクトップへ外部からアクセスしたり、ファイルを転送したりするための機能（同様の機能を持つソフトウェアとしてTeamViewerやVNC等があります）で、主にサーバを外部から管理する等の目的で用いられます。

- RDPが用いるTCP/UDPポート3389番もそうですが、第三者からアクセスされるべきでないサービスポートを不用意に外部ネットワーク等に対して開けておくことは危険ですので、UTMの設置などにより、ポートを完全に塞ぐか、特定のアクセス元からのアクセスのみ許可するようにすべきです。

- そもそも自分や管理者がPCへ外部からRDPでアクセスすることがないのであれば、RDPを設定で無効化することが安全であり、RDPを利用している場合でも、共有ドライブやクリップボードへの転送だけを無効化することや他の経路からブルートフォース攻撃によって侵入されないようにパスワードを十分に複雑なものに設定することも重要です。