2022 年 2 月 2 日
デジタルアーツ株式会社

PRESS RELEASE

復活した Emotet の 1 か月を追ったセキュリティレポートを公開
～感染手法はいずれもメールを起点、アプリインストーラーを用いた新たな手法も～

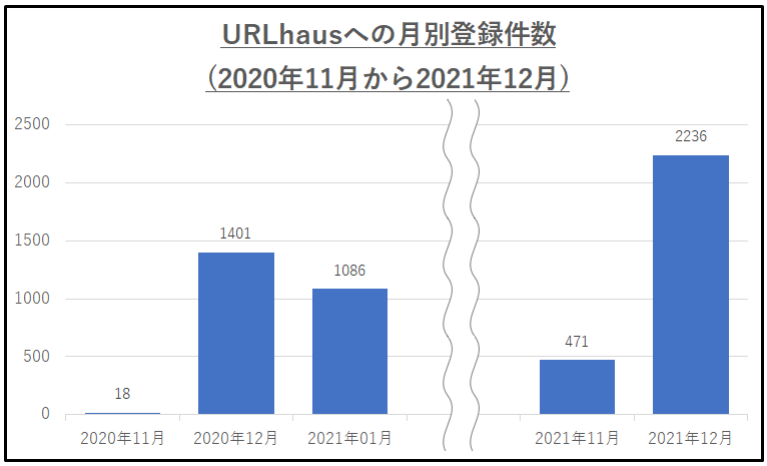
情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、復活した Emotet についてのセキュリティレポートを公開したことを発表します。

Emotet は 2014 年頃から活動が確認されているマルウェアで、従来のバンキングマルウェアとしての機能のほかに、他のマルウェアを呼び込む機能や、ネットワーク内部やメールの履歴をもとに自身を拡散する機能なども持ち合わせています。2019 年後半から 2021 年初頭にかけて猛威をふるっていたことで、ご記憶にある方も多いのではないでしょうか。このときの流行は、2021 年 1 月末に Emotet の用いるボットネットがテイクダウンされたことにより終了しました。

しかし、同年 11 月に活動を再開。弊社で観測した範囲でも、12 月上旬から Emotet に関連するとみられるメールが徐々に増えました。12 月 6 日および 9 日には、マルウェア感染の疑いのあるお客様へ感染情報やホームページの改ざん情報をお知らせする弊社の D アラートでも報告しております。今回は、11 月 15 日頃の Emotet 復活からの 1 か月で確認された、様々な感染手法について紹介します。

12 月 6 日公開分: https://www.daj.jp/bs/d-alert/bref/?bid=172
12 月 9 日公開分: https://www.daj.jp/bs/d-alert/bref/?bid=174

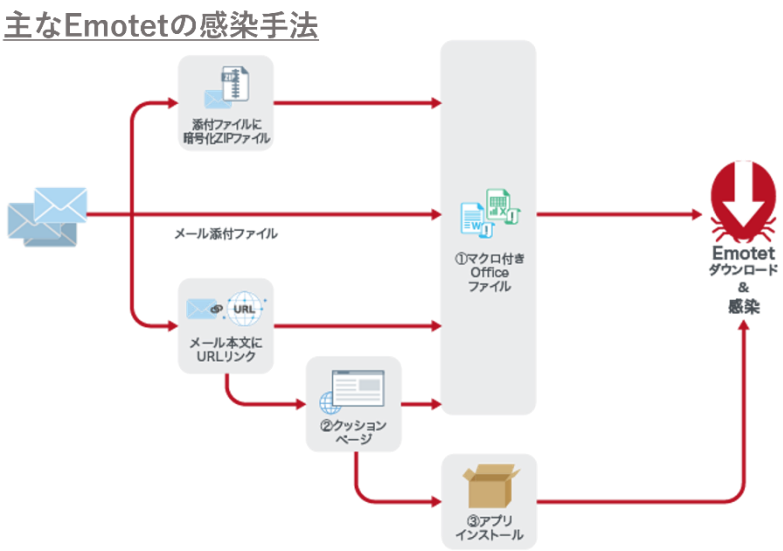
今回の復活は再度の流行となるか



2020 年 11 月から 2021 年 12 月まで、マルウェアの配布に使用された悪意ある URL を共有するプロジェクト URLhaus に報告された Emotet に関する URL の月別件数を示しました。特に 2021 年 12 月は、テイクダウンの直前と比べても多いことがわかります。これは 1 日当たりの報告数においても同様です。

1 か月間で用いられた感染手法

11 月中旬の活動再開以降、Emotet は短いスパンで感染手法が変化していきましたが、報告されている手法はいずれも、メールを起点としていました。



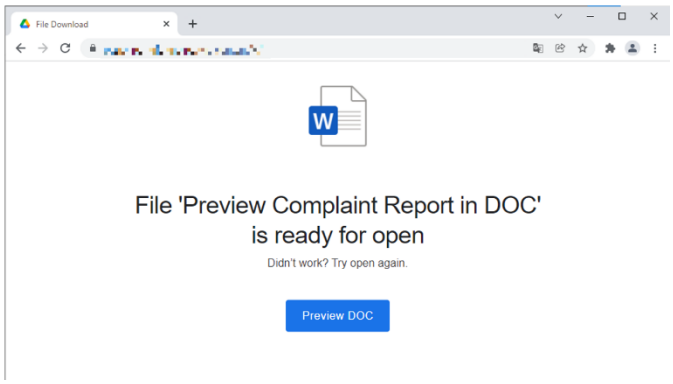
メール以降の感染手法の多くは、Excel や Word といった Microsoft Office ファイルに含まれるマクロによるものであり、これは以前流行した Emotet と近い特徴です。ただし、今回は、その Office ファイルがメールに直接添付されるケース、暗号化 zip ファイルに含まれるケース、メールにリンクされた Web ページからダウンロードされるケースなど、ファイルが端末に至るまでの手法は複数存在しました。また、Office ファイル内のマクロの挙動も複数確認されております。他に Office ファイルを用いない感染手法として、アプリインストーラーを用いたものもありました。この場合、メールのリンク先から APPINSTALLER ファイル（拡張子 .appinstaller)をダウンロードし、実行することで感染に至ることが確認されています。それぞれの手法について詳しく説明します。

① マクロを含む Office ファイル

Emotet の活動再開直後、多く取られた感染手法としては、メールへの Office ファイルの添付でした。この時、多く見られた拡張子は「.docm」および「.xlsm」でした。これらはそれぞれ、Microsoft Word マクロ有効文書、Microsoft Excel マクロ有効ワークシートというファイルの種類を示すものです。これらのファイルは Microsoft Office Word 2007 以降、あるいは Microsoft Office Excel 2007 以降で作られていること、そしてマクロが有効になっていることを示すファイル形式です。特徴としては、変数名やプロシージャ名に対してランダムな文字列が用いられていることや、複数回に分けて文字列を処理し、難読化を解除し実行していることがあります。難読化については不要な文字列を挿入してあるだけで比較的シンプルです。しかし、これにより exec や start などといった実行を示す文字列を見つけにくくなり、セキュリティ機能の回避を狙っているものとみられます。

② メールに書かれるクッションページの URL

クッションページの例



送られてきたメールに添付ファイルがないケースも多く見受けられました。その場合、メールに URL が記載されており、アクセスするよう書かれています。実際にアクセスすると、マクロを含む Word ファイルや Excel ファイルがダウンロードできるリンクがある設計となっていました。この URL をクッションページと呼んでいます。クッションページの多くは、WordPress などの脆弱性を用い、改ざんされた Web サイトからできていました。ファイルの閲覧にはプレビューボタンを押す必要があるようにも見受けられ、クリックするとまた別の改ざんサイトへアクセスし、マクロを含む Office ファイルをダウンロードします。クッションページや、そこにリンクされた悪性ファイルの置かれたページは、いずれも改ざんサイトであるため、サイト管理者の対応状況によっては数日間やそれ以上アクセス・ダウンロード可能な状態が続いているケースがあるのも特徴です。

③ 新たな感染手法:アプリインストーラーの利用

12 月上旬には、アプリインストーラーを用いた新たな感染手法も現れました。アプリインストーラーとは、Microsoft が提供するアプリケーションで、Windows10 から利用できるようになったものです。Windows 向けのアプリケーションのインストールが容易になるものとして、多くの Windows10 に標準で導入されているとみられます。アプリインストーラーは本来、拡張子「.appinstaller」である APPINSTALLER ファイルを読み込むことで、アプリケーションのインストールを開始します。Emotet での感染活動でも、このファイルが前述のクッションページから配布されました。アイコンは正常なものと同じであり、この時点で見分けることは難しいと考えられます。

▶デジタルアーツは、安全に Web とメールを利用していただける「ホワイト運用」を実現

① マクロを含む Office ファイルがメールに添付されていた場合

「m-FILTER」Ver.5 では、メールにマクロを含む Word 97-2003 文書(拡張子「.doc」)や Excel 97-2003 ブック(拡張子「.xls」)が添付されていた場合、旧型式マクロブロック機能でブロックが可能です。Microsoft Word マクロ有効文書(拡張子「.docm」)や Microsoft Excel マクロ有効ワークシート(拡張子「.xlsm」)の場合は、マクロ含有判定により検知が可能です。さらに、添付ファイルマクロ除去ができるメール無害化の機能もございます。
https://www.daj.jp/bs/mf/

② Office ファイルのマクロを実行してしまった場合

「i-FILTER」Ver.10 のダウンロードフィルターでは、改ざんサイトに埋め込まれた悪性ファイルのダウンロードを検知することが可能です。また、多様なアクセス制御には User-Agent による制御機能もございます。
https://www.daj.jp/bs/i-filter/

③ アプリインストーラーのダウンロード URL にアクセスしてしまった場合

今回確認されているアプリインストーラーのダウンロード URL は、*.web.core.windows.net ドメインでした。このドメイン自体は Microsoft Azure に関するものであり、すべてが有害な URL ではありません。また、「*」には様々なサブドメインが含まれており、特定のドメインのみを悪性と判断するのは難しい状態でした。このように簡単に生成される URL でもブロックできるよう、「i-FILTER」Ver.10 にはホワイト運用という機能がございます。生成されたばかりの URL はカテゴリされていない状態となりますので、ホワイト運用時にはブロックされます。
https://www.daj.jp/bs/ifmf/

▶復活した Emotet についてのレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。
セキュリティレポート　https://www.daj.jp/security_reports/220202_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