

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。

速報 | STUD/O | ベンチャー人 | 製品動向 | ネットの話題 | 社会とIT | セキュリティ | 企業・業界動向 | ブログ | 中堅・中小 | 過去話

ITmedia ニュース > 社会とIT > 国内大手サイトでハッキング？報告相次ぐ「シリア電子軍」が世界的に影響

2014年11月28日 01時11分 更新

国内大手サイトでハッキング？報告相次ぐ「シリア電子軍」が世界的に影響

毎日新聞など国内の複数の大手企業サイトで11月27日夜、アクセスすると「シリア電子軍」のものと思われる画像に飛ばされるとの報告が相次いだ。海外の大手報道機関サイトでも同様の報告がある。

[ITmedia]

印刷/PDF | ツイート | 621 | いいね! | 206 | チェック | 8+1 | 20 | Pocket | 90 | 通知

ビジネスとデータのどちらにも精通する「CDO」になる方法
うちの情シスは結構強？ 1%の容疑が乗り出す謎の物語

国内の複数の大手企業サイトで11月27日夜、アクセスすると「シリア電子軍」(Syrian Electronic Army)のものと思われる画像に飛ばされるとの報告が相次いだ。世界各国の大手報道機関サイトでも同様の報告があり、シリア電子軍を名乗るTwitterアカウントが犯行声明と見られる投稿をツイートしているが、関連は不明だ。

追記
その後、各社が採用しているサービスのWHOIS情報が何者かに書き換えられたことが原因と判明。⇒[詳細記事](#)

Twitterなどでは27日夜、毎日新聞やSo-net、ロジクールなどのサイトにアクセスすると「シリア電子軍にハッキングされた」というポップアップメッセージが表示され、「OK」を押すとシリア電子軍のマークと思われる画像が表示されるとの報告が相次いだ。ITmedia編集部でもこのうち1つのサイトで報告通りのことが起きるのを確認した。

ページ www.logicool.co.jp の記述:

You've been hacked by the Syrian Electronic Army(SEA)

OK

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。
- 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。

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。

記事一覧 | ITマシントピ | ビジネス | モバイル | ソーシャル | 海外速報 | セキュリティ | デバイス | 用語集 | ネットワーク

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。

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(観測予定値)

日	アクセス件数 (推定)
9月8日	0
9月9日	0
9月10日	0
9月11日	0
9月12日	0
9月13日	0
9月14日	0
9月15日	0
9月16日	0
9月17日	0
9月18日	0
9月19日	0
9月20日	0
9月21日	0
9月22日	0
9月23日	0
9月24日	0
9月25日	0
9月26日	0
9月27日	0
9月28日	0
9月29日	0
9月30日	0
10月1日	0
10月2日	0
10月3日	0
10月4日	0
10月5日	0
10月6日	0
10月7日	0
10月8日	0
10月9日	0
10月10日	0
10月11日	0
10月12日	0
10月13日	0
10月14日	0
10月15日	0
10月16日	0
10月17日	0
10月18日	0
10月19日	0
10月20日	0
10月21日	0
10月22日	0
10月23日	0
10月24日	0
10月25日	0
10月26日	0
10月27日	0
10月28日	0
10月29日	0
10月30日	0
10月31日	0
11月1日	0
11月2日	0
11月3日	0
11月4日	0
11月5日	0
11月6日	0
11月7日	0
11月8日	0
11月9日	0
11月10日	0
11月11日	0
11月12日	0
11月13日	0
11月14日	0
11月15日	0
11月16日	0
11月17日	0
11月18日	0
11月19日	0
11月20日	0
11月21日	0
11月22日	0
11月23日	0
11月24日	0
11月25日	0
11月26日	0
11月27日	0
11月28日	0
11月29日	0
11月30日	0

●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。
- 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。

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. (Flowtopography)

さまざまな味のフレーバーを楽しむ上に、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。