2021 年 10 月 5 日
デジタルアーツ株式会社

PRESS RELEASE

見慣れない XLL ファイル（Excel アドイン）を使う攻撃に要注意！
～サンドボックスやアンチウイルスをすり抜ける Excel アドインとは？～

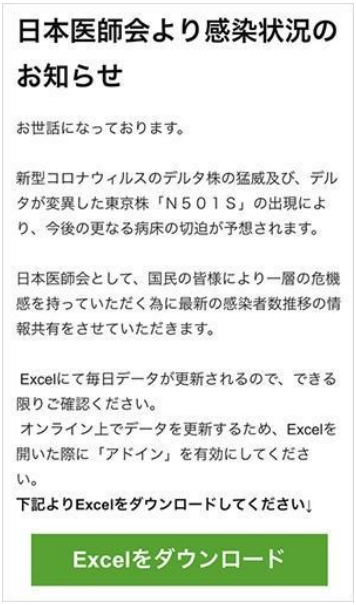
情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、まだ注意喚起がほとんど行われていない XLL ファイル（Excel アドイン）を使う攻撃についてのセキュリティレポートを公開したことを発表いたします。

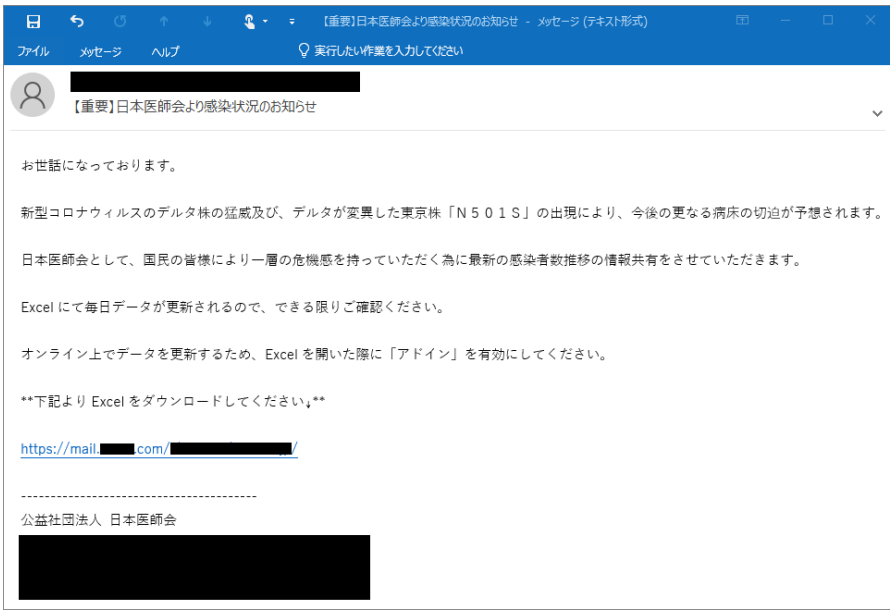
昨今、見慣れない XLL ファイル（Excel アドイン）を使う攻撃が増えています。弊社が入手した不審な XLL ファイルをもとに、どのようにマルウェアに感染するのか検証しました。また、XLL ファイルの懸念点として、サンドボックスで挙動を再現できず、アンチウイルス製品での検知率が低いことが判明しました。

見慣れない XLL ファイル（Excel アドイン）を使う攻撃が増加中

2021 年 9 月 2 日、日本医師会を騙る不審なメールがばらまかれているとして、日本医師会の公式サイトにて注意喚起が発出されました。

【注意喚起】日本医師会を騙る不審メールの流通について





左：日本医師会を騙る不審メールの例（公式サイトより）

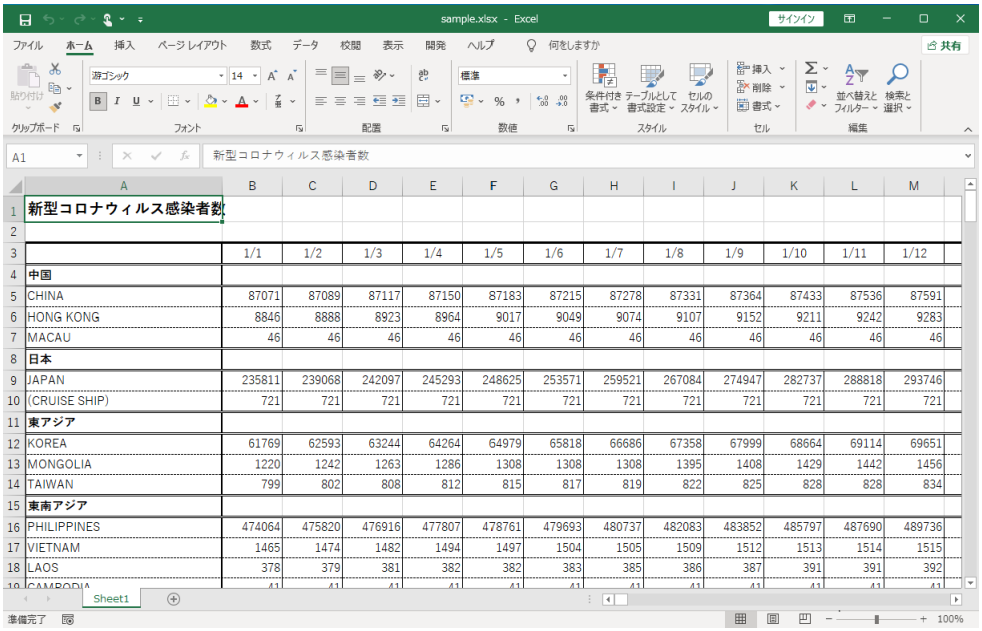
右：日本医師会を騙る不審メールの例（注：報告情報をもとに弊社で再現）

メールに記載のリンクをクリックすると、インターネット上から Excel ファイルのダウンロードがされたとのことです。デジタルアーツでは、この不審な Excel ファイルを入手しました。XLL ファイルを使用した攻撃は海外では観測されているものの、国内ではあまり観測されておらず、また注意喚起もほとんど行われていません。

メールから誘導される不審なファイルは Excel のアドインファイル

ダウンロードされた不審な Excel ファイル

ファイル名の末尾にはあまり見慣れない「.xll」という拡張子がありますが、これは Microsoft Excel のアドインファイルです。



新型コロナウイルス関連の資料を装うおとりファイル

XLL ファイルは「Warzone RAT」というマルウェアに感染するものでした。RAT（Remote Administration Tool または Remote Access Trojan）とは、遠隔操作型マルウェアです。「乗っ取り」の手法で、端末内の情報を盗む、もしくは端末に対して不正な操作を指示することにより、さらに攻撃の範囲を広げることなどが想定されます。今回の日本医師会を騙ったメールは、文章が日本語で記述され、おとりのファイルも日本語で作成されていました。明らかに日本をターゲットにしたものと想定されます。XLL ファイルを用いた攻撃について、サイバーリスク情報を無償で提供する弊社「D アラート」でも何度か発出しております。

08/27 から発生していたマルウェア（Warzone RAT）に感染させると考えられるメールの受信・URL アクセスを検知

08/12 から発生していたマルウェア（Vidar）に感染させると考えられるメールの受信・URL アクセスを検知

サンドボックスやアンチウイルスをすり抜ける Excel アドイン

・サンドボックスで挙動を再現できない場合がある

サンドボックス製品でインストールされている Excel が古いバージョンの場合、アドインを動かすことができず悪性の挙動を検知できません。また、一部のサンドボックス製品においては新しいバージョンの Excel を使っていても、XLL ファイルを Excel で開くように処理ができておらず、アドインの悪性の挙動を検知できていないものがありました。

・アンチウイルス製品での検知率が低い

オンラインマルチスキャンサービスを使って確認したところ、アンチウイルス 65 製品中 2 製品しか検知していなかったものもありました。もちろん確認する時間によって異なりますし、時間が経てば各アンチウイルス製品にシグネチャ（マルウェアや不正アクセスといった攻撃の特徴的なパターン）が登録されるため検知できる製品数は増えていきます。しかし、アンチウイルス製品に登録される前の、メールがばらまかれた当時にはアンチウイルスの検知をすり抜けているということが考えられます。

▶セキュリティ対策の新定番！「ホワイト運用」を実現

情報システム部門の運用負荷を削減でき、安全にアクセスできる情報のみ触れることができる「ホワイト運用」で、受信したすべてのメールを開け、アクセスしたい Web をクリックできるセキュアな世界を実現しませんか。「m-FILTER」Ver.5 では、メールに XLL ファイルが添付されている場合には偽装メール対策「添付ファイル偽装判定」により、添付ファイルを"実行形式ファイル"および"禁止拡張子"として危険性のあるファイルと判定するため、メールの受信を防ぐことが可能です。「i-FILTER」Ver.10 では、「ダウンロードフィルター」機能により Web からの XLL ファイルやその他の危険なファイルのダウンロードを防ぐことが可能です。
▸デジタルアーツの「ホワイト運用」https://www.daj.jp/bs/ifmf/

▶見慣れない XLL ファイル（Excel アドイン）を使う攻撃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/211005_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