2021 年 12 月 16 日
デジタルアーツ株式会社

PRESS RELEASE

「Qakbot」等に感染する日本語返信型マルウェア添付メールに注意

～メールの件名が日本語かつ返信型という厄介な特徴を持ち、今後日本語も巧妙化する恐れ～

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、日本語返信型の不審なメールで届くマルウェア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いたします。

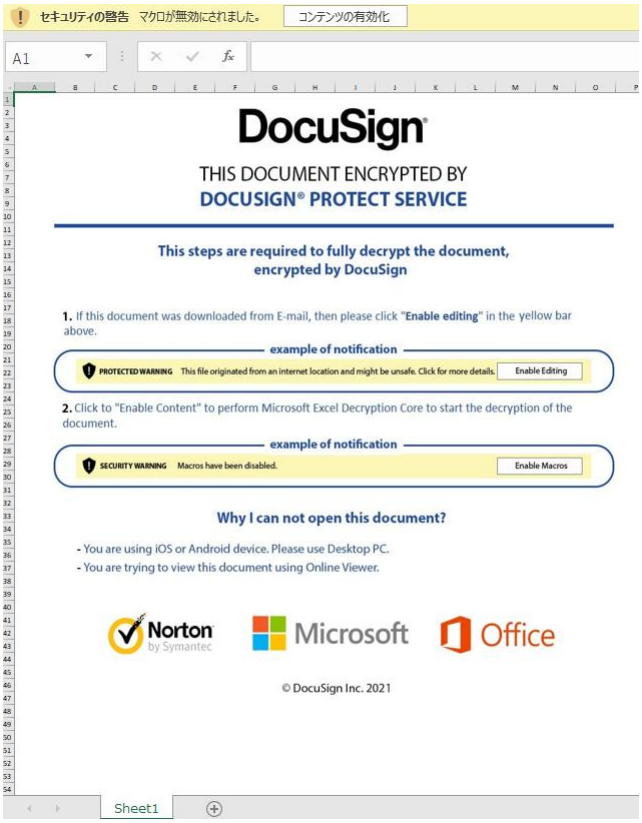
2021 年 11 月 2 日、デジタルアーツでは複数の不審なメールを観測しました。メールには、日本語のメールに返信したかのような件名と、マクロが含まれる Excel ファイルの入った zip ファイルの添付という共通する 2 つの特徴がありました。これらは Emotet など今までに流行した他のマルウェアにあった特徴です。

マクロを含む不審な Excel ファイル

今回観測されたメールには zip ファイル(.zip)が添付されており、その中には Excel ファイル(.xls)が入っていたとみられます。それぞれのファイル名の特徴は以下の通りです。

zipファイル名	Excelファイル名
CMPL-(8から10桁の数字)-Nov-01.zip□	CMPL-(8から10桁の数字)-Nov-01.xls

この Excel ファイルを開くと、図 1 のようなシートが現れます。



シート上には実在の企業やサービスのロゴ・名称が並んでおり、ファイル暗号化のためにこの画面が表示されているかのような説明が書かれています。そして、上部に表示されたボタンをクリックするよう指示しています。しかし、実際にはこのボタンを押すとマクロが有効化され、ペイロードと呼ばれる悪意のあるコードが自動で実行されます。

今回確認されたマクロの挙動では、非表示だったシートを有効化し、そこに書かれた情報をもとに拡張子が .dat であるファイルのダウンロードが開始します。この .dat ファイルが実行されると、Qakbot というマルウェアに感染するものとみられます。

Qakbot は別名 Qbot や Quakbot とも呼ばれ、2000 年代から存在するマルウェアです。もともとはバンキング型トロイの木馬として、オンラインバンキングなどのログイン情報の窃取を目的としておりましたが、近年流行している検体では様々な機能が追加されているとされています。

今回のキャンペーン（一連の活動）の厄介な特徴

今回観測したキャンペーン（一連の活動）には、いくつかの厄介な特徴が挙げられます。

■メールの件名が日本語かつ返信型

今回の日本語返信型の不審なメールは、約 1 日で 29 件観測しました。観測されたメールの件名の一例を下記にまとめています。なお実在の企業・組織名については伏せておりますが、製造業や保険業などさまざまな企業に対してメールが送られていました。

メール件名の一例
Re: FW: 本日の資料送付
Re: FW: 見積依頼
Re: RE: ■■■■■■■■様　御見積書
Re: RE: 御見積の件
Re: RE: 株式会社■■■■■■■■■様　御見積書　図面
Re: RE: 株式会社■■様　御見積書・図面
Re: Re: 株式会社■■■■■■■■■様　御見積書　図面
Re: Re: ■■■■追加見積
Re: ■■■■■■（■■■■■■）在宅ワーク
Re: ■■■■■■（■■■）様　パーテーション見積依頼の件
Re: 工事日程について
Re: 手続き完了のお知らせ　（■■■■■■■■■■■■■■株式会社）

いずれも実際に企業や組織の間で送信されているような件名であり、一見すると正常なメールかのように見受けられます。特に、すべての件名が「Re:」で始まっており、あたかも取引先などからの返信かのように見えます。さらには、「見積」「図面」など、添付ファイルが含まれそうなキーワードが多く、「在宅ワーク」「パーテーション」といったコロナ禍特有のキーワードが含まれているケースもあります。攻撃者は、ユーザにメールを開封させ添付ファイルから Excel を取り出させるために、このように身近にありそうなメールに偽装させているとみられます。自然な日本語を用いたメールであっても油断せず、添付ファイルを開かない・マクロを有効にしないといった注意が必要です。

■マクロの有効化を促す Excel の文面

Excel のシートには実在の企業やサービスのロゴ・名称が並んでおり、日本語化はされてないものの自然に見える構成です。さらに、マクロを有効化した場合も利用している OS に合わせたロゴが並んでいる画面を表示させるなど、外観にこだわっているように見受けられます。また、上部に表示されたマクロの有効化ボタンが、あたかも元のファイルを閲覧するために押す必要があるかのような文面も用意されています。Excel のマクロについて全く知らない人が読むと、素直にマクロを有効化してしまうケースも多くあるでしょう。ファイルの見た目が整っているかにとらわれず、マクロの有効化をしないよう注意が必要です。また、管理者にてマクロの実行を許可しないなどの設定も有効です。

今後も日本語返信型の不審メールに注意

今回紹介したメール以降にも、弊社では Qakbot への感染につながるとみられるファイルが添付されたメールをわずかながら確認しております。今後も継続的にメールがばらまかれる、あるいはその量が増加する可能性も考えられます。また、Qakbot の機能には感染端末のファイルやメール情報の窃取があるとされており、またメールサーバの侵害によって感染拡大を図っているという情報もあります。日本の企業・組織にてこのような被害が発生すると、さらにメールの文面や Excel ファイルの日本語表現がより精巧になることも予想されます。日本語で書かれたメールや、マクロを含む Excel ファイルの添付など、手法自体は以前から他のマルウェアでも利用されてきたものですが、今後も引き続き警戒が必要です。

▶デジタルアーツでは、マルウェア感染の疑いのあるメールをセキュアな状態で受信

今回受信した日本語返信型の不審なメールについて、添付された zip ファイルに含まれる Excel ファイルが旧形式(Microsoft Excel 97-2003 ワークシート)であり、かつマクロ付きであることを確認しています。このようなファイルについては、「m-FILTER」Ver.5 の旧型式マクロブロック機能でブロックが可能です。添付ファイルによるマルウェア感染で利用されやすい Office ファイル等の「マクロ」、「スクリプト」を除去し、セキュアな状態でメール受信することができます。
https://www.daj.jp/bs/mf/

▶日本語返信型の不審なメールで届くマルウェア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/211216_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　山田　　TEL　: 090-1555-7254　/ 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