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。

●日本も標的になったオンライン銀行詐欺ツール「Dridex」の攻撃者、FBIらが摘発

http://news.mynavi.jp/news/2015/10/17/121/
http://www.symantec.com/connect/ja/blogs/dridex

このニュースをザックリ言うと･･･

- 10月14日（米国時間）、大手セキュリティベンダーのシマンテック社は、ネットバンキングを狙うボット型マルウェア「Dridex」を利用していた犯罪グループがFBIやイギリス国家犯罪対策庁等の国際的な捜査活動によって摘発されたと同社ブログで発表しました。

- 記事によれば、Dridexは昨年度29,000件の検出が報告されており、今年は5月と6月にそれぞれ月間15,000件前後が検出されていたとのことで、国別での検出された割合では、米国の37%に次いで日本が22%、ドイツが20%となっています。

- 今回の摘発においては、マルウェアに感染した数千台のPCをボットネットによる制御から遮断し、不正な命令を送らない偽の指令サーバへリダイレクトする、いわゆる「シンクホール」対策がとられたとのことです。

AUS便りからの所感等

- 一つの大きなボットネットが撲滅されても、他のボットネットが取って代わるという「いたちごっこ状態」は続くという見方もできますが、とにかくユーザにできることはマルウェアに感染しないよう粛々と対策を行うことです。

- アンチウイルス・UTMの導入をはじめ、様々な対策を打っていくことがマルウェアに立ち向かう重要な一歩となっていくでしょう。

マイナビニュース　　シマンテック公式ブログ

日本も標的になったオンライン銀行詐欺「Dridex」の攻撃者、FBIらが摘発

[2015/10/17]

シマンテックは10月14日、オンライン銀行詐欺ツール「Dridex」でオンラインバンキング情報を盗み出すサイバー犯罪集団が国際的な捜査活動によって摘発されたとブログで公開した。

この摘発は、米国のFBI、英国の国家犯罪対策庁をはじめ、世界各国の捜査当局がDridexボットネットに対する捜査に参加した結果だ。今回の捜査により30歳のモルドバ人男性が告発された。この男性は8月にキプロスで逮捕されており、米国への引き渡し手続き中だという。

また、ボットネットによる制御から遮断するため、危殆化した数千台のコンピュータをシンクホールに捕捉する協力態勢も整ったという。この摘発によって、全世界の被害者から何千万ドルという金銭を盗み出してきたサイバー犯罪者の不正行為に歯止めをかけたと見られている。

Bugatとも呼ばれるDridexはシマンテックではW32.Cridexとして検出は、金融機関を狙い、感染したコンピュータをボットネットに追加。被害者のWebブラウザに自身を組み込み、オンラインバンキング情報などの情報を盗み出す。

フィッシングメールを通じた拡散が一般的で、そのメールは正規のソースから送信されたように見えるので、被害者は悪質な添付ファイルを開いてしまう。

また、マッピングされたネットワークドライブや、USBドライブなどのローカルストレージに自身をコピーして自己複製する機能も持っている。Dridexのグループは定期的に戦術を変えており、ごく最近では、Microsoft Office文書に悪質なマクロを仕込んでメールに添付、被害者に感染させたことが確認されている。

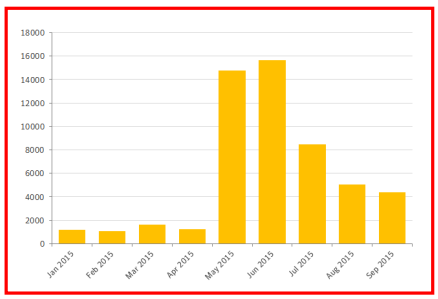

図1. 2015 年の Dridex 検出件数

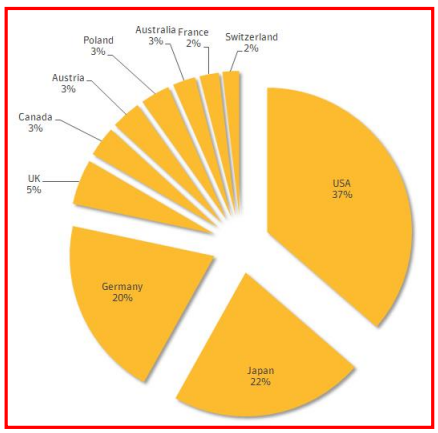

図2. 2015 年、Dridex 感染件数の上位 10 カ国

●NTPサーバソフトに脆弱性、システム時刻を変更される恐れ

http://www.itmedia.co.jp/enterprise/articles/1510/23/news052.html

このニュースをザックリ言うと・・・

- 10月21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として、Network Time Foundation（NTF）および米Cisco傘下のセキュリティ企業Talosから相次いで発表されました。

- この脆弱性（CVE-2015-7871）は、NTPサーバに対し攻撃者が不正なパケットを送信することにより、攻撃者が用意した悪意のあるサーバと強制的に時刻を同期させられ、時刻情報を改ざんされる等の可能性が指摘されています。
（現在、NTFからは、これを含め複数の脆弱性を修正したバージョンがリリースされています。）

AUS便りからの所感等

- サーバの時刻情報を不正に変更されることにより、サーバ上での時間帯ベースでのアクセス制限、定期的なコマンドの実行、あるいは各種ログ収集等に支障が出る可能性があります。

- NTPについては、以前より脆弱性が度々指摘されていること、また大抵は不特定多数に対し公開する必要がないことから、社内LANや組織で持っているIPアドレス以外からのアクセスを制限するよう設定することを強く推奨致します。

ITmedia エンタープライズ

2015年10月23日 07時30分 更新

NTPに脆弱性、システム時刻を変更される恐れ

被害者はntpdプロセスが悪質な時刻源と同期させられて、攻撃者の任意の時刻に変更されてしまう恐れがある。

[鈴木聖子, ITmedia]

インターネット経由で時刻を取得するためのNTPデーモン（ntpd）に脆弱性があり、攻撃者に時刻を変更されてしまう恐れがあることが分かった。Network Time Foundation（NTF）は10月21日、更新版を公開してこの脆弱性に対処した。

米Cisco傘下のセキュリティ企業Talosによると、脆弱性は特定の暗号NAKパケットの処理におけるロジックエラーに起因する。認証を受けない攻撃者が不正なパケットを送りつける手口で認証をかわし、被害者のntpdプロセスを悪質な時刻源と同期させて、任意の時刻に変更できてしまう恐れがある。

- 今後、Linuxサーバのみならず各種アプライアンス等のネットワーク機器のNTP機能において脆弱性が存在するか否かの情報がベンダーから出てくると思われますので、確認の上、必要に応じてアップデートの対応を行うようにすることと、不正なNTPパケットを遮断するためにUTMを前面に設置することも検討に値するかと思われます。

●Google Chromeになりすます偽物が確認される

http://headlines.yahoo.co.jp/hl?a=20151020-00000010-it_nlab-sci

このニュースをザックリ言うと・・・

- 10月16日（米国時間）、アンチウイルスソフト等を提供する米Malwarebytes社がGoogle Chromeになりすます偽のブラウザ「eFast browser」について同社ブログで警告しています。

- eFast browserは、PCにChromeがインストールされていた場合、自身をデフォルトブラウザとして設定し、デスクトップやタスクバーのChromeへのショートカットを削除する等の挙動をとるとされています。

- Malwarebytes社は、同ブラウザを悪意のあるソフトウェアとはまだ断定できてはいないものの、他のフリーソフトウェアにバンドルされてインストールされることが多いことを指摘、無断でユーザの情報を収集するなどの不審な動きをとる可能性があるとして注意を呼びかけています。

AUS便りからの所感等

- フリーソフトウェアのインストーラに他のソフトウェアがバンドルされるケースは多々見られ、一切のユーザの承諾なく密かにインストールするケースよりも、堂々とそれを示し、インストールする旨のチェックを外さないことにより、インストールに承諾したものとみなす、というケースが目立っています。

- とにかく、ソフトウェアのインストール時には、不要なバンドルソフトウェアの導入にうっかり承諾しないよう十分な注意を払うこと、また、正規のものではない不審なインストーラをダウンロードしようとする動きに対しても、Webブラウザセキュリティ機能あるいはアンチウイルスやUTMの活用によって防御することが重要です。

YAHOO! JAPAN ニュース

Google Chromeそっくりな悪質ブラウザ「eFast Browser」に注意
気付かないうちにGoogle Chromeと置き換わっていることも

ねとらぼ 10月20日(火)8時10分配信

ツイート 985　シェア 1692

eFast browser hijacks file associations

ユーザーが気付かないうちにGoogle Chromeになり変わってしまう「eFast Browser」というブラウザについて、海外のセキュリティブログが注意を呼びかけています。

【デザイン：Chromeとそっくりです】

「eFast Browser」の機能や挙動などは基本的にGoogle Chromeとほぼ同じ。アイコンもそっくりで、使い勝手も変わらないため、気付かないまま使っている人もいると指摘されています。