ファイルを介して感染するマルウェア「Emotet（エモテット）」についての注意喚起

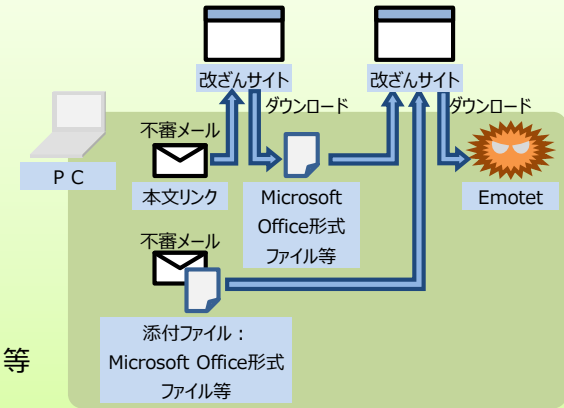
国内のWebサイトが改ざんされ、ファイルを介して感染するマルウェア「Emotet」の配布に利用される事例報告が多く寄せられていると、コンピュータセキュリティ関連情報の発信などを行う一般社団法人JPCERT/CCから公表されています。

「Emotet」の動作

「Emotet」は、ファイルに埋め込まれたマクロや、バッチファイルなどの実行可能ファイルを閲覧・実行することにより感染します。

例）

・不審メールに添付されたファイルを実行して感染
・不審メールに記載された（改ざんサイトの）URLにアクセスしてダウンロードし感染　等



注意喚起

不審メールに注意してください!!

メールに添付されたファイルや、メール本文に指定されたアドレスからダウンロードしたファイルを閲覧・実行する際には、以下のような点に注意して対応ください。

受信メール

差出人：aaa_bbb@EXAMPLE.CO.JP<abcd1234@malware.com>
宛先：　■■■
件名：　Re: 先日お問い合わせいただいた件

Hello. Please Download this file.
Download: http:GoogleDrive.com/id=382

http://download.malware.com/malware.ps1
クリックしてリンク先を表示

送信者のメールアドレスや件名の確認
送信者のメールアドレスがフリーメールでないことや、過去に送信されたアドレスなど既知のものであることを確認すること。また、メールの件名やメール本文が送信者との直近のやり取り等と不整合がないことなどにも注意する。

メールで指定されたダウンロードアドレスが送信者に関連するものであることや、表示アドレスと実際のダウンロードアドレスが同じであることの確認
ダウンロードアドレスが、パブリッククラウドのアドレスなどで送信者に関連するか不明な場合は、送信者に（メール以外の）電話等により確認すること。また、メールに表示されている文字列ではなく、実際にリンクされているダウンロードアドレスを確認すること

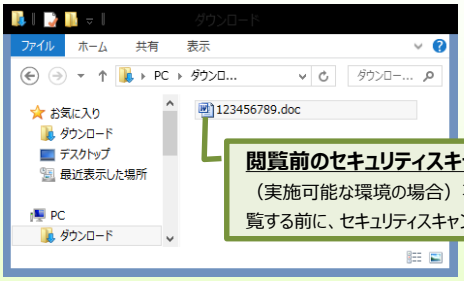
差出人：aaa_bbb@EXAMPLE.CO.JP<aaa_bbb@EXAMPLE.CO.JP>
宛先：　■■■
件名：　ファイルをお送りいたします

123456789.doc
申込書.doc　.exe

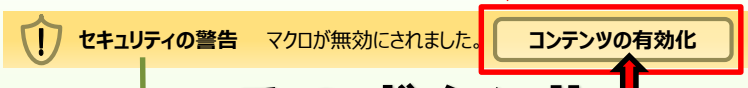
ファイル名、拡張子の確認
ファイル名、拡張子に不審な点がないか確認すること（ファイル名がメールの内容と合致しているか、数字だけで構成されていないか、拡張子に不要な空白がないかなど）

不用意にボタンを押さないで!!

メールの添付ファイル、ダウンロードしたファイル



閲覧前のセキュリティスキャンの実行
（実施可能な環境の場合）不審なファイルを閲覧する前に、セキュリティスキャンを実行すること



このボタン!!

閲覧時のマクロ実行の注意
ファイル閲覧時にマクロ実行が要求された場合には、送信者に（メール以外の）電話等により確認すること

（参考）Microsoft Office形式ファイル及び実行可能ファイルについて

Microsoft Office形式ファイル及び実行可能ファイルについて、よく利用される代表的な拡張子を示します。ここでは代表的な拡張子を掲載しており、これ以外にも拡張子があることに留意ください。

また、不審メールに添付される場合は、不必要に長い空白を含めるなどし、拡張子を問題のない形式に偽装している場合もあるため注意ください。

表 1 主なMicrosoft Office形式ファイルの拡張子

Microsoft Office アプリケーション	マクロ記載 不可/可/その他	拡張子例
Word	不可	**docx（Microsoft Word 2006以降の標準ファイル形式）**、dotx
	可	doc、docm、dot、odt
	その他	rtf(*1)
Excel	不可	**xlsx（Microsoft Excel 2006以降の標準ファイル形式）**、xltx
	可	xls、xlsm、xlt、xlsb、xla、xlam、xltm、xlw、ods
	その他	csv(*2)、iqy(*2)
PowerPoint	不可	**pptx（Microsoft PowerPoint 2006以降の標準ファイル形式）**、potx、odp、ppsx
	可	ppt、potm、pot、ppa、ppam、ppsm
	その他	-

*1 一般的にはマクロを含めることはできないが、特殊な方法を用いることでマクロを含めることができる。

*2 マクロを含めることはできないが、サイバー攻撃に使用される場合がある。

表 2 主な実行可能ファイルの拡張子

bat、cmd、com、cpl、exe、hta、jar、js、jse、lnk、msc、msi、scr、url、vbe、vbs、wsf、wsh

Microsoft Office形式ファイルを送受する必要がある際に、マクロを使用する必要がない場合は、マクロを含むことができないファイル形式を使用することを推奨します。

お問い合せ先：東京都産業労働局商工部　中小企業サイバーセキュリティ相談窓口
電話番号:０３-５３２０-４７７３（都庁開庁日　9:00~12:00、13:00~17:00）