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。

●バナー広告等からFlash Playerの脆弱性を突く攻撃発生…東京都職員のPCがマルウェア感染

http://www.sankei.com/affairs/news/150722/afr1507220004-n1.html
http://www.sankei.com/affairs/news/150722/afr1507220005-n1.html

このニュースをザックリ言うと・・・

- 7月21日（日本時間・以下同様）、東京都は、職員のPC9台が不正な広告を介してマルウェアに感染したことを発表しました。

- 問題となった広告は、Flash Playerの脆弱性を悪用し、Webサイト上に表示されるだけでPCに感染する仕組みになっており、大手新聞社サイトに配信されていた他、厚生労働省の外郭団体「安全衛生技術試験協会」のサイトが改ざんされてマルウェアが置かれていたとのことです。

- 感染したPC9台は外部との不正な通信を行っており、うち4台において、内規に反して約2,700人分の住所・口座番号などの個人情報が保存されていたとされていますが、流出したかについては不明のようです。

AUS便りからの所感等

- Flash Playerの修正版がリリースされたのは7月9日、一方感染が発覚したのは14日で、修正版を適用する前のテストを行っていたタイミングで感染が発生したとされています。

- トレンドマイクロ社によれば、7月13日～22日の間にFlash Playerの脆弱性を攻撃するマルウェアがWebサイト上に配置されるケースが25件あり、日本人ユーザを狙った同種の攻撃が引き続き行われる可能性もあります。

- 「ゼロデイ攻撃」がこういった数日の差で入り込むことを鑑みれば、理論上最も安全なのは修正の適用までの間無効化することですが、それができない状況で少しでも感染または不正なサイトへの誘導の可能性を抑えるため、アンチウイルス・UTMによる防御が必要不可欠でしょう。


産経ニュース

朝日、読売のニュースサイトからも感染　バナー広告表示、即感染　都職員のPC被害

ブログに書く 5　ツイート 800　おすすめ 365　g+1 42　(1/2ページ)

東京都は21日、インターネットのサイト上に表示されたバナー広告を介し、職員のパソコン（PC）9台がウイルスに感染したと発表した。広告をクリックしなくても、表示されただけで感染するプログラムが仕掛けられていたという。

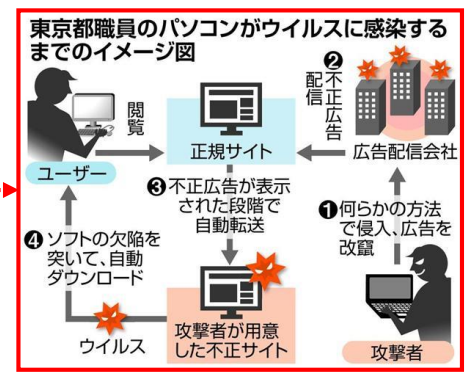
動画再生ソフトの欠陥悪用　プログラム改竄→不正サイトへ転送か

ブログに書く 1　ツイート 32　おすすめ 12　g+1 1　(1/2ページ)

今回、東京都職員のPCがウイルス感染する原因となったバナー広告は、広告配信業者が、契約を結んでいる各サイトに、広告を自動配信して表示させる「ネットワーク広告」だったとみられている。

では、どうやってウイルスに感染するのか。

情報セキュリティー会社トレンドマイクロ（東京）によると、一般的に攻撃者側は広告配信業者のシステムに侵入するなどして、特定の広告のプログラムを改竄（かいざん）。それを知らずに業者が改竄された不正広告を配信した結果、サイトに広告が表示されただけで、攻撃者が用意した不正サイトに自動転送され、ウイルス感染する可能性があるという。



TREND MICRO トレンドマイクロ セキュリティブログ

Flash Playerの脆弱性を狙うWeb改ざん攻撃を多数確認

投稿日: 2015年7月23日
脅威カテゴリ: 不正プログラム，サイバー攻撃，脆弱性，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

イタリア企業「Hacking Team」から漏えいしたとされる情報からこれまで未確認だった脆弱性が多数確認されています。中でも、Adobe Flash Playerに関する脆弱性については、日本を狙う改ざんWebサイト経由での標的型サイバー攻撃で利用されていた事例を7月14日付のトロブログ記事でお伝えしています。そして今回トレンドマイクロでは、この Adobe Flash Player の複数の脆弱性の利用した攻撃が、日本国内の改ざんされたWebサイト経由で継続して行われている事を確認しました。

●Windows定例アップデート直後に緊急パッチリリース

http://www.ipa.go.jp/security/ciadr/vul/20150721-ms.html
https://technet.microsoft.com/ja-JP/library/security/MS15-078

このニュースをザックリ言うと・・・

- 7月21日（日本時間）、マイクロソフト社が定例外の「緊急」セキュリティ情報「MS15-078」を発表し、修正パッチをリリースしました。

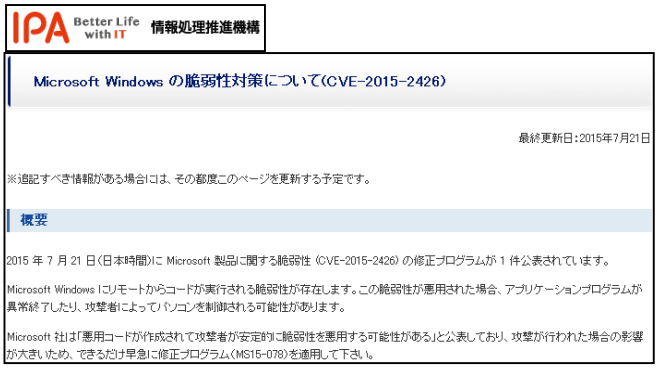
- 修正された脆弱性はWindowsにおけるフォントの処理機能に存在し、不正なフォントが埋め込まれたWebページやOffice文書等の読み込みにより、PCがマルウェアに感染する等の可能性があります。

- 今回リリースされた修正パッチはWindows Vista以降およびWindows Server 2008以降に対するもので、15日をもってサポートが終了したWindows Server 2003（以下Win2003）に対してはパッチがリリースされていません。

AUS便りからの所感等

- Windows XPが2014年4月にサポート終了した後、Internet Explorer（IE）の重大な脆弱点が修正され、XP上のIEについてもパッチがリリースされたことがありましたが、あくまで特例であり、今回についても同様の対応がとられることは期待できません。

- マイクロソフト社のページではパッチを適用しない場合の回避策も掲載されていますが、手順を誤るとOSが正常に動作しなくなる可能性もあるため、実行にあたっては十分に注意が必要です。


IPA Better Life with IT 情報処理推進機構

Microsoft Windows の脆弱性対策について(CVE-2015-2426)

最終更新日：2015年7月21日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

2015 年 7 月 21 日(日本時間)に Microsoft 製品に関する脆弱性 (CVE-2015-2426) の修正プログラムが 1 件公表されています。

Microsoft Windows にリモートからコードが実行される脆弱性が存在します。この脆弱性が悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御される可能性があります。

Microsoft 社は「悪用コードが作成されて攻撃者が安定的に脆弱性を悪用する可能性がある」と公表しており、攻撃が行われた場合の影響が大きいため、できるだけ早急に修正プログラム(MS15-078)を適用して下さい。

- サポートが終了したOS上でのWebやOffice文書等の閲覧を避けること、アンチウイルス・UTMの使用、そしてそれでもマルウェアに感染してしまうことを想定した様々な防御策が欠かせません。

●DDoS攻撃による国内初の逮捕者

http://www3.nhk.or.jp/news/html/20150724/k10010164501000.html
http://mainichi.jp/select/news/20150724k0000e040241000c.html

このニュースをザックリ言うと・・・

- 7月24日（日本時間）、警視庁サイバー犯罪対策課は、2月にWebサーバに対してDDoS攻撃を行ったことによる電子計算機損壊等業務妨害容疑で、ベトナム人留学生を逮捕したと発表しました。

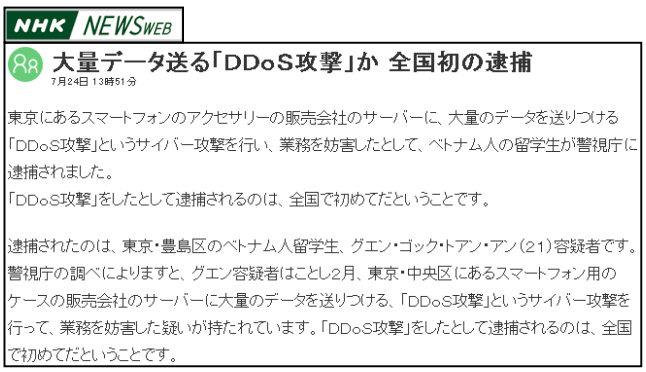
- 発表によれば、犯人は今月1日午後から同3日未明にかけて東京都中央区の携帯電話用品販売会社のサーバに1,000万回以上のアクセスを行うDDoS攻撃を仕掛け、サーバに通常の30倍の負荷をかけ、一時的にサイトを閉鎖に追い込むなど業務を妨害したとされています。

AUS便りからの所感等

- DDoS攻撃は、6月にもネットバンキングサイトに対して発生する等の事例が発表されています。

- Webサイトの閲覧によるもののみならず、メールサーバに対し大量のメールを送りつける、もしくはより高度な手段による攻撃もあり、サーバソフトウェアあるいはTCP/IPプロトコルの弱点を突いた、闇雲に負荷をかけない攻撃も存在します。

-自社ネットワークに公開サーバを設置している場合は、DDoS対策に特化した機器の導入またはUTMのDDoS対策機能の利用、レンタルサーバ・VPS上で公開しているサーバについては、CloudFlare等DDoS対策機能を提供するCDN（コンテンツデリバリネットワーク）の導入を検討することも良いでしょう。


NHK NEWSWEB

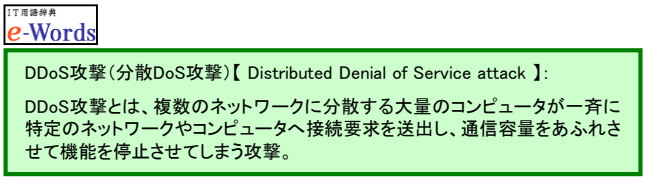
大量データ送る「DDoS攻撃」か 全国初の逮捕

7月24日 13時51分

東京にあるスマートフォンのアクセサリーの販売会社のサーバーに、大量のデータを送りつける「DDoS攻撃」というサイバー攻撃を行い、業務を妨害したとして、ベトナム人の留学生が警視庁に逮捕されました。

「DDoS攻撃」をしたとして逮捕されるのは、全国で初めてだということです。

逮捕されたのは、東京・豊島区のベトナム人留学生、グエン・ゴック・トアン・アン（21）容疑者です。警視庁の調べによりますと、グエン容疑者はことし2月、東京・中央区にあるスマートフォン用のケースの販売会社のサーバーに大量のデータを送りつける、「DDoS攻撃」というサイバー攻撃を行って、業務を妨害した疑いが持たれています。「DDoS攻撃」をしたとして逮捕されるのは、全国で初めてだということです。


IT用語辞典 e-Words

DDoS攻撃（分散DoS攻撃）【 Distributed Denial of Service attack 】:

DDoS攻撃とは、複数のネットワークに分散する大量のコンピュータが一斉に特定のネットワークやコンピュータへ接続要求を送出し、通信容量をあふれさせて機能を停止させてしまう攻撃。