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。

## ●マルウェアが混入したZoomの偽インストーラーに注意喚起

https://cybersecurity-jp.com/news/37378
https://blog.trendmicro.co.jp/archives/25286

### このニュースをザックリ言うと・・・

- 6月23日(日本時間)、トレンドマイクロ社より、オンラインビデオ会議ツール「Zoom」のインストーラーに偽装してマルウェアをインストールしようとする攻撃について注意喚起が出されています。

- 注意喚起では二種類の不正なファイルが挙げられており、一つはPCに外部から攻撃者が侵入するためのバックドアを設置し、ユーザー認証情報の窃取や遠隔操作を目的とした細工等を行うもの、もう一つはPCを「Devil Shadow」と呼ばれるボットネットに組み入れ、やはり遠隔操作等を行うものとなっています。

- これらのインストーラーが不審なサイトで配布されていたということもあり、同社では「アプリケーションやソフトウェアは、正規のマーケットプレイスと公式プラットフォームからのみダウンロードする」「端末にインストールされているソフトウェアを最新バージョンに更新し、会議にはパスワードを使用し、ホストコントロールを設定する」ことを呼び掛けています。

### AUS便りからの所感等

- 偽のZoomインストーラーは正規のインストーラーと比べファイルサイズが大きいという特徴が指摘されている一方、正規のインストーラーをダウンロードしてインストールすると同時にバックドア等のコンポーネントもダウンロードしてPCに感染する挙動をとることも挙げています。

- よって、攻撃者の出方次第では、マルウェア自体に正規のインストーラーを含まずとも、正規のインストーラーと全く同じサイズに調整された偽インストーラーが出回る可能性も考えられます。

- アプリをインストールしようとしてこのような偽のインストーラーを掴まされるのは、往々にして検索エンジンでの検索結果の上位に出たサイトに安易にアクセスするケースが多くみられるため、アンチウイルスやUTMあるいはWebブラウザーのアンチフィッシング機能を有効にするとともに、正規のインストーラーがどこで入手できるか、検索結果をより詳しく調査して情報収集することが、偽インストーラーの回避に有用でしょう。

TREND MICRO

偽のZoomインストーラに隠されたバックドアとボットネット「Devil Shadow」

投稿日: 2020年6月23日
脅威カテゴリ: ボットウイルス
執筆: Trend Micro

サイバー犯罪者は、新型コロナウイルスの流行がもたらした「新しい常識」を攻撃に利用しています。具体的な手法の1つとして、テレワークや在宅勤務に欠かせないものとなった人気のアプリケーションやソフトウェアを偽装したり、悪用したりすることによってユーザの端末をマルウェアに感染させる手口があります。トレンドマイクロは、マルウェアのコードを含む、Zoomインストーラを偽装する2つのファイルを発見しました。これらの偽インストーラは、当然、Zoomの公式サイトで配布されたものではありません。偽インストーラのうち1つは、サイバー犯罪者がリモートで不正活動を実行するためのバックドア型マルウェアを感染コンピュータへインストールし、もう1つは、「Devil Shadow(デビルシャドウ)」と呼ばれるボットをインストールします。

| Name | Size |
|---|---|
| ZoomInstaller-ZAPIZ.exe | 15,778 KB |
| ZoomInstaller-DEVILSHADOW.exe | 14,087 KB |
| ZoomInstaller-legit.exe | 11,650 KB |

図1:偽インストーラは、正規のZoomインストーラと比較してファイルサイズが大きい

# ●Microsoft、Windows 7/8.1にも新しい「Edge」を自動配信

https://forest.watch.impress.co.jp/docs/news/1261004.html

## このニュースをザックリ言うと・・・

- 6月17日(現地時間)、Microsoft Edgeブラウザー(以下Edge)をWindows 7 SP1(以下7)および8.1向けにも提供する更新プログラム「KB4567409」がリリースされました。

- Edgeはこれまでの独自レンダリングエンジンを用いた古いバージョンに代わってGoogle Chromeと同じレンダリングエンジンを採用した新しいバージョンが6月に配信を開始しており、当初Windows 10専用だったものが7/8.1にも対応した形となっています。

- なお、一般向けのサポートを終了している7にも提供されてはいるものの、有償延長サポート(ESU)に加入している企業を除き、「Edge」の利用は推奨しないとしています。

## AUS便りからの所感

- ChromeがWindows 7(およびServer 2008 R2)のサポートを2021年7月15日まで行うことから、新しいEdgeも同日まで7に提供することが4月に発表されていました(https://forest.watch.impress.co.jp/docs/news/1247077.html)。

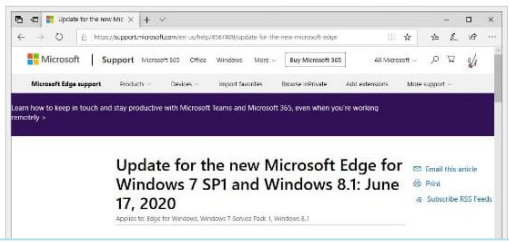
- 既にセキュリティパッチの無償提供がされていないWindows 7、特にIE11でのインターネットへのアクセスを少しでも抑制することが目的とみられていますが、アンチウイルスやUTMによる防御を固めたとしても、そういったサポートが終了したソフトウェアを使用し続けることは常に何らかのリスクを抱えることとなりますので、基本的にはWindows 10への移行を計画することが重要です。

窓の杜 WINDOWS FOREST

**Microsoft、Windows 7 SP1/Windows 8.1にも新しい「Edge」を自動配信**

既定のWebブラウザーはそのまま。IEも引き続き利用可能

樽井 秀人　2020年6月24日 06:00




米Microsoftは6月17日（現地時間）、「Windows 7 SP1」および「Windows 8.1」向けの更新プログラム「KB4567409」を公開した。“Windows Update”を通じて自動でダウンロード・インストールされ、適用が完了すると「Chromium」ベースの新しい「Microsoft Edge」がシステムにインストールされる。

# ● DrupalとMagentoに脆弱性、アップデートを

https://news.mynavi.jp/article/20200622-1060848/
https://news.mynavi.jp/article/20200624-1063565/

## このニュースをザックリ言うと・・・

- 6月17日(現地時間)、CMS「Drupal」にWebサーバー上を乗っ取られる可能性のある脆弱性が存在することが開発者より発表され、翌18日には米US-CERTからも注意喚起が出されています。

- 同22日にはAdobe社より、同社が開発するECサイト構築用ソフトウェア「Magento」に同様の脆弱性の存在が発表されています。

- それぞれセキュリティアップデートがリリースされており、早急な適用が推奨されています。

## AUS便りからの所感

- DrupalはWordPressと同様にWebサイトコンテンツ管理システムとして人気がある一方、脆弱性が頻繁に報告されており、今年だけでも3月・5月にセキュリティアップデートが行われています。

- MagentoのようなECサイト構築のためのソフトウェアに脆弱性が存在することは特に注意が必要で、同種のソフトウェアであるEC-CUBEでは、古いバージョンに存在する脆弱性の悪用により、利用者のクレジットカード情報を含む個人情報が流出するケースが発生しています(AUS便り2020/1/14号参照)。

- Webサーバーあるいはその前面にWebアプリケーションファイアウォール(WAF)やUTMを設置することにより、脆弱性を悪用しようとする不正なリクエストを遮断すること等が期待できますが、根本的な対策としては、やはりサーバー上においてWebアプリケーションのみならず、OSや各種ソフトウェアを随時最新のバージョンにアップデートする体制を確立することが肝要です。

マイナビニュース

**Drupalに緊急の脆弱性、ただちにアップデートを**

後藤大地　2020/06/22 10:17

関連キーワード：脆弱性、 オープンソース、 CMS

United States Computer Emergency Readiness Team (US-CERT)は6月18日(米国時間)、「Drupal Releases Security Updates | CISA」において、Drupalに脆弱性が存在すると伝えた。これら脆弱性を悪用されると、攻撃者によって影響を受けたシステムの制御権が乗っ取られる危険性がある。

**ECプラットフォーム「Magento」に脆弱性、アップデートを**

後藤大地　2020/06/24 09:01

関連キーワード：脆弱性、 JPCERT/CC

JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）は6月23日、「Magento に関するアップデート (APSB20-41) について」において、AdobeのMagento Commerce 1.14系およびMagento Open Source 1系に脆弱性が存在すると伝えた。これら脆弱性を悪用されると、攻撃者によって任意のコードが実行される危険性がある。