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。

●「不審なメールに注意する」だけでは不十分、「不審と気付けない標的型メール」への対策が急務

http://internet.watch.impress.co.jp/docs/news/20150820_717053.html
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20150818013824.html

このニュースをザックリ言うと・・・

- 8月20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が2015年第2四半期（4～6月）のセキュリティ動向を分析したレポート「セキュリティラウンドアップ」を公開し、その中でのトピックの1つとして、国内の企業・組織が相次いで被害を公表した標的型メールによる「気付けない攻撃」について取り上げています。

- レポートでは、情報窃取を目的とした主なサイバー攻撃事例15件のうち12件が標的型メールによって組織内部へ侵入されたものであること、また14件は外部からの指摘があって初めて発覚したことを指摘しています。

- この他、標的型サイバー攻撃で頻繁に使用される遠隔操作ツールによる事例19件において、送信された標的型メールの79%が送信者情報を国内組織のものに偽装していたこと、また5件においては「パスワード付きの添付ファイルを送信→2通目でパスワードを送信」という手口がとられ、「ビジネスマナーで通常行われる方式」を逆手に取った、添付ファイルを開きやすくする工夫がなされたものと分析しています。

- 同社では、「標的型メールは一見しただけでは不審と気付かない偽装工作が複数施されているため、受信者側の『不審なメールに注意する』という心がけでは不十分」と指摘、「サンドボックス(※)などの技術で添付ファイルを解析する標的型メール対策や、『気付けない攻撃』を侵入後に早期発見できる対策の導入・体制整備が急務となっている」としています。

- 上記以外のトピックとしては、第2四半期における攻撃ツールが設置されたサイトへのアクセスは前期の67%増となる396万8709件、うち国別のアクセス元が最も多かったのは日本の49%で、2位アメリカ（22%）を大きく上回っていたとのことです。

AUS便りからの所感等

- 例えば、攻撃メール等に用いられる文言も以前は違和感の多い日本語であったものが最近では洗練されたものとなっており、一昔前には安心できていたことが通用しなくなってきています。

- マルウェアへの感染あるいは回避において、人間の判断が分かれ目となってしまうことが無いよう、その前段でアンチウイルスやUTMをはじめ様々なシステムがマルウェアの侵入を食い止める、安全な環境への見直しが重要となるでしょう。


INTERNET Watch

最新ニュース

マネーフォワード、給与明細のペーパーレス化サービスを無料提供
2015/08/28

JR北海道、標的型メールでマルウェア感染、列車運行システムに影響はなし
2015/08/28

Facebook、1日の利用者が10億人を超える＝地球上の7人に1人
2015/08/28

Instagram、「横長」「縦長」フォーマットにも対応
2015/08/28

パスワードに依存しない新たな認証の仕組み「FIDO」を推

ニュース

「不審なメールに注意する」だけでは不十分、「不審と気付けない標的型メール」への対策が急務

(2015/8/20 14:59)

トレンドマイクロ株式会社は20日、セキュリティ動向を分析した四半期レポート「2015年第2四半期セキュリティラウンドアップ」を公開した。同社サイトよりPDFファイルでダウンロードできる。

今回の報告書では、四半期のトピックの1つとして、国内の企業・組織が相次いで被害を公表した標的型メールによる“気付けない攻撃”について取り上げている。巧妙な偽装工作が施された標的型メールによる攻撃が多数確認されており、トレンドマイクロが把握している15件の事例のうち12件が、標的型メールによって組織内部へ侵入されたものだったという。

また、15件のうち14件が、外部からの指摘などで発覚したものであり、被害に遭った組織自身では被害に遭ったことをそもそも気付けなかったとしている。

IT用語辞典 e-Words

（※）サンドボックス【 sandbox 】

サンドボックスとは、保護された領域内でプログラムを動作させることで、その外へ悪影響が及ぶのを防止するセキュリティモデル。「子供を砂場（サンドボックス）の外で遊ばせない」という言葉が語源だと言われている。

このモデルでは、外部から受け取ったプログラムを保護された領域、「箱」の中に閉じ込めてから動作させる。「箱」は記憶域内の他のファイルやプロセスからは隔離され、内部から外界を操作することは禁じられている。

このため、そのプログラムが暴走したり、外部から侵入した悪質なウイルスであっても、「箱」の外にあるデータなどに影響を与えることはできない。

●IEの脆弱性攻撃発生、日本のユーザに影響集中

http://www.itmedia.co.jp/enterprise/articles/1508/26/news111.html
http://www.symantec.com/connect/ja/blogs/sundown-internet-explorer

このニュースをザックリ言うと･･･

- 8月25日（日本時間）、大手セキュリティベンダーのシマンテック社が同12日に修正パッチがリリースされたIEの脆弱性「MS15-079」を悪用する攻撃を確認したと同社ブログで発表しました。

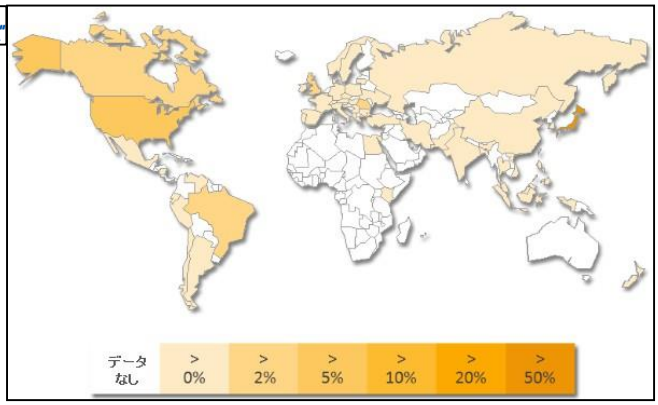
- 攻撃の影響は日本のユーザに集中しており、正規のWebサイトをクラックしてバックドア型のマルウェアを仕込み、ターゲットとするユーザがサイトにアクセスして感染するのを待ち受ける、いわゆる「水飲み場型攻撃」の形をとっている模様です。

- また、攻撃にあたっては「Sundown」と呼ばれる攻撃ツールが用いられ、前述した以外のIE・WindowsおよびFlash Playerの脆弱性を悪用する他、先に相手PCの環境をチェックし、特定のセキュリティソフトが存在する場合には感染行為を停止するといった、検出を回避する機能を持ち合わせているとのことです。

AUS便りからの所感等

- IEについては、8月19日にも定例外のセキュリティ情報「MS15-093」が発表されていますので、両方とも（もちろんその他の全てのパッチも）必ず適用してください。

- アンチウイルスやUTMからマルウェアの存在を隠すことにより、安心したユーザがそれらの防御をしていない環境からアクセスして感染してしまう可能性には注意すべきですし、どんな場合であっても適切な防御機構を介してインターネットへアクセスするよう注意をはらうことが肝要です。



攻撃の影響を受ける地域の割合。半数以上が日本に（Symantecより）

●自称「情報強者」ほど、モバイルセキュリティは脆弱?

http://prtimes.jp/main/html/rd/p/000000004.000012831.html

このニュースをザックリ言うと･･･

- 8月20日（日本時間）、モバイルに特化したセキュリティソリューションを提供するルックアウト社が国内スマートフォン所有者の「モバイルプライバシーIQ」、すなわちスマートフォン使用時における安全なプライバシー保護に関する個人の知識レベルについての調査結果を発表しました。

- 調査の中で、「自分のモバイルプライバシーIQは平均以上～高レベルである」と評価している人はわずか3%でしたが、該当するユーザの多くは他のユーザよりも公共Wi-Fiやオープンネットワークに接続したり、非公式マーケットプレイスからモバイルアプリをダウンロードしたりなどの危険な行為を取る可能性が高く、モバイルセキュリティ対策において全般的に意識の欠如が見られる、と指摘されています。

- 一方、企業が憂慮すべき事態として、消費者は自分が勤務している企業の機密データの保護よりも個人情報の保護に対する懸念が高いこと、また情報漏えいが発生しないよう最も気をつけるべきデータは企業の機密データであると答えたのはわずか3%であること、が示されています。

- 同社はこの結果から、「プライバシー問題に関する意識とプライバシー保護のために行っている実際の行動の間にギャップがある」と結論付けており、またモバイル端末に保存されている個人情報を保護する方法として「PINやパスコードの設定」「公共Wi-Fiではメール・SNSを使わずそれ以外のWebサイトの閲覧に留める」「アプリのダウンロード時はレビューに注意する」等を挙げています。

AUS便りからの所感等

- モバイル機器の利用にあたっては、「簡単にネットにアクセスできる方法」に依存せず、可能な限り自前で用意したより安全なネットワークを経由してアクセスすることが重要であり、特に端末とそのネットワークの間では、盗聴等が発生しないようVPN等を用いた暗号化通信を行うことが不可欠となります。

- VPN機能を提供するUTMを利用することにより、社内LANからのアクセス並みの安全性を保ちながらのネットへのアクセスが期待できるでしょう。