— ＡＵＳ（アルテミス・ユーザ・サポート）便り 2014/10/27号 —

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。

●身代金要求マルウェアに感染させる不正広告、日本含む大手サイトに

http://www.itmedia.co.jp/enterprise/articles/1410/24/news052.html
http://www.proofpoint.com/threatinsight/posts/malware-in-ad-networks-infects-visitors-and-jeopardizes-brands.php

このニュースをザックリ言うと・・・

- 10月22日（現地時間）、米国のセキュリティ企業Proofpoint社は、大手サイトにおいて表示するだけでマルウェア「CryptoWall」に感染するような悪意のある広告が配信されていた、と同社ブログで発表しました。

- CryptoWallには、感染したPC上のファイルを強制的に暗号化し、「元に戻すために金銭を要求する」という特徴があります。

- 当該広告は、Yahoo!等の米国の大手サイトの他、日本のWebサイトでも配信された所があるとのことです。

AUS便りからの所感等

- CryptoWallのような、PC上のファイルを「人質」として金銭を要求するマルウェアは「ランサムウェア」と呼ばれますが、ひとたび感染すればデータが事実上破壊されるとみてよいでしょう。

- CryptoWallは他のマルウェアと同様、アンチウイルスベンダにより多数の亜種が確認されており、感染防止のためのクライアント側の各種ソフトウェア（OS・Flash PlayerおよびJava等）のアップデートと共に、今後も現れ得る新種への対応としてアンチウイルス・UTMによる防御は必須と言えるでしょう。


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 ＞ ニュース ＞ 身代金要求マルウェアに感染させる不正広告、日本含 ...

2014年10月24日 07時35分 更新

身代金要求マルウェアに感染させる不正広告、日本含む大手サイトに

ユーザーは問題の広告を表示しただけでマルウェアに感染する恐れがある。不正な広告が表示された中には日本のWebサイトも含まれるという。

[鈴木聖子, ITmedia]

印刷／PDF | ツイート 123 | いいね！ 41 | チェック | 0 | Pocket 15 | 通知

PR 情報漏洩対策と標的型攻撃対策の「オイシイ関係」【 G-2 】
PR "安全な最短ルート"で実現する最新サーバー移行手法とは？

米Yahoo!など各国の大手サイトに不正な広告を配信し、ユーザーのHDDを人質にして身代金を脅し取るランサムウェア「CryptoWall 2.0」に感染させる攻撃が発生していたとして、セキュリティ企業Proofpointが10月22日のブログで詳細を伝えた。不正な広告が表示された中には日本のWebサイトも含まれるという。

米セキュリティ機関のUS-CERTも同日、ランサムウェアに関する情報を公開して注意を呼び掛けていた。

Proofpointによると、今回の攻撃ではインターネットの広告ネットワークを利用して正規サイトに表示される広告に不正なコードが仕込まれていた。

問題の広告はAdobe Flashを使って密かに攻撃コードを呼び込み、脆弱性を突いてユーザーのコンピュータにCryptoWall 2.0を感染させる仕組みで、ユーザーが問題の広告を表示しただけで感染する恐れがある。

不正広告の一例
（Proofpointより）

●UPnP対応機器を踏み台としたリフレクター攻撃が増加、警察庁が注意喚起

http://internet.watch.impress.co.jp/docs/news/20141020_672198.html
http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf

このニュースをザックリ言うと・・・

- 10月17日、警察庁より、UPnP（Universal Plug and Play）に対応したネットワーク機器を踏み台とした「SSDP（Simple Service Discovery Protocol）リフレクター攻撃」が9月上旬以降増加していると注意喚起がありました。

- 攻撃内容としては、UPnPで使用されるSSDPが使用するUDPポート1900番に対し発信元IPアドレスを偽装したパケットを大量に送信し、反応があった多数のネットワーク機器から、返信パケットを偽装した発信元へ集中させるというものです。


INTERNET Watch

ニュース

UPnP対応機器を踏み台としたリフレクター攻撃が増加、警察庁が注意喚起

(2014/10/20 18:42)

警察庁は17日、UPnPに対応したネットワーク機器を踏み台とした「SSDPリフレクター攻撃」が確認されているとして、注意を喚起した。

この攻撃は、UPnPで使用されるプロトコルのSSDPを悪用して、発信元を偽装することで応答パケットを攻撃対象に送信するもの。送信したパケットに対して応答パケットの方が大きくなるため、大量のパケットを攻撃対象に送りつけるDoS攻撃などに用いられる。

警察庁の定点観測システムでは、SSDPが使用するUDP 1900番ポートに対して、機器情報の送信を要求する「M-SEARCH」メッセージの送信が、9月上旬ごろから増加していることを確認。攻撃者が、SSPDリフレクター攻撃の踏み台となるネットワーク機器を探索していると考えられるとしている。

図1 攻撃の踏み台とするネットワーク機器の探索

攻撃の踏み台とするネットワーク機器の探索

AUS便りからの所感等

- SSDPのようなUDPベースのプロトコルについては、既にDNSやNTPにおいてサービスを悪用したDDoS攻撃の存在が知られています。

- 上記のサービスを含め、外部からアクセスされるべきでないサービスは設定により無効化、あるいはフィルタリングすることが重要であり、さらにファイアウォール・UTMの設置によるアクセス遮断を行うといった対策が望まれます。

●Windowsに未対策の脆弱性、PowerPointによる攻撃発生

http://www.itmedia.co.jp/enterprise/articles/1410/22/news085.html
https://www.jpcert.or.jp/at/2014/at140043.html

このニュースをザックリ言うと・・・

- 10月22日（日本時間）、マイクロソフト社は、Windowsの各バージョンにおいてパッチがリリースされていない脆弱性が存在し、それを突いた攻撃が確認されていることを発表しました。

- 細工されたOfficeファイルを開くことにより、PCがマルウェアに感染する等の可能性があり、既に不正なPowerPointファイル（.pptx/.ppsx）を開かせてPCを乗っ取ろうとする標的型攻撃が確認されているとのことです。


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 ＞ ニュース ＞ Microsoft OLEにゼロデイ脆弱性、PowerPoint悪用の...

2014年10月22日 14時13分 更新

Microsoft OLEにゼロデイ脆弱性、PowerPoint悪用の標的型攻撃も

Windows Server 2003を除く現在サポートされている全てのWindowsに影響するといい、限定的な標的型攻撃も発生している。

[ITmedia]

印刷／PDF ツイート 53 いいね！ 48 チェック 6 Pocket 13 通知

cybozu.com カンファレンス 2014 東京／大阪で開催！
"安全な最短ルート"で実現する最新サーバー移行手法とは？

Microsoftは10月22日、Microsoft OLEに未修正の脆弱性が見つかったとしてセキュリティアドバイザリーを公開した。Windows Server 2003を除く現在サポートされている全てのWindowsに影響する。

この脆弱性はMicrosoft OLEに起因し、リモートから任意のコードを実行できてしまう。攻撃ではメールやメッセンジャーなどのリンクや添付からユーザーに細工したOfficeファイルなどを開かせ、脆弱性を突いて任意コード実行を可能にするという。実際にPowerPointを使って脆弱性を突く限定的な標的型攻撃が発生している。

マイクロソフト セキュリティ アドバイザリ 3010060

Microsoft OLE の脆弱性により、リモートでコードが実行される

概説

AUS便りからの所感等

- 今月マイクロソフトから公開されたセキュリティ情報の一つ「MS14-060」と似通っていますが、これに対するパッチで修正されなかった別の脆弱性であり、現時点でパッチを全て適用したからと言って、決して油断してはいけません。

- パッチがリリースされる前に脆弱性を突く攻撃（ゼロデイ攻撃）が流行することは決して珍しいことではありませんので、今後もこういったケースへの対応のために、アンチウイルス・UTMによる防御は有効となるでしょう。