— AUS（アルテミス・ユーザ・サポート）便り 2016/04/11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。

●金融機関を狙う「トロイの木馬」減少も･･･上位10カ国のうち日本は4位

https://zuuonline.com/archives/102607
http://www.symantec.com/connect/ja/blogs/2015-73

このニュースをザックリ言うと･･･

- 3月26日（米国時間）、セキュリティベンダーのシマンテック社より、金融機関を狙う「トロイの木馬」の2015年の動向に関するブログ記事が発表されました。

- 大規模なボットネットの活動停止やサイバー犯罪グループの逮捕により、トロイの木馬の検出総数自体は前年(2014年)比で73%減少していますが、脅威は依然として横行しているとのことです。

- 国別では1位が前年同様アメリカ、2位・3位にはそれぞれドイツとインドが前年より上昇してランクインしており、4位は前年同様で日本となっています。

AUS便りからの所感等

- 記事に掲載されている「可能な限り最高レベルのセキュリティを確保するために」推奨されている対策方法では、長年提唱され続けてきた基本的な対策から、二段階認証のような近年登場した手法まで様々です。

- 今や勢いではトロイの木馬はランサムウェアに押されているようにも感じられますが、油断は禁物であり、アンチウイルス・UTM等できうる対策を一通り実施することが肝要です。

ZUU online

金融機関が「トロイの木馬」に狙われている10カ国　日本は4位

（写真＝Thinkstock/Getty Images）

米ソフトウェア会社シマンテックが、最も「トロイの木馬」の標的となっている10カ国を発表した。

最も狙われているのは3年連続で米国。金融機関と
ている消費者数、インターネットの普及率などを考慮
結果ではないだろう。2位のドイツと4位のインドは昨年
加。2013年には米国に次いで2位だった日本は昨年

「トロイの木馬」が狙いうちしている10カ国

9位　豪州
9位　ロシア
8位　フランス
7位　イタリア
6位　カナダ
5位　英国
4位　日本
3位　インド
2位　ドイツ
1位　米国

シマンテック公式ブログ

金融機関に対する脅威 2015 年版: 金融機関を狙うトロイの木馬への感染は 73% 減少しましたが、脅威は依然として横行

検出の件数こそ減少しましたが、金融機関を狙うトロイの木馬はますます高度になり、金融機関を直接狙うケースも増えてきました。

投稿者: Candid Wueest　シマンテック技術者

作成日 23 Mar 2016

0　共有

金融機関を狙うトロイの木馬を利用して、オンラインバンキングのユーザーから金銭を詐取する手口は、儲けを狙うサイバー犯罪者の間では今でも多用されています。検出される件数は減少する傾向にありますが、金融機関を狙うトロイの木馬は高機能になりつつあり、まだ当面その脅威は続くでしょう。しかも、マルウェアを使って、ある

金融機関と
イの木馬の
した。

対処方法

可能な限り最高レベルのセキュリティを確保するために、以下の推奨事項に従ってください。

- 迷惑メールや予想外のメール、疑わしいメールを受信したり、電話を受けたりした場合には注意する。
- セキュリティソフトウェアとオペレーティング・システムを最新の状態に保つ。
- 可能であれば、2FA（2 段階認証）などの高度なアカウント保護機能を有効にする。
- すべてのアカウントに強力なパスワードを使う。
- セッションが終了したら必ずログアウトする。
- 可能であれば、アカウントのログイン通知を有効にする。
- 疑わしい取引がないか、オンラインバンクの取引明細を常に監視する。
- サービスの利用中に不自然な挙動があった場合には、金融機関に通知する。
- オンラインバンキングでの取引には慎重を期し、特に銀行の Web サイトの動作や外見が変わっていないかどうか注意を払う。
- Microsoft Office 文書を添付したうえ、マクロを有効にして内容を確認するよう勧めてくるメールには、特に警戒する。信頼できる差出人から送信された正規のメールであることが絶対に確実な場合を除き、マクロはけっして有効にせず、そのままメールを削除してください。
- BEC 詐欺の被害にあわないように、取引の承認ビジネスプロセスを強化する。

●NEC製無線LANルータに「CSRF」の脆弱性

http://internet.watch.impress.co.jp/docs/news/20160404_751525.html

このニュースをザックリ言うと・・・

- 3月30日（日本時間）、NECプラットフォームズ株式会社は、同社製無線LANルータ「Aterm」シリーズにクロスサイトリクエストフォージェリ（CSRF）の脆弱性が存在することを発表しました。

- ルータの「クイック設定Web(管理画面)」にログインしたブラウザが攻撃者が用意した悪意のあるWebページにアクセスした場合、ルータ管理者の権限で設定の変更や再起動等意図しない動作を密かに実行される可能性があるとされています。

- Atermシリーズのうち、9機種については同日に脆弱性を対策するファームウェアのアップデートがリリースされ、また2機種については後日リリース予定となっており、この他、回避策として「クイック設定Webの利用後は一旦全てのブラウザを閉じる」ことが示されています。

AUS便りからの所感等

- Atermシリーズは上記機種以外にも多くの機種が出回っていますが、サポート期限が切れた等の理由からアップデートはリリースされないとみられ、回避策をとる必要があります。

- 「クイック設定Web」へのログインで用いられているBASIC認証の仕様上、一度ログインした後ブラウザを起動したままログアウトはできないことに注意してください。

- CSRFを不正に実行するようなWebページをアンチウイルス・UTM等で検出することは困難とみられ、一方で、マルウェアに感染した場合はルータ側の脆弱性の有無に拘わらず不正行為を実行される可能性もあり、いずれの観点においても必要な対策をとるべきでしょう。

INTERNET Watch

無線LANルーター「Aterm」シリーズの複数機種にCSRFの脆弱性

(2016/4/4 17:20)

NECプラットフォームズ株式会社は3月30日、同社が提供する「Aterm」シリーズの無線LANルーター製品にクロスサイトリクエストフォージェリ(CSRF)の脆弱性が存在することを公表し、そのうちの9機種について、この脆弱性を修正するファームウェアを公開した。

この脆弱性は、Aterm製品のウェブ管理画面にログインしたままの状態で、細工された悪意のあるウェブページにアクセスした場合、意図しない操作(設定変更や再起動)をさせられる可能性があるというもの。2016年3月以前に発売した製品が対象(一部を除く)となっている。

「W300P」「W500P」「WF300HP2」「WF800HP」「WR8165N」「WF1200HP」「WF1200HP2」「WG1400HP」「WG1800HP2」の9機種については、3月30日公開のファームウェアで修正した。さらに「W300P(HC100RCセット品)」「WG1800HP」についても、4月中に修正版ファームウェアを公開する予定だ。

●ランサムウェア感染からのリカバリ能力に自信があるセキュリティプロフェッショナルはわずか38%・・・Tripwire調査

https://www.tripwire.co.jp/press/2016/0406.html

このニュースをザックリ言うと・・・

- 3月24日（米国時間）、データ改ざん検知ソリューション等を提供する米Tripwire社より、情報セキュリティカンファレンス「RSA Conference」にて200人のセキュリティプロフェッショナルを対象に行ったセキュリティに関する調査の結果が発表されました。

- 「ランサムウェアの感染から重要なデータを失うことなくリカバリできるか」という質問に対し、「非常に自信がある」と答えた回答者は38%に留まったとのことです。

- この他、「自社の幹部はフィッシング詐欺を見抜けない」と答えたのは52%、「過去12ヶ月間でスピア(標的型)フィッシング攻撃が増加した」と答えたのは58%にのぼっています。

AUS便りからの所感等

- 近年になって話題となったランサムウェア、古典的な手法ながら常に新しい手口が登場するフィッシング詐欺やスピア型(標的型)攻撃、いずれにおいても、今どういった攻撃手法が流行しているか、どうすれば回避できるか、あるいはシステムやデータが破壊された場合にどうすれば復旧できるか、等についてシステム管理者が把握していることは重要です。

- 例えばデータのバックアップにおいても、定期的に、確実にバックアップしていることはもちろん、その全体あるいは一部を必要なときに適切に復元できることこそが大事です。

- システムをアンチウイルスやUTM等によって防御する体制を構築することはもちろんですが、加えて情報収集を行いそれをユーザに対し共有することも、組織全体における安全度を高めるために効果的な方策です。

tripwire

TripwireによるRSAカンファレンスにおける調査：

ランサムウェア感染からのリカバリ能力に自信があるセキュリティプロフェッショナルはわずか38%

(本資料は、2016年3月24日にTripwire, Inc.が発表した情報の対訳です)

米オレゴン州ポートランド － 2016 年 3 月 24 日 － 高度な脅威、セキュリティ、コンプライアンスの主要なグローバルプロバイダである Tripwire, Inc. は本日、2016 年 2 月 29 日から 3 月 4 日まで開催された RSA カンファレンス 2016 に参加した 200 人のセキュリティプロフェッショナルに対する調査の結果を発表しました。

「ランサムウェアの感染から、重要なデータを失うことなくリカバリできるかという質問に対し、「非常に自信がある」と答えたのは回答者のうち、わずか38%でした。