2022 年 3 月 24 日
デジタルアーツ株式会社

PRESS RELEASE

【セキュリティレポート】
最新の Emotet 攻撃メールに使われる添付ファイルは 2 種類のみ

～注意すべきは「xlsm」と「パスワード付き ZIP」 マクロは「VBA」から「Excel4.0」を多用する手口に変化～

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、マクロ付き Office ファイルについてのセキュリティレポートを公開したことを発表します。

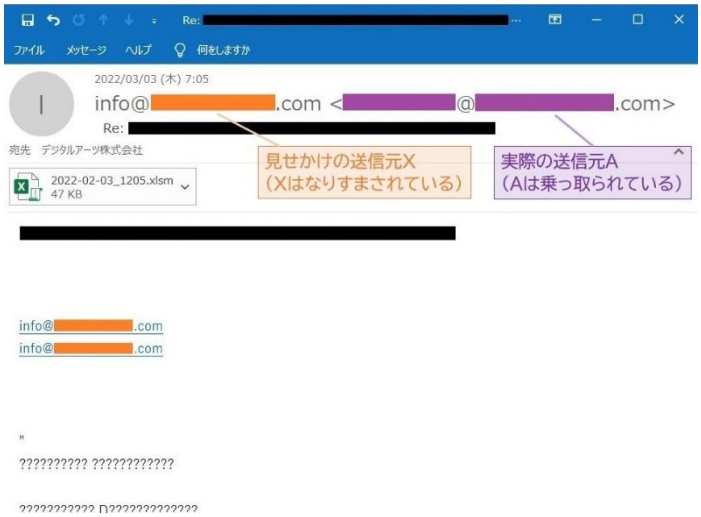
Emotet は、2019 年後半から 2020 年前半にかけて国内で猛威を振るったことで、一気に知られるようになったマルウェアです。2021 年 1 月末に一度テイクダウンしましたが、同年 11 月に活動再開が確認され、現在国内で被害を大きく拡げています。

Emotet の多くは、メールに記載された URL リンクや、添付ファイルに仕込んだマクロを実行させ、マルウェアをダウンロードさせる手口です。こうした添付ファイルは、マクロ付きの「doc」ファイルまたは「xls」ファイル、さらに、「docm」や「xlsm」が使われています。

今回、復活した Emotet の攻撃メールをデジタルアーツで分析し、メール拡散に使われるファイルのパターンを改めて抽出しました。最新の Emotet の攻撃パターンを紹介します。

2022 年 3 月時点で、Emotet の攻撃メールに使われる添付ファイルは 2 種類のみ

Emotet が 2021 年 11 月に再開して以後、メールによる拡散活動では「doc」「docm」「xls」「xlsm」の添付ファイルと、これらを格納した「パスワード付き ZIP ファイル」、メール内の URL リンクからダウンロードさせるものなど、さまざまな変化が見られました。そして、2022 年 3 月時点でのメールによる拡散活動は、「xlsm」ファイルが添付されているパターンと「xlsm」を格納した「パスワード ZIP ファイル」が添付されているパターンの 2 種類のみとなっているようです。



【図 1】デジタルアーツが受信した Emotet メールの例

従来の「VBA マクロ」ではなく、「Excel4.0 マクロ」を用いる手口に変化

「Excel4.0（XLM）マクロ」とは、現在ではあまり使われなくなった古いマクロの記述方法です。しかし、新しいバージョンの Excel でも、未だに実行可能となっており、アンチウイルス回避や解析妨害のため、このマクロを悪用した攻撃が多く存在します。「xlsm」ファイルを開いてコンテンツを有効化（マクロを有効）すると、非表示のシートにばらばらに記述された文字を使って組み立てられたコードによって「Excel4.0 マクロ」が実行され、感染へと至ります。従来の Emotet は、VBA マクロ実行後に PowerShell を呼び出して感染させる手法が多く用いられていましたが、2022 年 3 月時点では、「Excel4.0 マクロ」しか用いられていません。

近年の Office 製品における、マクロのセキュリティリスクへの対応

Microsoft は、2021 年と 2022 年に 2 つの特徴的な発表をしています[※1]。まず、「VBA マクロ」については、「インターネットから取得した Office ファイルの VBA マクロをデフォルトで無効化」する措置を、2022 年 4 月以後に適用する予定です。「インターネットから取得した Office ファイル」とは、メールの添付ファイルも含まれます。また、現在のように利用者がワンクリックで簡単に「VBA マクロ」を有効できる、という状況も改善される見通しです。次に、「Excel4.0 マクロ」については、「VBA マクロ」が有効であっても、「Excel4.0 マクロ」だけを無効にできるという措置です。こちらはすでに適用されており、2021 年末までに Microsoft 365 ではデフォルトで「Excel4.0 マクロ」は無効となっています。

Emotet に効果は？

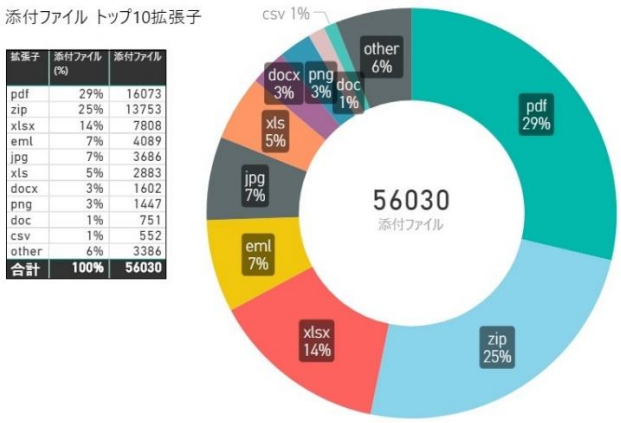
以下に、Emotet においての懸念事項をまとめました。侵入経路の多くはメールの添付ファイルやメール本文に記載された URL です。このため、メールゲートウェイ部分でメール攻撃を防ぐ、マルウェアのダウンロードを Web プロキシで防ぐ、といった対策が有効ではないでしょうか。

	対象バージョン	動作	Emotetに効果があるか （対 Excel4.0を使うダウンローダー）
1. インターネットから取得したOfficeファイルのVBAマクロをデフォルトで無効化	MS365、Office LTSC 2021、Office 2021、Office 2019、Office 2016、Office 2013	デフォルト無効に（2022年4月～予定）	× 効果が無い可能性 • 「VBAマクロ」とは明記されているが、VBAと異なる「Excel4.0マクロ」については述べていない。 • zipファイルに格納されている場合、解凍後のファイルは「インターネットから取得したファイル」だと判定されない可能性がある。
2. Excel4.0マクロの無効化	MS365	デフォルト無効（2021年末）	○ 効果あり
	Office LTSC 2021、Office 2021	デフォルト有効だが設定で無効にできる	△ 設定すれば効果あり
	Office 2019、Office 2016、Office 2013	設定が無いため無効にできない	×

【図 2】Emotet においての懸念事項

業務利用の受信メールでマクロ付きファイルは非常に少ない

下記で紹介する数値・グラフは、国内 75 組織が外部から受信したメールデータのうち「何らかのファイルが添付された受信メール」に限定し、その「添付ファイルの拡張子」を調査した結果です※2。



【図 3】左：添付ファイルトップ 10 拡張子
【図 4】右：全添付ファイルのうち、Word/Excel だけに限定した場合での拡張子の割合

この調査によって、マクロ付きの Office ファイルを業務利用することは非常に少ないということがわかりました。業務利用しないのであれば、あらかじめ受信しないように設定することも検討して良いでしょう。

▶デジタルアーツは、最新の攻撃メールにも対応した、メールセキュリティ製品を提供

メールセキュリティ製品「m-FILTER」 Ver.5 は、Emotet など、あらゆるメール攻撃を防ぐ外部攻撃対策、電子メールフィルタリング（送受信制御）による誤送信対策、全保存（メールアーカイブ）・検索機能による内部統制・コンプライアンス強化、スパムメール対策が可能なメールセキュリティ製品です。
https://www.daj.jp/bs/mf/

①「パスワード付き ZIP ファイル」による攻撃メールを防ぐ

「パスワード付き ZIP ファイル強制検査機能」により、パスワード付き ZIP ファイルを受信者の端末ではなく「m-FILTER」上で解凍して検査することができます。偽装したパスワード付き ZIP ファイルを使った攻撃メールへの対策が可能です。

②マクロ付きの添付ファイルによる攻撃メールを防ぐ

「添付ファイル偽装判定」により、添付ファイルの拡張子やフォーマットを検査することができます。マルウェア本体を添付する攻撃メールはもちろん、マルウェアをダウンロードするマクロ付き添付ファイルの攻撃メールも逃さずにブロックします。

▶最新の Emotet 攻撃メールに使われる添付ファイルについてのレポートはこちら
セキュリティレポート https://www.daj.jp/security_reports/220324_1/

※1 Microsoft365 ブログ
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805
https://techcommunity.microsoft.com/t5/excel-blog/excel-4-0-xlm-macros-now-restricted-by-default-for-customer/ba-p/3057905

※2 調査は Emotet が流行していない時期に行ったものです。https://www.daj.jp/security_reports/200316_1/

デジタルアーツ株式会社 概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー14F ▶URL: https://www.daj.jp/

＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社 広報担当 松岡 TEL : 080-8163-0311 / E-mail : press@daj.co.jp
※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせは上記とさせていただきます