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。

●クラッカーによるネットサービスのドメインハイジャック、利用していたWebサイトが被害に

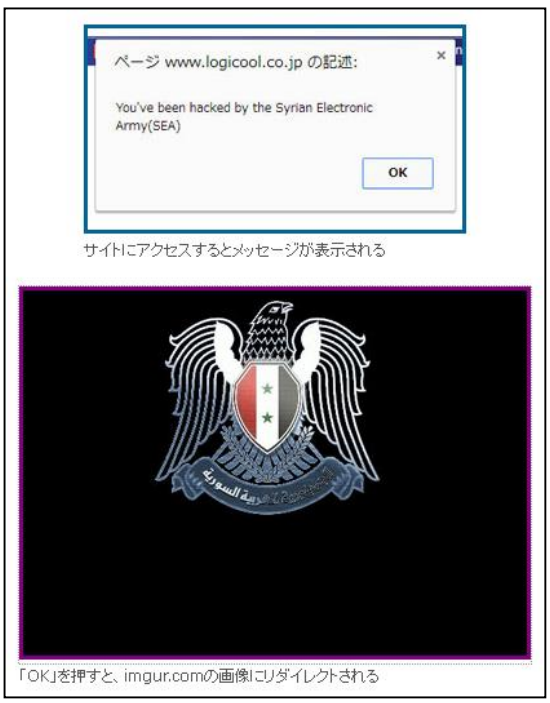
http://www.itmedia.co.jp/news/articles/1411/28/news057.html
http://japan.cnet.com/news/business/35057159/

このニュースをザックリ言うと・・・

- 11月27日（現地時間）、世界中の大手メディア・企業のWebサイトにおいて、クラッカー集団「シリア電子軍（SEA）」のロゴマークがポップアップ表示されるという現象が発生しました。
- これらのWebサイトでは、サイトのソーシャル化プラットフォーム「gigya」を利用していましたが、gigyaのドメインがSEAにハイジャックされたことが今回の攻撃が発生した原因であることが明らかになっています。
- 海外においてはCNBC・Guardian等の大手メディアが、国内においても毎日新聞・So-net等が被害を受けています。

AUS便りからの所感等

- 今回の攻撃では、多くのサイトが利用するサービスに対するドメインハイジャックが行われたことから、直接攻撃を受けたわけでない利用サイトの運営が気付かないまま、間接的に大規模なクラッキングを行うことができたと見られます。
- サイトを運営する側にとってはサーバへの攻撃のみならず、閲覧するユーザの立場に立って、サイト上で利用しているサービスの乗っ取り等による不審な兆候が発生していないか監視を行うことが重要となるでしょう。
- ユーザ側での対策としては、ドメインハイジャックそのものの検知が困難であるため、攻撃者の誘導によるマルウェアのダウンロード等を食い止めるためにもUTMやアンチウイルスによる防御が肝要です。



サイトにアクセスするとメッセージが表示される

「OK」を押すと、imgur.comの画像にリダイレクトされる

●SNMP悪用攻撃か、警察庁が「踏み台対策」を呼び掛け

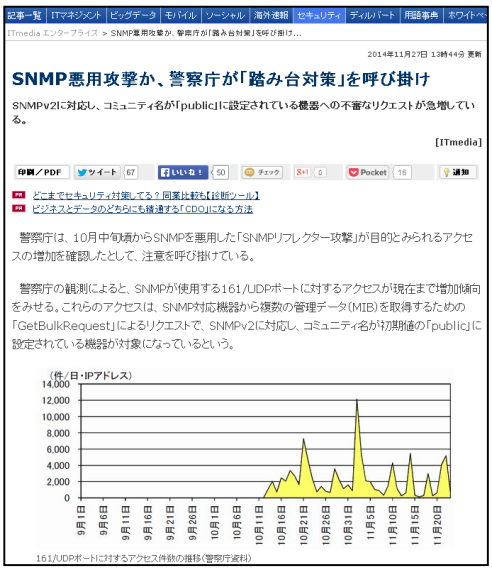
http://www.itmedia.co.jp/enterprise/articles/1411/27/news092.html
http://www.npa.go.jp/cyberpolice/detect/pdf/20141126.pdf

このニュースをザックリ言うと・・・

- 11月26日、警察庁がSNMP（Simple Network Management Protocol）を悪用したSNMPリフレクター攻撃を企図するアクセスの増加を確認したとして注意を呼びかけています。

- 発表によれば、10月中旬から、SNMPサービスポート（UDP 161番）への外部からのアクセス増加が確認され、最大で1日に12,000件のアクセスを観測したとのことです。

- 警察庁では、この攻撃への対策として、
「該当ポートへのパケットをファイアウォールでフィルタリングする」
「不要なサービスは停止する」
「コミュニティ名（SNMPサービスにアクセスするためのID）として、初期値に設定されている”public”は避ける」等を呼びかけています。


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 > SNMP悪用攻撃か、警察庁が「踏み台対策」を呼び掛け...

2014年11月27日 13時44分 更新

SNMP悪用攻撃か、警察庁が「踏み台対策」を呼び掛け

SNMPv2に対応し、コミュニティ名が「public」に設定されている機器への不審なリクエストが急増している。

[ITmedia]

印刷／PDF ツイート 67 いいね！ 50 チェック 8+1 0 Pocket 16 通知

どこまでセキュリティ対策してる？同業比較も【診断ツール】
ビジネスとデータのどちらにも精通する「CDO」になる方法

警察庁は、10月中旬頃からSNMPを悪用した「SNMPリフレクター攻撃」が目的とみられるアクセスの増加を確認したとして、注意を呼び掛けている。

警察庁の観測によると、SNMPが使用する161/UDPポートに対するアクセスが現在まで増加傾向をみせる。これらのアクセスは、SNMP対応機器から複数の管理データ（MIB）を取得するための「GetBulkRequest」によるリクエストで、SNMPv2に対応し、コミュニティ名が初期値の「public」に設定されている機器が対象になっているという。

161/UDPポートに対するアクセス件数の推移（警察庁資料）

AUS便りからの所感等

- UDPベースのサービスを狙うリフレクター攻撃は、少し前にもDNSやNTPに対するものが話題になっていました。

- SNMPはネットワーク上の機器管理等に用いられるサービスであり、複合機等は必ずと言っていいほどSNMPに対応していますが、一方で、攻撃者から機器の構成情報を奪取する目的で狙われることもあります。

- 不要なサービスを停止すること、外部に公開する必要のないサービスをフィルタリングすることはセキュリティの鉄則であり、特に後者を実現する方法としてUTMの設置は効果的です。

●USBタバコからマルウェア感染の可能性

http://gigazine.net/news/20141126-chinese-e-cigarette-malware/
http://www.theguardian.com/technology/2014/nov/21/e-cigarettes-malware-computers

このニュースをザックリ言うと・・・

- 11月21日（現地時間）、イギリスの新聞「The Guardian」が中国製のリキッド式電子タバコからマルウェアに感染したとされる事例を報じています。

- 記事では、「OS・アンチウイルスソフト等が最新版にアップグレードされていた」かつ「インターネットへのアクセスログについても不審な点はなかった」にも拘らずマルウェアに感染したPCについて、何らかのデバイスをUSB接続したことがないか確認したところ、電子タバコを給電のためUSBケーブルで接続しており、その電子タバコを調査した結果、PCへの接続によりマルウェアが侵入するよう仕組まれていた模様です。

AUS便りからの所感等

- USB接続によってデータを転送するUSBメモリやメディアプレイヤー等からマルウェアが感染したという事例はこれまでも見られましたが、一見そういったストレージ機能やネットワーク機能を持たず、USB接続を充電用途にのみ用いているように見える機器から感染するという、警戒心を薄める意味では効果的な攻撃方法であったと言えます。


2014年11月26日 09時00分50秒

中国製の電子タバコにマルウェアが仕組まれていた可能性

By Florian F. (Flowtography)

さまざまな味のフレーバーを楽しめる上に、禁煙を手助けしてくれる「リキッド式電子タバコ」は海外で人気が上昇し、日本でも使用する人が増えているようです。電子タバコは専用のUSBケーブルで充電するタイプがほとんどなのですが、マルウェアに感染したPCの感染経路を調べたところ、電子タバコからUSBケーブル経由で感染した可能性が指摘されました。

- ネットワークを全く介さない攻撃であることも鑑みると、現時点でユーザ側がとれる対策としては、「最低でもOS・アプリケーション・セキュリティソフトを最新に保つ」「海外製の名の知られていないメーカーの機器を避ける」「安易に機器をUSB接続しないよう物理的に制限する」等が挙げられますが、今後OS側でこういった問題に対するセキュリティ面での新たな対応がとられることを期待したいものです。