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。

●2015年、脆弱性を最も悪用されたソフトウェアは「Adobe Flash Player」

http://news.mynavi.jp/news/2016/03/16/152/
http://blog.trendmicro.co.jp/archives/13017

このニュースをザックリ言うと･･･

- 3月15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より、エクスプロイトキット（さまざまな脆弱性を攻撃するためのパッケージ化されたプログラム）の2015年を通した分析が同社のセキュリティブログにて公開されました。

- 2015年に新たにターゲットとされた脆弱点18件のうち実に15件がFlash Playerの脆弱点を狙ったものとなっていたとのことで、残り2件はInternet Explorer（IE）、1件はSilverlight（Flashと同様にWebサイト上のコンテンツに用いられる技術）に対するものでした。

- また、ユーザに対してエクスプロイトキットによる攻撃へと誘導する手法としては、「Web改ざん」と「不正広告」が多く用いられていたとのことです。

- 前者に関しては1500近くのWebサイトが改ざんされ、後者に関しては多くのWebサイトで利用されるアドネットワークに対し攻撃者が自ら不正な広告を出稿するパターンを用いていたとのことで、特に2015年12月にはエクスプロイトキットによる攻撃の88%が不正広告経由によるものだったとされています。

AUS便りからの所感等

- Flash Playerは概ねマイクロソフトのセキュリティ情報発表と同じタイミングでセキュリティアップデートがリリースされていますので、自動更新機能が有効になっており、最新バージョンにアップデートされているか、必ず確認を行うようにしてください。

- 「Web改ざん」および「不正広告」はいずれも、自社のサイト・他のサイトの区別なく注意が必要で、自社サイトを改ざんしようとする攻撃に対する防御、内部から他のサイトへのアクセス時のアクセス先からの攻撃に対する防御、いずれにおいてもアンチウイルスやUTM、その他による対策は可能な限り行うべきです。

マイナビニュース

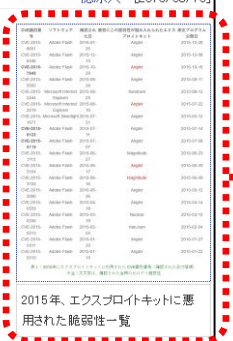
2015年、脆弱性を最も悪用されたソフトウェアは「Adobe Flash Player」

徳原大　[2016/03/16]

トレンドマイクロは3月15日、エクスプロイトキット(さまざまな脆弱性を攻撃するためのパッケージ化されたプログラム)の2015年を通した分析を、同社のセキュリティブログで公開した。

これによると、2015年に公開され、エクスプロイトキットに利用された18件の脆弱性のうち、15件はエクスプロイトキットに悪用される前に修正プログラムが公開されていた。ただ、3件は"ゼロデイ脆弱性"として修正プログラムが提供される前にエクスプロイトキットに組み込まれていた。

その多くはAdobe Flash Playerを対象としており、18件中15件がFlash Player、2件がMicrosoft Internet Explorer、1件がMicrosoft Silverlightだった。これらの脆弱性の半数以上で、最初に対応したエクスプロイトキットは「Angler Exploit Kit(Angler EK)」となっていた。Angler EKは2015年に最も猛威をふるったエクスプロイトキットといわれており、SymantecやESETの調査結果でも同様の傾向が見られる。



2015年、エクスプロイトキットに悪用された脆弱性一覧

TREND MICRO トレンドマイクロ セキュリティブログ

CVE識別番号	ソフトウェア	確認された日	最初にこの脆弱性が組み入れられたエクスプロイトキット	修正プログラム公開日
CVE-2015-8651	Adobe Flash	2016-01-26	Angler	2015-12-28
CVE-2015-8446	Adobe Flash	2015-12-15	Angler	2015-12-08
CVE-2015-7645	Adobe Flash	2015-10-29	Angler	2015-10-16
CVE-2015-5560	Adobe Flash	2015-08-28	Angler	2015-08-11
CVE-2015-2444	Microsoft Internet Explorer	2015-08-25	Sundown	2015-08-12
CVE-2015-2419	Microsoft Internet Explorer	2015-08-10	Angler	2015-07-22
CVE-2015-1671	Microsoft Silverlight	2015-07-21	Angler	2015-05-12
CVE-2015-5122	Adobe Flash	2015-07-11	Angler	2015-07-14
CVE-2015-5119	Adobe Flash	2015-07-07	Angler	2015-07-08
CVE-2015-3113	Adobe Flash	2015-06-27	Magnitude	2015-06-23
CVE-2015-3104	Adobe Flash	2015-06-17	Angler	2015-06-09
CVE-2015-3105	Adobe Flash	2015-06-16	Magnitude	2015-06-09
CVE-2015-3090	Adobe Flash	2015-05-26	Angler	2015-05-12
CVE-2015-0359	Adobe Flash	2015-04-18	Angler	2015-04-14
CVE-2015-0336	Adobe Flash	2015-03-19	Nuclear	2015-03-12
CVE-2015-0313	Adobe Flash	2015-02-02	HanJuan	2015-02-04
CVE-2015-0311	Adobe Flash	2015-01-20	Angler	2015-01-27
CVE-2015-0310	Adobe Flash	2015-01-15	Angler	2015-01-22

表1：2015年にエクスプロイトキットに利用された CVE識別番号（確認された日付降順）
※注：太文字は、確認された当時のゼロデイ脆弱性

●Mac OS X初の「完全体」なランサムウェア出現

http://internet.watch.impress.co.jp/docs/news/20160307_747119.html

このニュースをザックリ言うと・・・

- 3月6日（米国時間）、大手セキュリティベンダーの米Palo Alto Networks社より、OS X（Mac）で初めての「完全体」なランサムウェア（感染したPCのファイルを人質に金銭等を要求するマルウェア）を確認したとして警告が発表されました。

- 「KeRanger」と名付けられたランサムウェアは、BitTorrent（P2Pファイル共有）用クライアント「Transmission」のインストーラーにRTF（文書ファイル）形式に偽装した形で混入していたもので、インストールから3日後に指令サーバにアクセスし、文書・画像・オーディオデータ等の暗号化を実行後、約400ドルをビットコイン（暗号通貨）で支払うよう脅迫する文書を指令サーバからダウンロードする仕組みになっているとのことです。

- KeRangerはまだ発展途上とされており、「Time Machine（OS Xを以前の状態に戻すためのバックアップ機能）」のデータをも暗号化する機能を開発中の痕跡も確認された模様です。


INTERNET Watch

Mac OS X初の"完全体"なランサムウェア出現、「Time Machine」も暗号化するよう開発中か

(2016/3/7 19:11)

G+1 13 B! 27 ツイート リスト いいね！ シェア 182 Pocket 48

オープンソースプロジェクトであるMac用BitTorrentクライアント「Transmission」のインストーラーに、新種のランサムウェア「KeRanger」が混入していたことを、米Palo Alto Networksが報告した。同社によれば、Mac OS Xで初の"完全体"なランサムウェアだという。

「Transmission」の公式サイト

AUS便りからの所感等

- Macに感染するマルウェアも段々珍しいものではなくなってきていますが、Windowsのような事例の蓄積が乏しく、OS搭載のセキュリティ機能も突破されたということもあり、今後の動向が注目されるところです。

- インストーラーが正規のものか、可能な限り何らかの確認手段をとるよう努め、併せてアンチウイルスやUTMの導入による防御と組合わせることは、WindowsでもOS Xでも大切なことです。

●国内WebサイトでSQLインジェクションの脆弱性・・・中小企業や個人も対象に

http://news.mynavi.jp/news/2016/03/16/135/

このニュースをザックリ言うと・・・

- 3月15日（日本時間）、セキュリティ専門機関JPCERT/CCより、国内のWebサイトにおいてSQLインジェクションの脆弱性が存在していると国内外から多く報告を受けたとして、注意が発表されました。

- 悪意ある第三者によりSQLインジェクション攻撃が行われた場合、認証回避や任意のプログラム実行、情報漏えい、ウェブサイトの改ざんなど、深刻な影響を受ける可能性があるとして警告しています。

- JPCERT/CCによれば、既にオープンソースのSQLインジェクション診断ツール「sqlmap」によるとみられる国内のWebサイトへの海外からのアクセスが確認されており、こういったアクセスは組織規模の大小を問わず、企業から個人のWebサイトにまで行われているとのことです。

マイナビニュース

国内WebサイトでSQLインジェクションの脆弱性 － 中小企業や個人も対象に

徳原大 [2016/03/16]

JPCERTコーディネーションセンター(JPCERT/CC)は3月16日、国内外から複数の報告が寄せられたとして、国内のWebサイトにSQLインジェクションの脆弱性が存在するとして注意喚起を行った。

JPCERT/CCによると、オープンソースのSQLインジェクション脆弱性診断ツール「sqlmap」を利用し、国内のWebサイトで動作するWebアプリケーションを対象としたSQLインジェクションの脆弱性を検出しようとするアクセスが海外から行われているという。このアクセスは、組織規模の大小を問わず、中小企業や個人のWebサイトでも行われているため、注意が必要としている。

AUS便りからの所感等

- 「SQLインジェクション」とは、内部のデータベースサーバにアクセスするWebアプリケーションの脆弱性を突き、データベースサーバへ送信するSQLコマンドに任意の不正なコマンドを挿入する攻撃方法です。

- 多少技術的な説明になりますが、SQLインジェクションを防ぎ、安全にSQLコマンドを実行するには、SQL文のテンプレートとなる文字列とパラメータの組を安全に処理する「静的プレースホルダ（バインド機構、プリペアード･ステートメント）」を用いることが重要です。

- SQLインジェクション等を狙う不正なアクセスを遮断するために、サーバやUTMにおいてWAF（Webアプリケーションファイアウォール）を設置することはある程度の効果が見込めるとは言え、様々な脆弱性の根本的な対策のため、Webアプリケーション診断を受けることを推奨致します。