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。

●脆弱性攻撃サイトへの誘導経路の9割が「不正広告」と「Web改ざん」経由･･･トレンドマイクロ

http://japan.cnet.com/news/service/35073756/
http://blog.trendmicro.co.jp/archives/12591

このニュースをザックリ言うと･･･

- 11月19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、2015年第3四半期（7～9月）における国内外の脅威動向についての分析結果が発表されました。

- 同社の調査によれば、マルウェア感染等を目的とする「脆弱性攻撃サイト」への誘導経路の実に9割が「不正広告」と「Web改ざん」を合わせた「正規サイト汚染」経由、即ち正規サイトにアクセスしてきたユーザを攻撃サイトへリダイレクトさせるケースとなってます。

- また、脆弱性攻撃のために使用される「エクスプロイトキット(※)」についても新たな脆弱性の利用が迅速化しており、7月に発覚したFlash Playerの脆弱性等にパッチがリリースされる1～3日前に対応し、ゼロデイ攻撃に悪用していたことを一例として挙げています。

- これらの「脅威連鎖」は金銭の詐取を主な目的としており、マルウェアの85%がオンラインバンキングをターゲットとした詐欺ツールとランサムウェア(※)で占められていたとのことです。

AUS便りからの所感等

- 「怪しいサイトにはアクセスしない」のようなユーザ側での注意は全く無意味というわけではありませんが、それだけに依存してマルウェア感染から回避することはもはや不可能であると改めて認識し、多重の対策によって個々の対策を補完することが重要です。

- PCへのアンチウイルスの導入、各種ソフトウェアのアップデート、ブラウザのセキュリティ機能や実績のあるアドオンのインストール、そしてUTMの導入は、いずれも正規サイトの中で牙をむく攻撃からの防御に役立つものであり、またこれらもいずれか一つに依存しないことがマルウェア感染の可能性を限りなく軽減させるために必要でしょう。

CNET Japan

脆弱性攻撃サイトへの誘導経路の9割が「不正広告」と「Web改ざん」経由--トレンドマイクロ

飯塚 直　2015/11/19 13:32

トレンドマイクロは11月19日、2015年第3四半期（7～9月）における国内外の脅威動向についての分析を発表した。それによると、「脅威連鎖」の中心的存在である「脆弱性攻撃サイト」への誘導経路のおよそ9割が「不正広告」と「Web改ざん」を合わせた正規サイト汚染経由であるという。

不正広告による攻撃の概念図

eset ENJOY SAFER TECHNOLOGY　マルウェア情報局

（※）エクスプロイト　英語表記:Exploit

ソフトウェアの脆弱性を暴く行為、またはそのための検証コード。ソフトウェアの脆弱性を発見した場合、実際に悪用が可能であることを実証するため、実際に想定される攻撃を実装した簡単な検証コードが公開されることがある。

その目的は、実際に攻撃するコードを示すことで脆弱性のリスクや影響を明確にし、注意を喚起することである。このようなコードを「エクスプロイトコード」と呼ぶ。この場合のエクスプロイトコードには、攻撃が可能なことを示す部分のコードだけが実装され、実際に攻撃を完結させて破壊や犯罪行為を成立させてしまう部分までは実装されていないことが多い。

現在では、悪意を持ったプログラムコードそのものを「エクスプロイト（コード）」と呼ぶことも増えている。特に「エクスプロイトキット」といった場合、攻撃者が配布、販売する、さまざまな脆弱性を攻撃するコードモジュール群（パッケージ）のことを意味する。エクスプロイトキットは闇市場（アンダーグラウンドマーケット）などで流通しており、プログラムなど専門的な知識がなくても利用できるようユーザーインタフェースを備えていたり、高度な機能を持ったソフトウェアであることもある。

IT用語辞典 e-Words

（※）ランサムウェア【 ransomware 】身代金型ウイルス

ランサムウェアとは、「トロイの木馬」型のコンピュータウイルスの一種で、感染したコンピュータが正常に利用できないよう「人質」に取り、復元のために代価の支払いを要求するソフトウェア。“ransom”は「身代金」の意。

ランサムウェアがコンピュータに感染すると、パスワードを入力しないと利用できないようコンピュータをロックしたり、ファイルを暗号化して読み取れないようにしてしまう。そして、犯人に「身代金」を支払えば復元する旨のメッセージが現れる。従来のウイルスは単に感染を広げたり、コンピュータ内部のファイルを無差別に破壊するなど、愉快犯的な動機によると思われるものが多かったが、ウイルスによって金銭的な利益を上げようとする新しいタイプのウイルスとして広がっている。

●高度サイバー攻撃への対処におけるログ活用と分析方法を公開

http://www.jpcert.or.jp/research/apt-loganalysis.html

このニュースをザックリ言うと・・・

- 11月17日（日本時間）、セキュリティ専門機関JPCERT/CCより、「高度サイバー攻撃への対処におけるログの活用と分析方法」と題した文書が公開されました。

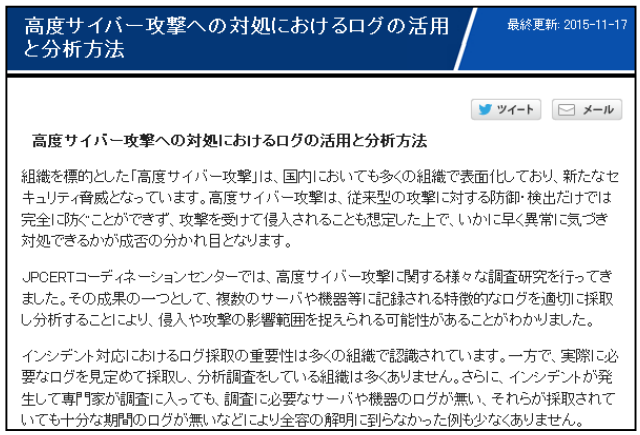
- JPCERT/CCでは、従来型の攻撃に対する防御・検出だけでは完全に防ぐことができない「高度サイバー攻撃」に対し、攻撃を受けて侵入されることも想定した上で、いかに早く異常に気づき対処できるかが成否の分かれ目であるとしています。

- 高度サイバー攻撃に関する様々な調査研究の成果の一つとして、複数のサーバや機器等に記録される特徴的なログを適切に採取し分析することにより、侵入や攻撃の影響範囲を捉えられる可能性があるとして、一般的に利用される機器に、攻撃者の活動の痕跡をログとして残すための考え方、それらのログから痕跡を見つけ出す方法などをこの文書に記載しています。

AUS便りからの所感等

- 取得可能な場面で可能な限りログを取得すること、一方でそれによって膨大な量となるであろうログデータを的確に分析すること、いずれも攻撃や侵入を速やかに検知するためには重要なものとなります。

- 当文書をもとに、各種サーバにおいて確実にログを取得しているかの確認を行うとともに、UTMの設置により、特に外部への通信のログ取得に役立てることを強く推奨します。



●88%のネットワークが特権アカウントの乗っ取りに弱い状況

http://news.mynavi.jp/news/2015/11/16/143/

このニュースをザックリ言うと・・・

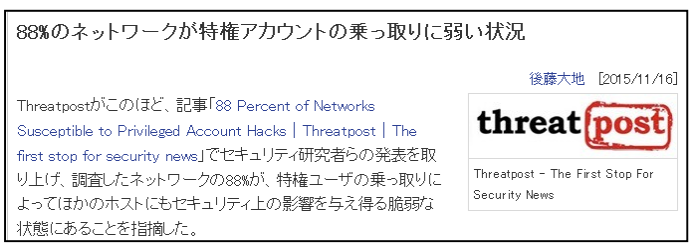
- 11月10日（現地時間）、セキュリティブログ「Threatpost」において、セキュリティ研究者が調査したネットワークの88%が「管理者等の特権を持つユーザアカウント」の乗っ取りによって重大な影響を及ぼす可能性があるような脆弱なネットワークである、とする記事が発表されました。

- こういったネットワークにおいては、特定の担当者に割り当てられた特権アカウントが乗っ取られたり盗まれたりした場合、対象となるホストのみならず、そのホストが所属しているネットワークの他のホストにも危険性が及ぶ恐れがあるとしています。

- また、こうしたリスクを防ぐには、ファイアウォールやセキュリティ・ソフトウェアなどの導入のみでは不十分であり、適宜ネットワークを分割し、必要なユーザが必要なネットワークに必要な権限のみでアクセスできるようにすることを薦めています。

AUS便りからの所感等

- 今年多くの組織で発生した個人情報流出事件の中には、組織内ネットワークが分離されていないことが原因で、本来個人情報へのアクセスを想定していない箇所からアクセスされたケースも多々ありました。



- また、管理者のパスワードを各サーバで統一しているような場合、万が一あるサーバの管理者パスワードが漏洩してしまうと、そこからアクセス可能なあらゆるサーバを乗っ取られることにつながり得ます。

- 侵入されてしまう可能性、あるいは管理者権限を乗っ取られてしまう可能性をも考慮し、全体への被害を最小限に抑えるためのネットワーク構成・サーバ等管理ポリシーの見直し等が決して欠かしてはいけないものとなるでしょう。