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。

●広告配信ネットワークの乗っ取りによる攻撃、1日あたり12,500人が被害に

http://news.mynavi.jp/news/2015/05/21/607/
http://blog.trendmicro.co.jp/archives/11453

このニュースをザックリ言うと・・・

- 5月18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、米国のWeb広告配信ネットワーク「MadAdsMedia」が攻撃者に乗っ取られ、広告を閲覧したユーザが不正なサイトに誘導するよう仕向けられていたと発表しました。

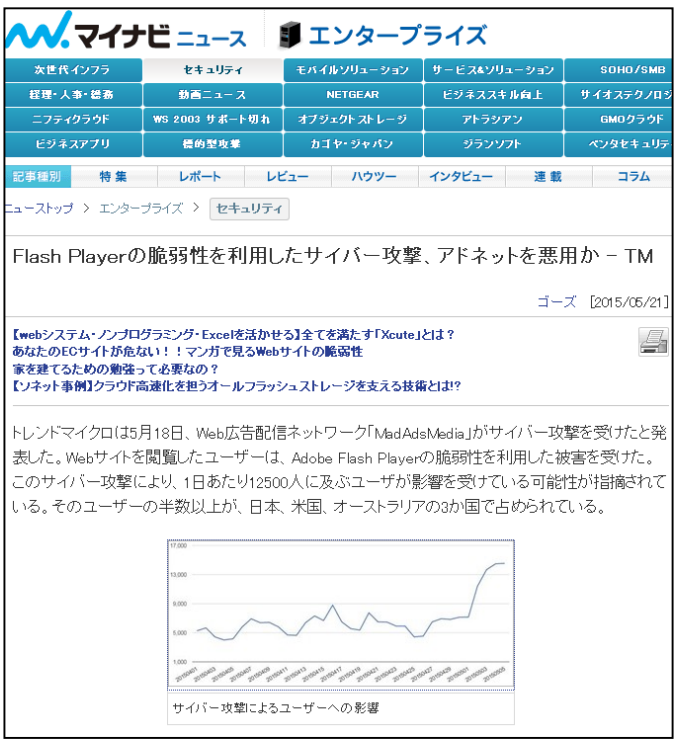
- 攻撃により、広告を表示するためのスクリプトを取得しようとする際、悪意のあるサイトへリダイレクトされ、Flash Playerに存在する脆弱性を攻撃されるよう仕向けられていた模様です。

- 5月2日には全世界で1日あたり12,500人のユーザが広告の閲覧によって被害を受けており、うち半数以上が日本・米国およびオーストラリアのユーザで占められていたとのことです。

AUS便りからの所感等

- 攻撃の対象となったFlash Playerの脆弱性は4月にリリースされた17.0.0.169で修正されていますが、また今月になって別の脆弱性を修正した17.0.0.188がリリースされていますので、根本的な対策のため、当該バージョンにアップデートされているか確認することを推奨致します。

- また、そういったアップデートが済んでいない状態での、マルウェアの読み込みや悪意のあるサイトへの誘導を抑止するため、ブラウザ自身およびそのアドオン、もしくはアンチウイルスやUTMによる防御を組合わせることも重要です。



2015年4月に初めて確認され、当初は比較的少ないトラフィック数だったが、5月に入り急増し、同月2日には 12,500人に及ぶユーザに影響

●大手ホームページサービスに不正アクセス、18万人分のFTPパスワード漏洩か

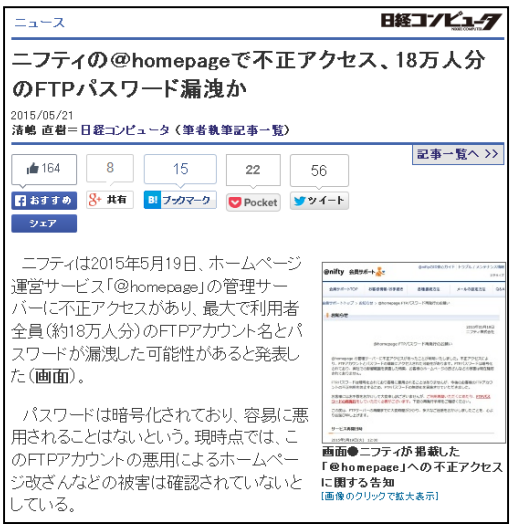
http://itpro.nikkeibp.co.jp/atcl/news/15/052101687/
http://support.nifty.com/cs/suptopics/detail/150519478420/1.htm

このニュースをザックリ言うと・・・

- 5月19日（日本時間）、@nifty を運営する大手ISPのニフティ社は、同社のホームページサービス「@homepage」が不正アクセスを受け、FTPアカウント情報が漏洩した可能性があると発表しました。

- 発表によれば、少なくとも5月11日頃からFTPアカウント情報への不正アクセスが行われていたとみられており、最大で利用者18万人全員についてアカウント情報にアクセスされた可能性があるとされています。

- 同社ではサーバ上のパスワードは暗号化されているとしていますが、現時点でのパスワードの無効化を行い、ユーザに対しパスワードの再設定を行うよう求めています。


ニュース　日経コンピュータ

ニフティの@homepageで不正アクセス、18万人分のFTPパスワード漏洩か

2015/05/21
清嶋 直樹＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

164　8　15　22　56
おすすめ　共有　ブックマーク　Pocket　ツイート
シェア

ニフティは2015年5月19日、ホームページ運営サービス「@homepage」の管理サーバーに不正アクセスがあり、最大で利用者全員（約18万人分）のFTPアカウント名とパスワードが漏洩した可能性があると発表した（画面）。

パスワードは暗号化されており、容易に悪用されることはないという。現時点では、このFTPアカウントの悪用によるホームページ改ざんなどの被害は確認されていないとしている。

画面●ニフティが掲載した「@homepage」への不正アクセスに関する告知
（画像のクリックで拡大表示）

AUS便りからの所感等

- 実際には可能性は低いようですが、万が一攻撃者にユーザのパスワードが奪取されていた場合、以前と同じパスワードを設定していたら当該サービスへ不正ログインされてしまうでしょうし、それ以上に、そのパスワードを使いまわしている他のサービスも連鎖的に被害を受ける恐れがあります。

- 近年度々報じられている大手サービスへの不正ログイン事件の教訓として、サービスごとに全く同じパスワードの使い回しをしていないか、この機会に確認することが重要です。

●仮想環境からホスト全体を乗っ取る脆弱性「VENOM」

http://japan.zdnet.com/article/35064485/
http://www.st.ryukoku.ac.jp/~kjm/security/memo/2015/05.html#20150514_VENOM

このニュースをザックリ言うと・・・

- 5月13日（現地時間）、米CrowdStrike社が複数のOS仮想化ソフトウェアに影響する脆弱性「VENOM」について発表しました。

- この脆弱性を悪用することにより、ゲスト(子)OS上の攻撃者がホスト(親)OS上で任意のコードを実行する等の攻撃を行うことが可能であり、ホストOSを丸ごと乗っ取られる恐れがあります。

- VENOMの影響を受けるソフトウェアとしてVirtualBox・XenおよびKVM等（※）が挙げられている他、こういった仮想化ソフトウェアを利用してVPSを提供している多くの業者にも影響が及んでおり、アップデートに伴い、各ユーザのVPSについて再起動を実施するところも出ています。

（※）一方でVMWareおよびHyper-V等は問題ないとされています。

AUS便りからの所感等

- 今日では、コスト削減やセキュリティ確保等の様々な目的から、一つのホストPC内に複数のゲストOSを立ち上げて運用するケースは珍しくなくなってきていますが、今回発表されたVENOMは「仮想化によってOSが分離されている」「ゲストOSから直接ホストOSにはアクセスできない」という前提を破りかねないもので、ホストOSはもちろん、そこにぶら下がっている別のゲストOSへの侵入にもつながることから、大きく騒がれています。

- 特に外部公開のサーバを仮想化によるゲストOSで運用している場面等で、万が一の侵入からホストOSへのセキュリティ侵害に繋がることがないよう、使用している仮想化ソフトウェア等が影響を受けないか確認、適宜アップデートを行うことが求められます。

- この他、そもそものサーバOS上への侵入の可能性を抑止するためのUTMの導入は必須ですし、クライアントPC上で仮想化されたゲストOSを実行しているケースについて、可能な限りアンチウイルスの導入・ファイアウォールの設定を検討することもまた重要です。