— AUS（アルテミス・ユーザ・サポート）便り 2016/06/27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。

●国内ネットバンキングを狙う「URSNIF」が新たに拡散中･･･年休申請メール等に偽装

http://blog.trendmicro.co.jp/archives/13471
https://www.jc3.or.jp/topics/gozi.html
http://nlab.itmedia.co.jp/nl/articles/1606/17/news081.html

このニュースをザックリ言うと･･･

- 6月15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および日本サイバー犯罪対策センターより、国内ネットバンキングを狙うマルウェア「URSNIF（アースニフ）」（別名Gozi）が5月末以降多く確認されているとして、相次いで警告が発表されています。

- URSNIFは主にスパムメールにzipファイルで添付される形で拡散しており、地方銀行を含む中小金融機関を中心に40件弱の国内ネットバンキングを狙うものが確認されています。

- 特に「年休申請」を偽装したメールは、トレンドマイクロ社が把握した分だけでも6月1日～6月7日前後に2000通が出回っていたほか、「請負契約書」「年次運用報告書」「算定届出書」「状況一覧表」、およびネット通販からの「支払確認」等に偽装したものも確認されているとのことです。

AUS便りからの所感等

- ネットバンキングのアカウントを詐取するマルウェアはかれこれ10年近く前から存在しており、メールの添付ファイルで拡散するもののほか、Webサイトの改ざんや不正な広告を介して感染するものも多くあります。

- トレンドマイクロ社では後者のケースにおいて、古いバージョンのFlash Player、Internet Explorer、Javaに存在する脆弱性を突いて感染するケースを挙げており、これらを含めたPC上のOS・アプリケーションを欠かさずアップデートするよう推奨しています。

- もちろんこれだけではなく、アンチウイルスやUTMによる防御のほか、ネットバンキングで近年使われるようになっている二段階認証の利用も必要不可欠でしょう。

TREND MICRO トレンドマイクロ セキュリティブログ

国内ネットバンキングを狙う「URSNIF」が新たに拡散中

投稿日：2016年6月15日
脅威カテゴリ：不正プログラム，スパムメール，スパイウェア，サイバー犯罪，Webからの脅威
執筆：セキュリティエバンジェリスト 岡本 勝之

2016年に入り、ランサムウェアが一層の猛威を振るっていますが、その裏で国内ネットバンキングを狙うオンライン銀行詐欺ツールも活発化が見られています。トレンドマイクロではこの 5月末以降、オンライン銀行詐欺ツール「URSNIF（アースニフ）」の電子メール経由での拡散を国内で確認しました。トレンドマイクロの調査では、今回拡散している「URSNIF」（別名：GOZI）では、地方銀行などの中小金融機関を中心に 40件弱の国内ネットバンキングを狙うものも確認されています。

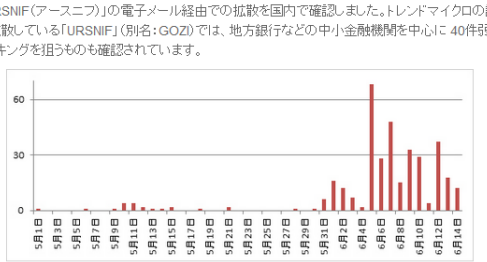


図1：日本国内での「TSPY_URSNIF」の検出台数推移

■拡散の主体はメール経由
検出台数の推移をみると、オンライン銀行詐欺ツール本体である「TSPY_URSNIF」の国内での検出は 6月に入り急増していることがわかります。この検出台数急増に関わる主な拡散経路は、マルウェアスパムが中心です。トレンドマイクロでは最終的に「URSNIF」の拡散を行う多種多様なマルウェアスパムを確認しており、5月末以降本稿執筆時の 6月13日までにその数は合わせて 3万件以上となっています。中でも「年休申請」を偽装したメールは 6月1日から 6月7日前後まで拡散が確認され、トレンドマイクロが確認しただけでもおよそ2000通が出回っていました。

JC3 一般社団法人 日本サイバー犯罪対策センター

インターネットバンキングマルウェア「Gozi」による被害に注意

2016年 6月15日更新

JC3では、IT事業者、セキュリティ事業者、金融機関、警察などのJC3会員と協力して、不正送金の被害軽減に向けた分析を進めています。
今般、警察庁からの情報提供により、インターネットバンキングマルウェアGoziの感染及びこれによる被害の発生を確認し、会員企業からのデータと合わせて分析したところ、Goziの感染が広がりつつあり、その被害が拡大するおそれがあると認識しています。
Goziは、金融機関関連情報を窃取するなどの機能がある不正プログラムであり、Goziに感染した端末を使用してインターネットバンキングを利用すると、ID・パスワードなどの情報が窃取され、銀行口座から不正送金が行われてしまうおそれがあります。
Goziに感染してインターネットバンキングに係る不正送金などによる被害にあわないよう、以下を参考に、適切なセキュリティ対策を講じてください。
JC3では、今後も分析を継続してまいります。

○ 適切な対策
- ウイルス対策ソフトを導入し、パターンファイルを常に最新の状態に更新する。
- 基本ソフト（OS）や、ウェブブラウザーなどの各ソフトウェアを常に最新の状態に更新する。
- インターネットバンキングにアクセスした際に不審な入力画面等が示された場合、ID・パスワード等を入力しない。
※このような場合には、ご利用の金融機関等に連絡してください。
- 可変式パスワード生成機（ハードウェアトークン）等によるワンタイムパスワードを利用する。
- 金融機関が二経路認証やトランザクション認証など高度なセキュリティ対策を導入している場合は、これらを利用する。
- 意図しないログイン履歴がないか、自分の口座の入出金明細等を定期的に確認する。

ねとらぼ

» 2016年06月17日 10時46分 更新

年休申請メールを開いたら銀行詐欺ツール　地方ネットバンクを狙うスパムメールが活発化

他にも「請負契約書」「年次運用報告書」「算定届出書」「状況一覧表」などの偽装メールが確認されています。

[コンタケ，ねとらぼ]

トレンドマイクロのセキュリティブログによると、国内のネットバンキングを狙う銀行詐欺ツール「URSNIF（アースニフ）」が活動を活発化させています。地方銀行などの中小金融機関を中心に、40件近いネットバンキングが攻撃対象になっているとのこと。

この銀行詐欺ツールは、主にスパムメールで拡散されています。特に、「年休申請」を偽装したメールは6月1日から6月7日前後までで、トレンドマイクロが確認しただけでもおよそ2000通が出回っていたとのこと。

●女性雑誌「ViVi」の通販サイトから個人情報流出

http://news.mynavi.jp/news/2016/06/22/431/

このニュースをザックリ言うと・・・

- 6月22日（日本時間）、講談社発行の女性雑誌「ViVi」の公式通販サイト「NET ViVi Coordinate Collection」（以下Net ViVi）が不正アクセスを受け、2015年8月22日から2016年4月18日までの注文者10,946人分の個人情報、および注文情報15,581件が流出していたことが講談社、同サイトを共同運営するウェアハート社、およびサイト構築を行ったパイプドビッツ社の3社から発表されました。

- 発表によれば、4月に同サイトへの一連の不正アクセスが発生し、結果4月18日に注文履歴情報がダウンロードされたとのことで、6月に入りウェアハート社が不正な注文情報に気付き、調査を行った結果発覚したものとされています。

- 個人情報には、注文者および発送先の氏名・住所・メールアドレス・電話番号等を含んでいたとされており、会員のアカウント情報やクレジットカード番号等は含まれていなかったとのことです。

AUS便りからの所感等


マイナビニュース
「ViVi」通販サイトで約1.1万人の個人情報流出、脆弱性攻撃で
[2016/06/22]
講談社は22日、「ViVi」公式通販サイト「NET ViVi Coordinate Collection」に外部からの不正アクセスがあり、会員10,946名の個人情報の流出を確認したと発表した。
「NET ViVi Coordinate Collection」は、パイプドビッツが提供するアパレル特化型ECプラットフォーム「スパイラルEC」を利用し、2015年8月22日からパイプドHDグループ会社のウェアハートと講談社が共同運営している。
講談社
「ViVi」公式通販サイト
「NET ViVi Coordinate Collection」不正アクセスによる
個人情報流出についてのお詫び
講談社による発表文(一部)

- パイプドビッツ社による発表では、攻撃者は同社開発によるECプラットフォームの脆弱性を突いてバックドアをアップロードし、管理画面に不正ログインおよび注文履歴情報のダウンロードを行ったとみられています。

- 不正アクセスの成功に至ったポイントとしては、Webサーバにおいて「WebDAV」が有効になっており、かつ適切なアクセス制限が行われていなかったこと、管理画面へのログインパスワードが推測され易いものになっていたことの2点でしょう。

- 確認された問題点に対し、例えばUTMの設置のような一つの対策だけ行えばOKということはなく、一方で、外部から直接アクセスされることはないと油断していれば、今回のようにバックドアを介して侵入される恐れは十分あると言えるでしょう。

●Apache Struts 2に深刻な脆弱性、既に有効な攻撃コードが公開

https://www.ipa.go.jp/security/ciadr/vul/20160620-jvn.html

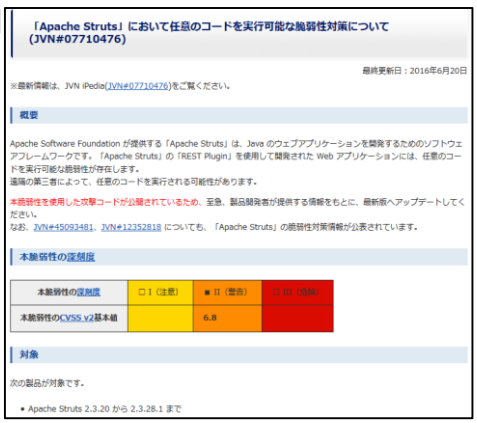
このニュースをザックリ言うと・・・

- 6月20日（日本時間）、IPA（独立行政法人情報処理推進機構）や国内大手セキュリティベンダーのラック社より、Webアプリケーションフレームワーク「Apache Struts 2」に重大な脆弱性が発見されたとして警告が発表されました。

- 脆弱性が存在するのはStruts 2.3.20～2.3.28.1で、不正なWebアクセスにより、サーバ上で任意のOSコマンドを実行される恐れがある模様です。

- ラック社ではStrutsを対策バージョン2.3.29にアップデートする等の対策をとることを推奨しています。

AUS便りからの所感等


IPA Better Life with IT 情報処理推進機構
「Apache Struts」において任意のコードを実行可能な脆弱性対策について
(JVN#07710476)
最終更新日：2016年6月20日
※最新情報は、JVN iPedia(JVN#07710476)をご覧ください。
概要
Apache Software Foundation が提供する「Apache Struts」は、Java のウェブアプリケーションを開発するためのソフトウェアフレームワークです。「Apache Struts」の「REST Plugin」を使用して開発された Web アプリケーションには、任意のコードを実行可能な脆弱性が存在します。
遠隔の第三者によって、任意のコードを実行される可能性があります。
本脆弱性を使用した攻撃コードが公開されているため、至急、製品開発者が提供する情報をもとに、最新版へアップデートしてください。
なお、JVN#45093481、JVN#12352818 についても、「Apache Struts」の脆弱性対策情報が公表されています。
本脆弱性の深刻度
本脆弱性の深刻度 | □ I（注意） | ■ II（警告） | □ III（危険）
本脆弱性のCVSS v2基本値 | | 6.8 |
対象
次の製品が対象です。
• Apache Struts 2.3.20 から 2.3.28.1 まで

- StrutsはJavaによるWebアプリケーション作成のために用いられるソフトウェアの一つで、より軽量で新しいフレームワークがリリースされている今日でもよく利用されている一方、セキュリティホールが比較的多く見つかることでも知られており、また、以前のバージョンであるStruts 1についても、2014年でサポートが終了したにも拘らず、依然として用いられているケースは少なくないとされています。

- セキュリティホールの発見によるアップデートの少ないプロダクトへの移行は、セキュリティリスクを下げる意味で検討に値するでしょうが、大抵のケースではそう簡単に移行できるものではなく、それならばせめてベンダー情報を随時チェックし、アップデートを適宜行える体制を整えておきたいものです。

- そして、アップデート体制が整えられるか否かに拘らず、Webアプリケーションに対する攻撃を検知・遮断するため、サーバの前面にUTMを設置する等の防御策も可能な限りとるべきでしょう。