【参考資料】

WIZファイル(※)を悪用する攻撃手口に関する注意点

2018年 10月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

※ Microsoft社のWordウィザードに関する情報
https://msdn.microsoft.com/ja-jp/library/cc377002.aspx

はじめに

Microsoft WordのWIZ（Wizard）ファイルを悪用する攻撃手口の情報が、2018年9月に海外で公開されました。

本資料は、この攻撃手口について紹介し、注意点を説明するものです。

（この攻撃手口は、従来より多く観測されている、「.doc/.docx/.docm」といったWord文書ファイルでマクロ機能を悪用するものと本質的には同じです。
不審なOffice文書ファイルのマクロは有効にしないよう、注意してください。）

【参考情報】

- WIZファイルとは
  Microsoft Wordに関連付けされているファイルで、次のようなアイコンのファイルです。
  ファイルを開くと、Microsoft Wordが起動します。ファイルの拡張子は、「.wiz」です。

※本資料では、Microsoft Office 2016 の画面で説明しています。
バージョンにより、表示されるアイコン等は異なる場合があります。

本資料をもとに、攻撃の手口について知っていただくとともに、不審なメールや、不審な添付ファイルに対して警戒いただくようお願いいたします。

攻撃手口

攻撃手口

- 標的を絞った攻撃であるのか、無作為にばらまかれたものであるのかは不明ですが、悪意のあるWIZファイルを添付した攻撃メールの存在を確認しています。

  メールに添付されたWIZファイルを開くと、悪意のあるサーバからウイルスがダウンロードされて、端末がウイルスに感染させられることを確認しています。

- メールに添付されるOffice文書ファイルによる攻撃の多くは、Microsoft Officeの「保護ビュー」の機能で防御することが可能です。本攻撃手口でも「保護ビュー」を有効にしている状態ではウイルスに感染しません。

WIZファイルを悪用する攻撃の観測状況

- 2018年9月時点で、日本語のメールで攻撃が行われた可能性を示す情報は確認しておりません。ただし、今後、日本語のメールで攻撃が行われる可能性もあるため、不審なメールに注意してください。

➡ 本資料にて、攻撃の特徴と対応方法について説明します。

特徴と対応方法

- 現時点で確認している「WIZファイルを悪用する攻撃手口」には次のような特徴があります。

特徴

① メールに添付されたWIZファイルを開くと、**「マクロを有効にする」または、「コンテンツの有効化」というボタン**が表示される。

② 上記①のボタンをクリックすると、**ウイルスに感染させられてしまう。**

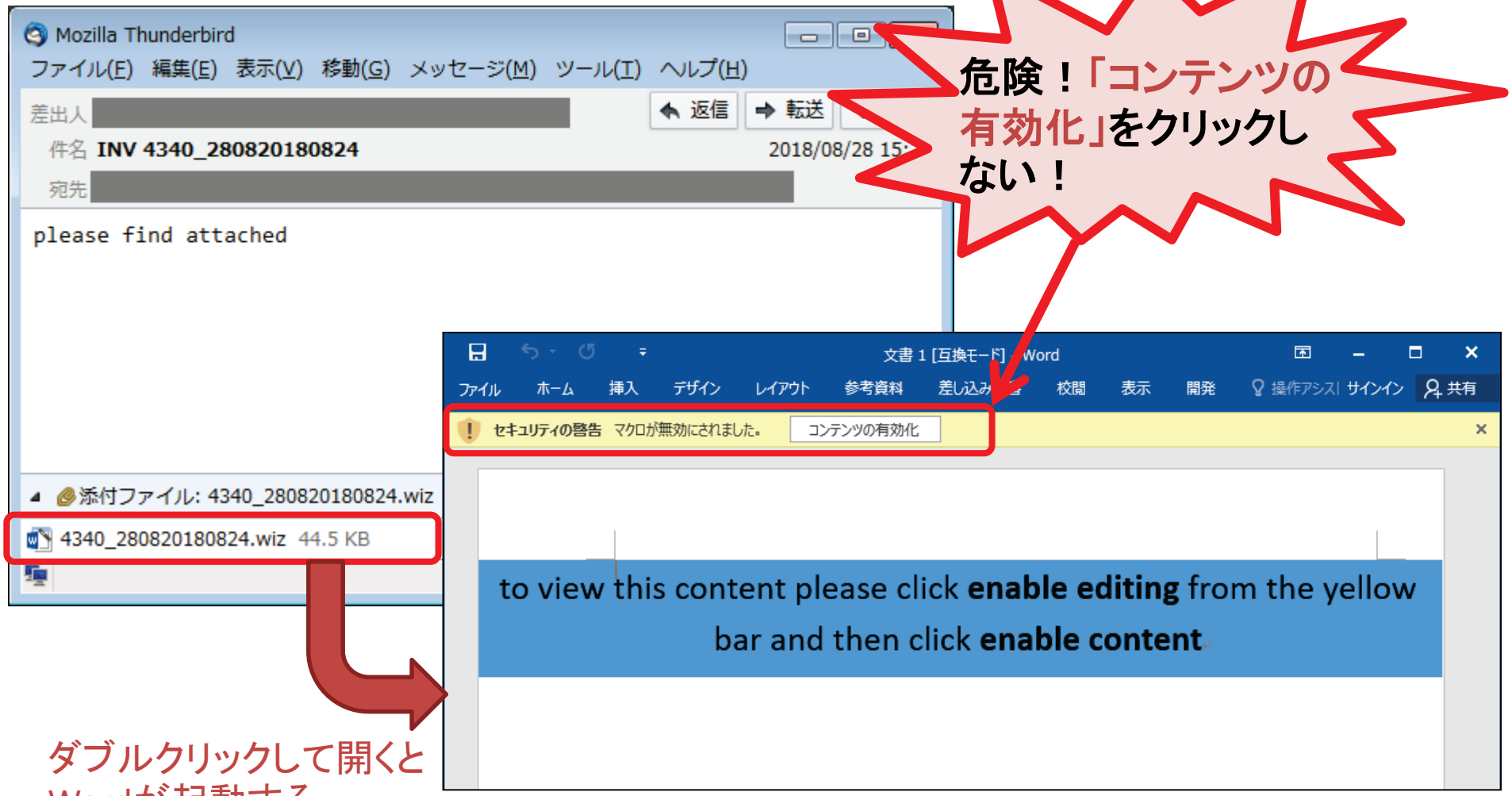
対応方法

上記の特徴にあてはまる、身に覚えのないメールを受信した場合、WIZファイルを開かないよう注意するとともに、**システム管理部門等へ連絡**してください。
（なお、WIZファイルを開いただけではウイルスには感染しません）

次のページからは、実際の悪意のあるメールを例にして説明します。

事例紹介

- メールに添付された、罠が仕込まれたWIZファイルを開いた場合



おわりに

本資料で説明したマクロに関する警告が表示された場合、**「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない**でください。

また、身に覚えのないメールや添付ファイルを開いてしまった場合は、**すぐにシステム管理部門等へ連絡**してください。

本資料で説明したタイプの攻撃のほかにも、Microsoft Officeの機能を悪用したウイルスが存在します。

これらのウイルスに感染しないよう、次のような基本的なウイルス対策を行ってください。

- ✓ **不審なメールの添付ファイルは開かない。**
- ✓ **OSやアプリケーション、セキュリティソフトを常に最新の状態にする。**
- ✓ **メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、警告の意味が分からない場合は操作を中断する。**