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。

●フィッシング報告件数は2540件、前月度の10倍･･･フィッシング対策協議会

http://www.antiphishing.jp/report/monthly/201512.html
http://securityblog.jp/news/20160115.html

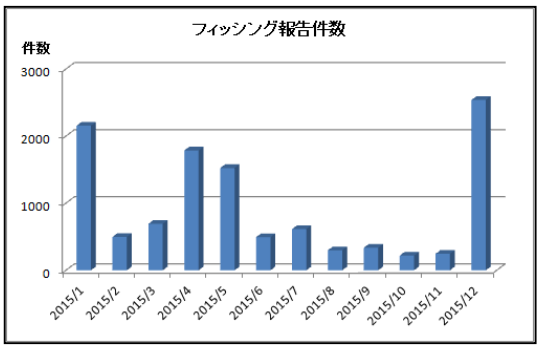
このニュースをザックリ言うと･･･

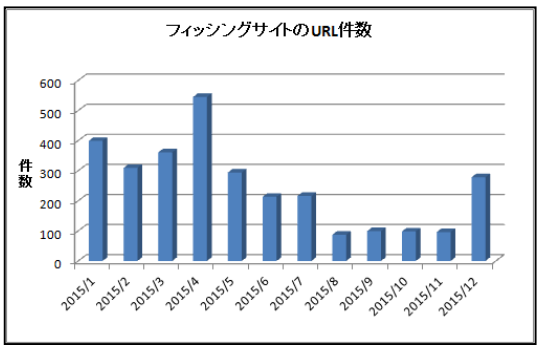
- 1月15日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、2015年12月の月次報告書が公開されました。
- 同協議会に寄せられた12月のフィッシング報告件数は2,540件で、同年11月の246件より2,294件増加で約10倍となっており、同年1月の2,156件を上回る結果となりました。
- また、フィッシングサイトのURL件数も11月より182件増・3倍弱の278件となっています。
- 同協議会では、フィッシング報告件数急増の原因として、銀行などの金融機関をかたるフィッシングの報告が増加したことを挙げており、全体の98%がこれにあたる他、オンラインゲームや通信事業者をかたるフィッシングの報告もあったとのことです。

AUS便りからの所感等

- 同協議会によるフィッシング報告件数は、ここ数年は1月に急増するケースが多く、12月の時点で既にこれだけの件数がみられていることから、1月にはさらなる増加傾向となる可能性も考えられるでしょう。
- 数字を見て注意を払うに越したことはありませんが、普段よりフィッシングメールの傾向について情報収集を行い、「URLを安易にクリックしない」「利用している正規のサイトはブラウザのブックマークからアクセスする」といった行動をとること、またアンチウイルスやブラウザ・UTMに搭載されたアンチフィッシング機能の活用といった十分な防御をとることを推奨します。

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





【フィッシング対策協議会　総評】
2015 年 12 月のフィッシング報告件数は 2,540 件となり 11 月と比較すると約 10 倍以上の増加となります。12 月のフィッシングの特徴としては金融機関をかたるフィッシングが複数の銀行で発生したことが上げられます。協議会の窓口にも多くの報告が寄せられたため、フィッシングメールが不特定多数に対して大量に送られたと思われます。また 12 月全体のフィッシング報告件数に対する金融機関をかたるフィッシングの割合は 98% となりましたが、オンラインゲームや通信事業者をかたるフィッシングの報告もありました。引き続き 2016 年 1 月以降もご注意ください。
フィッシングかどうかの判断に迷うメールや、不審なメールを受け取った場合は、各サービス事業者の問合せ窓口やフィッシング対策協議会（info@antiphishing.jp）までご連絡ください。

日立ソリューションズ 情報セキュリティブログ

セキュリティニュース

12月は前月の約10倍以上のフィッシング報告件数を確認

2016年1月15日

フィッシング対策協議会は、1月4日、2015年12月の月次報告書を公開した。

これによると、フィッシング報告件数は2,540件と前月の246件より2,294件増加した。また、フィッシングサイトのURL件数は278件で、前月より182件増加している。そして、フィッシングに悪用されたブランド件数は17件で、前月より2件増加した。

同協議会によると、12月は、前月と比較して約10倍以上のフィッシング報告件数があった。手口の内訳は、金融機関をかたるフィッシングが98%を占め、年末にかけて複数の銀行でフィッシングが発生したことが原因として挙げられる。

●アークン社に不正アクセス、顧客3,859社情報流出

http://internet.watch.impress.co.jp/docs/news/20160113_738731.html

このニュースをザックリ言うと・・・

- 1月13日（日本時間）、情報セキュリティ対策製品・サービス等を手掛けるアークン社より、同社顧客リストの一部が不正アクセスによって窃取されていたことが発表されました。

- 不正アクセスを受けたのは社外のデータセンターに設置している同社バックアップサーバで、今月4日に同社に対し金銭を要求する恐喝があったことにより発覚したとしており、同社が確認した限りで顧客3,859社の会社名、電話番号、住所、担当者名およびメールアドレスが窃取された模様です。

- 現在同社では、警察および外部の専門機関の協力を得て、事実関係の調査および再発防止に向けた対応を行っているとのことです。


INTERNET Watch

ニュース

アークン、不正アクセスで顧客情報を窃取され、恐喝を受ける

(2016/1/13 15:08)

G+1 9 B! 7 ツイート リスト いいね！ シェア 20 Pocket 11

情報セキュリティ対策製品・サービスなどを手掛ける株式会社アークンは13日、同社の顧客企業リストの一部を不正アクセスにより窃取したとして、同社に対して金銭を要求する恐喝未遂事件が発生していたことを公表した。

窃取された可能性が判明しているのは3859社。社名、担当者名、メールアドレス、電話番号、住所の5項目が含まれる。情報窃取とは別に、3社の顧客アカウントへの不正アクセスの痕跡も確認しているという。

1月4日、要求額を支払わなければ窃取した顧客情報を公開すると恐喝する匿名の封書を受理。調査の結果、社外データセンターに設置しているバックアップサーバーに不正アクセスされた痕跡を確認した。公表が遅れたのは、捜査に支障が生じる恐れがあるため公表を控えるよう警察から要請があったためだという。

アークンでは謝罪するとともに、対象となる顧客に500円のクオカードを送るとしている。

AUS便りからの所感等

- セキュリティ会社が不正アクセス・情報流出の被害を受けたということで、ネット上ではセンセーショナルな反応がされている事件と言えますが、全ての企業にとって、決して対岸の火事で済まされるものではありません。

- 今後同社が行った調査結果が開示される可能性がありますので、発生し得る不正アクセスのケースの研究および今後の対策のための指針とし、
「アンチウイルスやUTM等が適切に導入されているか」
「個人情報・顧客情報の取り扱いの面で問題がないか」
など油断することなく改めて確認・点検を行うべきでしょう。

●許可なしでダウンロード・インストール・ルート権限取得を勝手に行うアプリがGoogle Playで見つかる

http://gigazine.net/news/20160108-unauthorized-download-app-found/

このニュースをザックリ言うと・・・

- 1月6日（現地時間）、モバイルに特化したセキュリティソリューションを提供するLookout社より、ユーザの許可なくマルウェアをダウンロードするAndroidアプリをGoogle公式のアプリストア「Google Play」で発見したとして警告が発表されました。

- マルウェア「BrainTest」は、端末に潜り込むと、他にもマルウェアを含んだアプリをダウンロードしたり、勝手に高い評価をつけたりするといった特徴があるとのことです。

- また、端末のルート権限を取得し、システム領域に不正なファイルのコピーを行うため、原因となったアプリをアンインストールしても復活し、復旧にはリフレッシュが必要になるとされています。

- Lookout社ではBrainTestが含まれたアプリ13種類を確認しており、現在では全てGoogle Playから削除されているとのことです。


GIGAZINE

2016年01月08日 16時00分00秒

許可なしでダウンロード・インストール・ルート権限取得を勝手に行うアプリがGoogle Playで見つかる

by MattysFlicks

モバイル端末に特化したセキュリティ企業・Lookoutが、ユーザーが許可していないにも関わらず勝手にダウンロードされるマルウェアを含んでいるアプリ(ゲーム)をGoogle Playで発見したことを報告しています。

AUS便りからの所感等

- マルウェア入りアプリのリスクは、特に非公式のサイトから入手してインストールした場合に顕著ですが、Google Playのような公式のサイトであっても皆無ではなく、インストールは既存の評価を十分に確認してから行うべきでしょうが、今回の場合は高い評価の水増しを行っていたため、低い評価の方で被害者等からの警告がなされていないかについても確認しましょう。

- セキュリティベンダーが提供するスマートフォン向けアンチウイルスを導入し、可能であればUTMを経由してのアクセスにより、マルウェアがインストールされる可能性を少しでも抑制することが良いでしょう。