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。

●日本の利用者を狙う偽通販サイト、犯罪者は悪用のため約7万件のドメイン名を取得

http://internet.watch.impress.co.jp/docs/news/20141224_681760.html
http://blog.trendmicro.co.jp/archives/10605

このニュースをザックリ言うと･･･

- 12月22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は、日本国内のユーザを狙ったフィッシング詐欺のWebサイトが急増していることをブログで報告しました。

- 記事によると、4月2日から12月17日までの間に、詐欺サイトの運営者とみられる同一のメールアドレスから69,079のドメイン名が登録されていることが確認されています。

- これによるサイトにアクセスした日本国内のユーザは約6,400人に上り、特に12月10日以降にアクセスが急増していることから、クリスマスと年末のオンラインショッピングが盛んになる時期に合わせて詐欺サイトへの誘導が行われた可能性が指摘されています。

AUS便りからの所感等

- 月並みではありますが、素性の知れない、見慣れないショッピングサイトで安易に物を購入しようとしないこと、また、普段利用しているサイトへのアクセスのはずが詐欺サイトに誘導されていないか確認すること、いずれも大事なことです。

- 一方で、こういった詐欺サイトへ迂闊に誘導されることのないよう、人間の判断のみで解決することには限界がありますので、ブラウザやセキュリティソフト、あるいはUTMのアンチフィッシング機能を有効活用することもやはり肝要です。


INTERNET Watch

ニュース

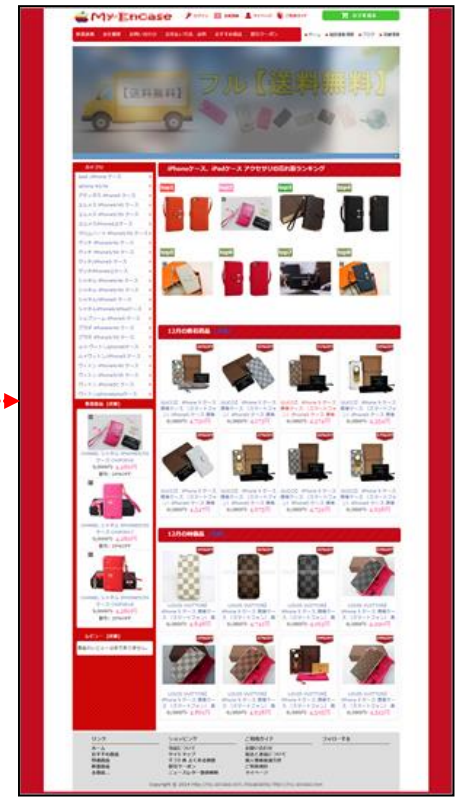
日本の利用者を狙う偽通販サイト、犯罪者は悪用のため約7万件のドメイン名を取得

(2014/12/24 19:19)

トレンドマイクロは22日、日本の利用者を狙う詐欺目的の偽サイト（なりすましECサイト）について調査を進めた結果として、日本国内からおよそ6400ユーザーが詐欺サイトに誘導されていたことや、詐欺サイトの設置者が約7万件ものドメイン名を取得していたことを報告した。

iPhoneのアクセサリー販売を偽装した詐欺サイト

トレンドマイクロでは、iPhoneのアクセサリー販売を偽装した詐欺サイトについて調査を実施。確認された詐欺サイトのドメイン名は、2014年4月2日に登録更新が行われており、4月2日から12月17日までの間に日本国内からおよそ6400ユーザーが詐欺サイトにアクセスしていた。アクセス数は12月10日以降に急増しており、犯罪者はクリスマスや年末などオンラインショッピングが盛んになる時期に合わせて、詐欺サイトへの誘導策を講じたと推察している。



今回確認された問題の詐欺サイト例：
iPhone のアクセサリー販売サイトを偽装

●DNSサーバソフト「BIND」の配布サイトに改ざん被害

http://www.itmedia.co.jp/enterprise/articles/1412/25/news108.html
http://internet.watch.impress.co.jp/docs/news/20141225_681971.html

このニュースをザックリ言うと・・・

- DNSサーバソフト「BIND」を開発している米ISCが同組織のWebサイトが改ざんされていたことを発表し、サイトを一時閉鎖しています。

- セキュリティ企業の米Cyphort社によれば、ISCのWebサイトは改ざんにより、外部のサイトにリダイレクトされるようになっており、IEやFlash PlayerおよびSilverlightの古いバージョンの脆弱性を突いてマルウェアに感染するよう仕向けられていたとのことです。

- ISCでは、最近サイトにアクセスしたことのあるユーザに対し、ウイルススキャンを行うよう呼びかけをしています。

AUS便りからの所感等

- 今回、12月にBINDにDoS攻撃を受ける脆弱性が発表・修正されたばかりであり、アップデート版をダウンロードしようとするユーザをマルウェアに感染させることを攻撃者が狙った可能性が考えられます。

- PCのOSや各ソフトウェアを最新に保ち、アンチウイルス・UTMによる防御を固めることが、まさかという場面でのマルウェア感染を予防するためには欠かせないものです。

記事一覧 | ITマネジメント | ビッグデータ | モバイル | ソーシャル | 海外速報 | セキュリティ | ディルバート | 用語事典 | ホワイトペ

ITmedia エンタープライズ ＞ 海外速報 ＞ DNSソフト開発元サイトがダウン、利用者にマルウェ...

2014年12月25日 14時23分 更新

DNSソフト開発元サイトがダウン、利用者にマルウェア検査を要請

BIND 9やDHCPなどの提供するInternet Systems ConsortiumのWebサイトにマルウェアが仕掛けられた可能性がある。

[ITmedia]

印刷／PDF | ツイート 187 | いいね！ 114 | チェック | 23 | Pocket 28 | 通知

PR バチカン図書館CIO来日 約4千万ページのデジタル文献化事業
PR ZOZOTOWNの強さを支える「顧客と友達のような関係性」とは？

DNSソフトのBIND 9やDHCPなどインターネットの中核となるソフトウェアを提供する米Internet Systems Consortium（ISC）のWebサイトが12月25日現在、メンテナンスモードになっている。ISCは「マルウェアに感染した可能性がある」として、ISCサイトへアクセスした全てのコンピュータでマルウェアスキャンを実施してほしいと呼び掛けている。

●NTPサーバソフトに深刻な脆弱性

http://jvn.jp/vu/JVNVU96605606/index.html
http://www.watchguard.co.jp/securityalert/2014/12/-ntpxtm-1.html

このニュースをザックリ言うと・・・

- 12月19日（米国時間）、PCの時計を調整するNTPサーバのソフトウェア「ntpd」に重大な脆弱性が存在することが発表されました。

- NTPサーバに対し不正なパケットを送信するだけで、サーバが稼働しているホストが乗っ取られる等の可能性が指摘されています。

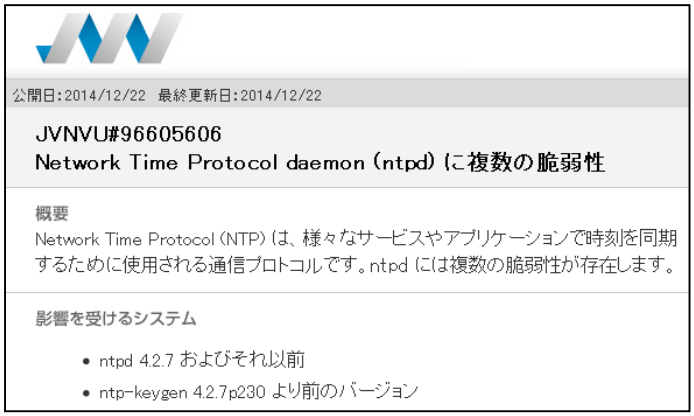
- Linux上のntpdについては、ディストリビューションのベンダーから修正版がリリースされています。

- なお、WatchGuard社「XTMシリーズ」および「Fireboxシリーズ」に含まれるNTPサーバについては、この脆弱性の影響を受けないことがベンダーサイトにて報告されています。

AUS便りからの所感等

- NTPについては、今回の脆弱性以前に、不特定多数からアクセス可能な場合に「DDoS攻撃」に悪用される可能性も指摘されているため、社内LANや組織で持っているIPアドレスからのみ利用できるよう設定を確認することを強く推奨致します（※これはNTPに限らず、外部に公開するもの以外のあらゆるサービスにおける鉄則です）。

- 一方、社内等からのみアクセス可能であっても、マルウェアに感染したクライアントPCがNTPサーバを攻撃する可能性も否定できないため、NTPサーバのアップデートは必要不可欠です。



公開日:2014/12/22 最終更新日:2014/12/22

JVNVU#96605606
Network Time Protocol daemon (ntpd) に複数の脆弱性

概要
Network Time Protocol (NTP) は、様々なサービスやアプリケーションで時刻を同期するために使用される通信プロトコルです。ntpd には複数の脆弱性が存在します。

影響を受けるシステム

- ntpd 4.2.7 およびそれ以前
- ntp-keygen 4.2.7p230 より前のバージョン