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。

●大手Webサイト相次いで接続障害･･･DNSサービスへのDDoS攻撃が原因

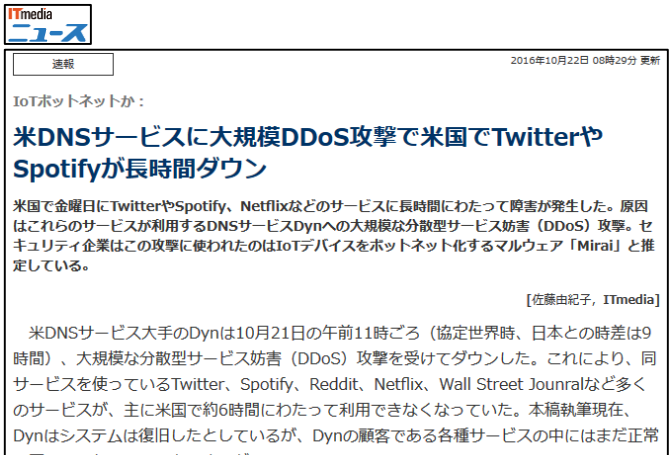
http://www.itmedia.co.jp/news/articles/1610/22/news024.html
http://www.yomiuri.co.jp/science/goshinjyutsu/20161028-OYT8T50051.html

このニュースをザックリ言うと･･･

- 10月21日の11:00頃から17:00頃（協定世界時：UTC）にかけて、米国のDNSサービスDynがDDoS攻撃を受け、ダウンしていたことが判明しました。
- Dynのダウンにともない、同サービスを利用するTwitterやPayPal等の著名なWebサービスに接続障害が発生する事態となっていました。
- Dynはその後復旧したものの、しばらくの間各サービスでの接続障害は続いていたとされています。
- 米Flashpoint社は、Webカメラをはじめとするいわゆるlot（Internet of Things：モノのインターネット）機器等がマルウェア「Mirai」に感染し、DDoS攻撃に加担させられた可能性があるとしており、Miraiは機器の管理画面やtelnetポート（TCPポート23番）等にデフォルトのパスワードで不正ログインし、感染するといった挙動をとるとされています。

AUS便りからの所感等

- Dynを利用していた大手サービスの中には別のDNSサービスに切り替えることにより復旧したところもありましたが、DNSサービス等において、複数の業者を利用することは可用性の維持のために重要です。
- 一方で、今後複数の大手サービスを同時にダウンさせられるレベルのDDoS攻撃が発生することも懸念され、各DNSサービスがDDoS攻撃にどう対応していくかが注目されます。
- LANがルータ・ファイアウォールやUTM等を隔てたNATの内側で構成される形が長年一般的になっていた一方で、IoTデバイスの多くはUPnP（Universal Plug and Play）を用い、外部からのアクセスを受け付けるようルータの自動設定を行う等、容易にネットワークへ参加するための機能を備えており、今回のMiraiのケースでもそういった機器が狙われたとみられています。
- パスワードをデフォルトから変更し、UPnP機能の有無を確認し、可能な限り無効化すること等、IoT機器そのもののセキュリティを強固な設定とする対策は必要不可欠であり、加えて、インターネットから機器に不正アクセス可能な状態でないか、適宜ネットワークに対する診断を受けることも検討に値するでしょう。


ITmedia ニュース

速報

2016年10月22日 08時29分 更新

IoTボットネットか：

米DNSサービスに大規模DDoS攻撃で米国でTwitterやSpotifyが長時間ダウン

米国で金曜日にTwitterやSpotify、Netflixなどのサービスに長時間にわたって障害が発生した。原因はこれらのサービスが利用するDNSサービスDynへの大規模な分散型サービス妨害（DDoS）攻撃。セキュリティ企業はこの攻撃に使われたのはIoTデバイスをボットネット化するマルウェア「Mirai」と推定している。

[佐藤由紀子，ITmedia]

米DNSサービス大手のDynは10月21日の午前11時ごろ（協定世界時、日本との時差は9時間）、大規模な分散型サービス妨害（DDoS）攻撃を受けてダウンした。これにより、同サービスを使っているTwitter、Spotify、Reddit、Netflix、Wall Street Jounralなど多くのサービスが、主に米国で約6時間にわたって利用できなくなっていた。本稿執筆現在、Dynはシステムは復旧したとしているが、Dynの顧客である各種サービスの中にはまだ正常に戻っていないものもあるようだ。


YOMIURI ONLINE

「IoT乗っ取り」攻撃でツイッターなどがダウン

2016年10月28日 19時35分

日本時間の10月22日早朝にツイッターやアマゾンなどの大手ネットサービスが世界的に5時間に渡って接続しにくくなった。攻撃元はネット接続された監視カメラ、デジタルビデオレコーダーなどの「IoT（モノのインターネット）」だったことがわかっている。（ITジャーナリスト・三上洋）

監視カメラなどを踏み台に大規模サイバー攻撃

今回被害に遭ったのは、ツイッター、アマゾンのほかに、音楽配信のスポティファイ（Spotify）、動画配信のネットフリックス（Netflix）などで、5時間に渡って接続しにくくなるトラブルが発生した。

原因は監視カメラ、デジタルビデオレコーダーなどの無人機器が乗っ取られ、大量のデータを送りつけたためと推測されている。いわゆるIoT（Internet of Things＝モノのインターネット）が踏み台として使われた大規模サイバー攻撃だ。

●住宅ローンの顧客情報流出か･･･役職員のメールが外部に転送される設定に

http://www.itmedia.co.jp/enterprise/articles/1610/26/news145.html

このニュースをザックリ言うと･･･

- 10月26日（日本時間）、住宅ローン「フラット35」を取り扱う優良住宅ローン社より、同社顧客等の個人情報が漏えいした可能性があると発表されました。

- 発表によれば、漏えいの可能性があるのは、ローン返済中の利用者35,738名、および借入手続者等を含む計37,247名の氏名・住所・電話番号・メールアドレスおよび返済口座情報等となっています。

- 同社は10月6日の時点で、メール管理サーバが9月10日に不正アクセスを受け、以後9月30日までの間、役職員5人の受信メールが外部のメールアドレスに転送される設定になっていたこと、および10月3日に不正アクセスの犯人とみられる人物からメールで脅迫を受けていたことを発表しており、以後調査およびサーバの変更といった対応の後に今回の発表を行ったとのことです。

ITmedia エンタープライズ

2016年10月26日 23時01分 更新

住宅ローン「フラット35」の顧客情報流出か、役職員のメールに不正な転送設定

住宅金融支援機構から業務委託を受けている優良住宅ローンは、不正アクセスで3万7247人分の個人情報が漏えいした可能性を発表した。メールサーバの設定が不正に変更されていたという。

[ITmedia]

住宅金融支援機構と同機構が業務を委託する優良住宅ローンは10月26日、住宅ローン「フラット35」利用者の個人情報が漏えいした可能性があるとして、調査状況などを発表した。優良住宅ローンのメールサーバの設定が不正に変更され、役職員のメールが外部に転送されていたという。

該当者	漏えいした可能性のある情報	人数
ローン返済中	返済口座の情報（氏名、金融機関名、支店名、口座科目、口座番号）、引落金額、契約番号	3万5738人
借入手続き者（連帯債務者、担保提供者の情報を含む）	氏名、住所、生年月日、国籍、電話番号、勤務先、年収、連絡先メールアドレス、資金計画情報、物件情報	112人
抵当権設定登記者（連帯債務者、担保提供者の情報を含む）	氏名、住所、物件情報、抵当権情報	93人
つなぎ資金利用者	氏名（漢字およびカタカナ）、住所、つなぎ融資実行情報、債権番号	1188人
問い合せや資料請求者	氏名、住所、電話番号、メールアドレス	233人

AUS便りからの所感等

- 顧客との正規のやりとりに関するメールが「メールサーバ上で第三者に転送される設定になっていた」ということで、スパムメールやマルウェア添付メールの要領で外部への送信を遮断することは困難でしょう。

- このような不審な宛先への送信メールを食い止める目的での出口対策としては、メール誤送信対策ソリューションをメールサーバあるいはその外側で導入し、宛先の確認を行うのが有用ですが、毎回の警告と承認が煩雑になりがちな点には注意が必要でしょう。

- 併せて、サーバ上の設定ファイルあるいはデータベースに格納された設定内容の改ざんを検知し、侵入の発生を早い段階で把握する体制を整備することも重要となります。

●Linuxカーネルに脆弱性発覚･･･ローカルの攻撃者にサーバを乗っ取られる恐れ

http://www.itmedia.co.jp/enterprise/articles/1610/24/news044.html

このニュースをザックリ言うと･･･

- 10月20日（米国時間）、Linuxカーネルに管理者権限を奪取可能な脆弱性が存在していたことが発表され、修正パッチがリリースされました。

- 「Dirty COW」と名付けられた脆弱性は、Linuxカーネルのメモリ管理機構に存在しており、管理者権限を持たないローカルの攻撃者にこれを悪用されることによりサーバを乗っ取られる可能性があるとされています。

- 既に攻撃コードは公開され、脆弱性に対する攻撃の傾向も観測されている模様です。

- 各種Linuxディストリビューションにおいて、カーネルの修正バージョンのリリースが進んでいるようです。

AUS便りからの所感等

- この脆弱性を突くには、攻撃者がサーバ上にログインして任意のプログラムを実行可能であることが条件で、リモートから不正なパケットを送信するだけで攻撃することは基本的に不可能です。

- 今後アンチウイルスやUTMのパターンファイル更新により、攻撃コードを含むプログラムの持ち込みを食い止められるようになる可能性も考えられますが、基本的にはカーネルのアップデートによる根本的な対策を強く推奨致します。

- SSHサービス等により、管理者以外のユーザが前述のような形でサーバにログイン可能な構成になっている場合には、ユーザの中の悪意のある者が攻撃を行う、あるいはユーザアカウントを攻撃者が奪取して侵入するというシナリオが考えられるため、特に早急な対策が必要となるでしょう。

ITmedia エンタープライズ

2016年10月24日 06時30分 更新

Linuxカーネルに脆弱性「Dirty COW」発覚、管理者権限を取得される恐れ

悪用は比較的容易とされ、この問題を悪用した攻撃が既に出回っているという。しかし攻撃を受けたとしてもログに痕跡が残らないことから検出は難しい。

[鈴木聖子，ITmedia]

Linuxカーネルに10年以上前から存在していた脆弱性に関する情報が公開され、悪用を狙う攻撃の発生が報告されている。Linuxディストリビューション各社がセキュリティ情報を公開し、米セキュリティ機関US-CERTも10月21日、ユーザーや管理者に対応を促した。

脆弱性は、Linuxカーネルのメモリサブシステムでcopy-on-write（COW）を処理する方法に起因し、バージョン2.6.22以降が影響を受ける。Linuxカーネルのパッチは10月20日に公開されており、リーナス・トーバルズ氏はこの問題について、「11年前に修正を試みたがうまくいかなかった」と明かしている。

COWに問題が存在することから「Dirty COW」と命名され、専用情報サイトが公開された。同サイトや米セキュリティ機関CERT/CCによれば、この脆弱性を悪用された場合、特権を持たないローカルユーザーによるリードオンリーメモリマッピングへの書き込みが可能になり、攻撃者にroot権限を取得される恐れがある。