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。

●「ご登録パスワード変更完了のお知らせ」フィッシングメールのだまし手口の巧妙化に警戒を

http://www.itmedia.co.jp/enterprise/articles/1608/30/news134.html
https://www.antiphishing.jp/news/alert/

このニュースをザックリ言うと･･･

- 前回に引き続き、今回は2週連続でフィッシングメールに関する記事をトップで取り上げていますが、手口が巧妙化しており、十分な注意が必要です。

- 8月29日と30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により、三井住友銀行とゆうちょ銀行を名乗るフィッシングメールおよびサイトを確認したとして警告が出されています。

- 今回のフィッシングメールでは、いずれも件名が「ご登録パスワード変更完了のお知らせ」となっており、本文では「お客さまご自身で変更していない場合は盗用の可能性がございます」といった文面とともに、以下のURLのような偽のサイトへ誘導するものとなっています。

http://www.ssmbc.●●●●.net/
http://www.postt.●●●●.net/

- この他、4月から7月まで月1～2件程度だったフィッシング詐欺発生状況に関して、8月は30日までの時点で7件発生している点についても注意喚起がなされています。

AUS便りからの所感等

- 前回、同協議会からの警告を取り上げたばかり（AUS便り 2016/08/29号参照）ですが、必ずしも同一の文面のフィッシングメールばかりが出回るとは限らず、手を変え品を変え偽サイトへ誘導しようとするのが基本的な手口であることに改めて注意が必要です。

- 今回は必ずしも偽の直接ログイン画面へアクセスするものではないようですが、いずれにせよログイン画面とみられるページでURLが「https://」であるか、EV-SSL証明書を使っているかを確認すること、またこれも繰り返しになりますが、アンチウイルス・UTM・Webブラウザのフィッシング対策機能の活用、正規サイトへはブックマークあるいはGoogle等の検索からアクセスすること等、複数の防御策によりフィッシングを回避することが肝要です。

ITmedia エンタープライズ

2016年08月30日 19時16分 更新

フィッシングメールの内容変更？　だまし手口の巧妙化に警戒を

従来はセキュリティの確認をうながす文面が使われていたが、今度は「パスワード変更をされた方へ」というメッセージが使われている。

[ITmedia]

国内でフィッシングメールが多数出回っているが、8月29日頃からメールの内容に変化があったようだ。メール受信者をだます手口の巧妙化が進んでいる。

フィッシング対策協議会の注意喚起情報によると、4月から7月までの発生状況は毎月1～2件だったが、8月は30日までに7件が発生。4日、19日、29日はそれぞれ2件ずつ発生しており、フィッシング攻撃が拡大しているとみられる。

特に金融機関をかたるメールでは、「システムセキュリティのアップグレードのため、貴様のアカウントの利用停止を避けるために」と、銀行のセキュリティ変更を理由にした文言でフィッシングサイトに誘導する手口が使われていた。

ITmedia エンタープライズ　フィッシング対策協議会 Council of Anti-Phishing Japan

■■
ご登録パスワードの変更完了のお知らせ
■■

このメールは登録パスワードを変更された方へのメールです。

確認のためにメールを送信しています。
お客さまご自身で変更した場合は、このメールを無視しても問題ありません。

お客さまご自身で変更していない場合は盗用の可能性がございます。
至急以下のURLをクリックしてください。
（PC?スマートフォンからご利用ください。）

http://www.smbc.co.jp/idinforeset/changelink.nhn?prm=R2f4thQReL91Td_CUaqNb7bismXy3rNoEqVinBRmwJ-QHg6pn9FIz4OPROjimL_WecGS--F9n5sQAKY6yS_bs8fbsGa5gzWNZzlsh-UnRv8
<http://www.ssmbc.●●●●.net/>

※このメールアドレスに返信頂きましても、ご返答はできませんので、
お問い合わせは三井住友銀行ヘルプのサポートフォームよりお願い申し上げます。
URL : http://www.smbc.co.jp/supportformselect.nhn
<h

今後と

三井住
URL :

29日、30日に発生した三井住友銀行とゆうちょ銀行を名乗る偽メールでは、「ご登録パスワードの変更完了のお知らせ」という文言が使われていた。本文ではパスワード変更がユーザー自身によるものなら無視してよいが、そうでない場合は盗用の可能性があると脅し、確認先と称するURLのリンクをクリックするようながしている。

●駐車場利用仲介サイトから個人情報11万件流出か

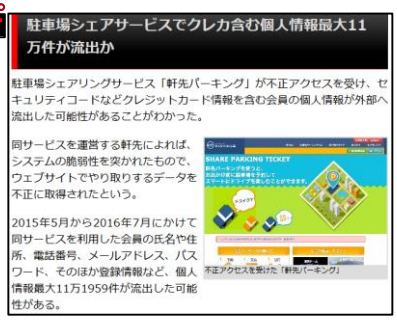
http://www.security-next.com/073174

このニュースをザックリ言うと・・・

- 8月26日（日本時間）、軒先株式会社より、同社の駐車場仲介サービス「軒先パーキング」のサイトが不正アクセスを受け、個人情報約11万件が流出した可能性があると発表されました。

- 流出の可能性のある情報は、2015年5月8日～2016年7月27日にサービスを利用したユーザの個人情報（メールアドレス、パスワード、氏名、住所、電話番号他）最大11万1959件、およびクレジットカード情報（セキュリティコード含む）最大3万8201件とされています。

- 発表によれば、流出は7月27日にクレジットカード決済代行会社からの指摘を受け、第三者機関への調査により発覚したもので、「データベースサーバ内の会員情報が流出したわけではなく、WEBサイト上でデータをやりとりする過程において、外部からの不正アクセスが行われた」としています。


Security NEXT

駐車場シェアサービスでクレカ含む個人情報最大11万件が流出か

駐車場シェアリングサービス「軒先パーキング」が不正アクセスを受け、セキュリティコードなどクレジットカード情報を含む会員の個人情報が外部へ流出した可能性があることがわかった。

同サービスを運営する軒先によれば、システムの脆弱性を突かれたもので、ウェブサイトでやり取りするデータを不正に取得されたという。

2015年5月から2016年7月にかけて同サービスを利用した会員の氏名や住所、電話番号、メールアドレス、パスワード、そのほか登録情報など、個人情報最大11万1959件が流出した可能性がある。

不正アクセスを受けた「軒先パーキング」

AUS便りからの所感等

- 発表の内容から、データベースサーバではなくWebサーバへの侵入があり、個人情報・クレジットカード情報を入力するフォームが改ざんされ、第三者のサイトに入力内容が送信される状態にあったと推測する声があります。

- UTM等により、Webサーバへの侵入や、サーバ内からの不審な通信を防止すること、さらにUTMで防ぎきれない場面をカバーする意味合いとして、外部の監視サービスによるフォームの改ざんの検知等を行うことを推奨致します。

- なお、同社では「より安全性の高いリンク型の決済システムの構築、及び厳重なセキュリティチェックを行った上で再開する」としており、この件を他山の石とし、まだ不正アクセスが発生していない各サービスにおいても、侵入発生時のリスクを最小限に抑えられるシステムへの移行を早い段階で検討することが将来的なコストの抑止の一助となることでしょう（例えば、クレジットカードのセキュリティコードはサーバ上に保存せず、すぐに削除すること等がセキュリティ基準「PCI DSS」において要求されています）。

●Linuxサーバを狙う新手のランサムウェア？Webフォルダを人質に身代金要求

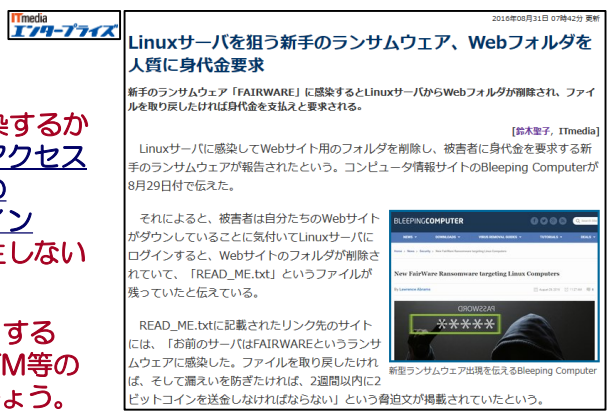
http://www.itmedia.co.jp/enterprise/articles/1608/31/news054.html

このニュースをザックリ言うと・・・

- 8月29日（現地時間）、コンピュータ情報サイトのBleeping Computerにより、Linuxサーバに新手のランサムウェア「FAIRWARE」が感染しているとする事案について警告が出されています。

- 発表によれば、被害者は自分たちのWebサイトがダウンしていることに気付いてLinuxサーバにログインすると、Webサイトのフォルダが削除されており、FAIRWAREを名乗って2週間以内に身代金を支払うよう要求する脅迫文が掲載されていたとのことです。

- 脅迫文では、「削除したファイルを暗号化して自分たちのサーバにアップロードしている」とも書いているとのことですが、Bleeping Computerでは、実際に暗号化まではしていない可能性があり、またファイルを保存しているかどうかについても疑わしく、身代金を支払ってもファイルを取り戻せるかはわからないとしています。


ITmedia エンタープライズ

2016年08月31日 07時42分 更新

Linuxサーバを狙う新手のランサムウェア、Webフォルダを人質に身代金要求

新手のランサムウェア「FAIRWARE」に感染するとLinuxサーバからWebフォルダが削除され、ファイルを取り戻したければ身代金を支払えと要求される。

[鈴木聖子，ITmedia]

Linuxサーバに感染してWebサイト用のフォルダを削除し、被害者に身代金を要求する新手のランサムウェアが報告されたという。コンピュータ情報サイトのBleeping Computerが8月29日付で伝えた。

それによると、被害者は自分たちのWebサイトがダウンしていることに気付いてLinuxサーバにログインすると、Webサイトのフォルダが削除されていて、「READ_ME.txt」というファイルが残っていたと伝えている。

READ_ME.txtに記載されたリンク先のサイトには、「お前のサーバはFAIRWAREというランサムウェアに感染した。ファイルを取り戻したければ、そして漏えいを防ぎたければ、2週間以内に2ビットコインを送金しなければならない」という脅迫文が掲載されていたという。

新型ランサムウェア出現を伝えるBleeping Computer

AUS便りからの所感等

- 現時点でFAIRWAREの挙動については、本当にLinuxに感染するか等を含め不明な点が多いのですが、一方で、Webサーバへのアクセス権限を持つWebサイトの管理者等がランサムウェアやその他のマルウェアに感染することにより、不正にWebサーバにログインされて、Webサイトを改ざんされるというシナリオが今後発生しないとは言い切れません。

- 上に挙げたようなWebサイト等の管理者は、特に自分が利用するPCへのマルウェアの感染に慎重を期し、アンチウイルス・UTM等の活用による防御が十分に行われているか、随時意識すべきでしょう。