アンラボ・セキュリティレター

Press Ahn

2022.5　Vol.101

繰り返される不正 Word 文書の配布、変化する攻撃手法

不正 Word 文書タイプに関する分析報告書

繰り返される不正 Word 文書の配布、変化する攻撃手法

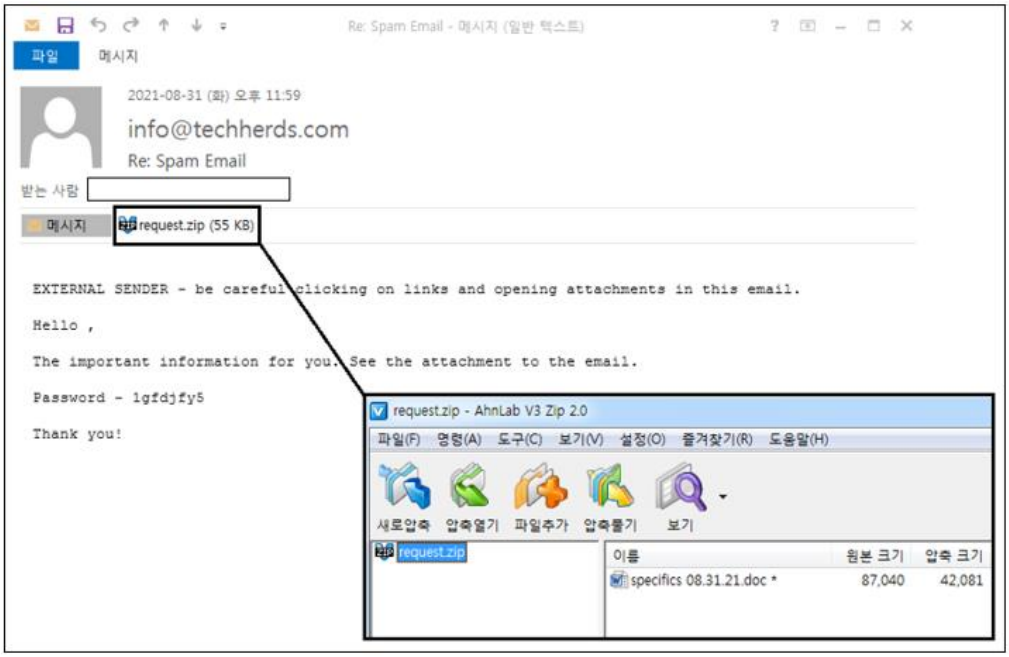
Word 文書は、最も多くのユーザーが使用するファイル形式のうちの一つである。これを悪用し、 Word 文書を利用した攻撃が収束することなく発生し続けている。 攻撃者は主に、フィッシングメールを介して不正な Word ファイルを配布し、ターゲットに応じて内容を変えたり、配布方式を進化させるなど、より巧妙な手口で攻撃を仕掛けてきている。

今回は、2021年から 2022年の初めにかけ、最も盛んに配布された不正な Word 文書のタイプと、その動作過程の変化に焦点を当てていく。

不正 Word 文書を利用した攻撃は、情報窃取等の悪意ある行為を行うため、ユーザーのシステムにマルウェアを配布することから始まる。この時配布されるマルウェアは、非常に多種多様なタイプや変形方式を有している。2021年から 2022年の初めにかけ、最も盛んに配布された不正 Word 文書は、TA551 (別名 Shathak) 攻撃グループが使用する Word 文書タイプであった。このタイプは、ここ最近ではなく以前よりその使用が確認されていた。しかし、ここで注目すべきは、2020年には同一タイプの Word 文書を介し、IcedID マルウェアのみが配布され続けていたのに対し、2021年からは IcedID、Qakbot、Trickbot、BazarLoader など、複数のマルウェアが配布されるようになったという点だ。ここで、TA551 グループが使用する Word 文書タイプ (以下 TA551 タイプ) の主な特徴を見てみよう。

不正 Word 文書：TA551 タイプの配布方式

不正な Word 文書ファイルのほとんどは、フィッシングメールに添付する形で、多数の企業ユーザーを対象に配布される。攻撃者は、特定ユーザーをターゲットにする場合、対象ユーザーに関連のある内容が含まれた本文、または Word ファイルを利用する。また、不特定多数のユーザーをターゲットにする場合、注文書や見積書などの一般的な内容が含まれた不正 Word 文書を利用することもある。このうち、TA551 グループの手口は後者にあたる。注文書に偽造した Word ファイルを暗号化し、ユーザーが添付された圧縮形式ファイルを実行するよう、メール本文に誘導文を記載する手法だ。 ([図1 参照])



[図1] 不正 Word 文書が添付されたフィッシングメール

2021年 6月以降に大量に発見された TA551 タイプの Word 文書は、変形を繰り返しながら配布されていた。変形の主な例として、マクロコードの形式変化、最終マルウェアのダウンロードプロセス増加、最終マルウェアの種類変形などが挙げられる。しかし、こうした変化の中でも、文書ファイル名やファイル内容の形式には目立った変化がなく、高い類似性を見せていた。

下記の [表1] は、2021年の間に配布された TA551 タイプの不正 Word 文書のうち、一部のファイル名をまとめたものである。TA551 タイプの Word 文書は、マクロが実行されると HTA ファイルをドロップした後、追加でマルウェアをダウンロードする流れで動作する。そのため、3 種類のファイルに関するファイル名を記載している。

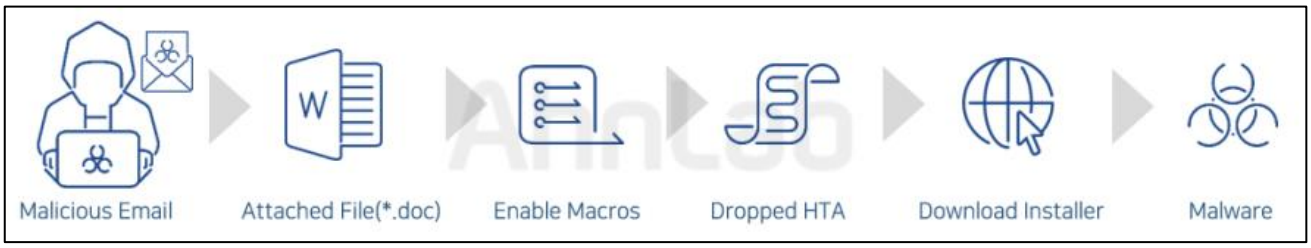
Attached File (*.doc)	Dropped HTA	Downloaded Malware
deed contract_06.21.doc	winSelBefore.hta	winSelBefore.jpg
charge, 06.28.2021.doc	dCurTable.hta	dCurTable.jpg
decree.06.28.2021.doc	doubleBorderInt.hta	doubleBorderInt.jpg
report-06.21.doc	repoRequestDocument.hta	repoRequestDocument.jpg
facts,06.21.doc	objectVarQuery.hta	objectVarQuery.jpg
report-09.21.doc	1.hta	docExObj.jpg

ordain_09.21.doc		divDocDev.jpg
direct 09.21.doc		winObj.jpg
adjure 09.21.doc		objWinDoc.jpg
commerce .08.21.doc		dirDirDrive.jpg
document-08.30.2021.doc		winEx.jpg
commerce -08.21.doc		devDevDiv.jpg
deed contract,09.21.doc		docDirObj.jpg
deed contract-09.21.doc		devDirWin.jpg

[表1] 配布ファイル名 (一部)

動作方式および特徴

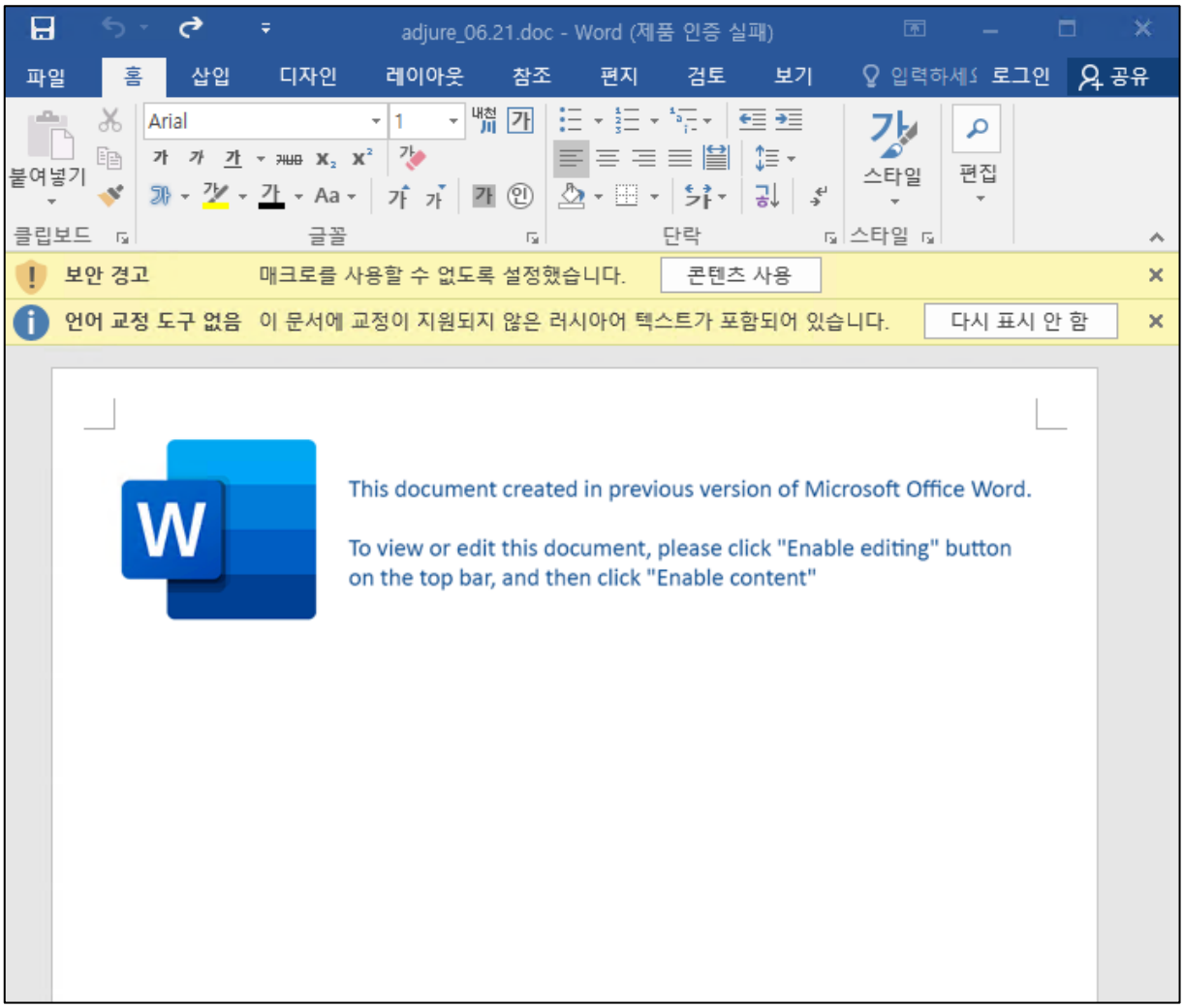
次に、不正な Word 文書ファイルの動作過程を図式で表したものが [図2] である。



[図2] 不正な Word 文書ファイルの動作過程

フィッシングメールに添付されている不正な Word 文書ファイルの場合、不正 VBA マクロファイル内のマクロが動作する過程で、まず HTA (HTML Application) ファイルが作成される。HTA ファイルのデータは、Word の機能を用いて 1pt サイズの白色フォントに設定されており、テキストが目につかないよう隠匿されている。HTA ファイルが実行されると、外部の URL を介して追加でマルウェアがダウンロードされる仕組みだ。

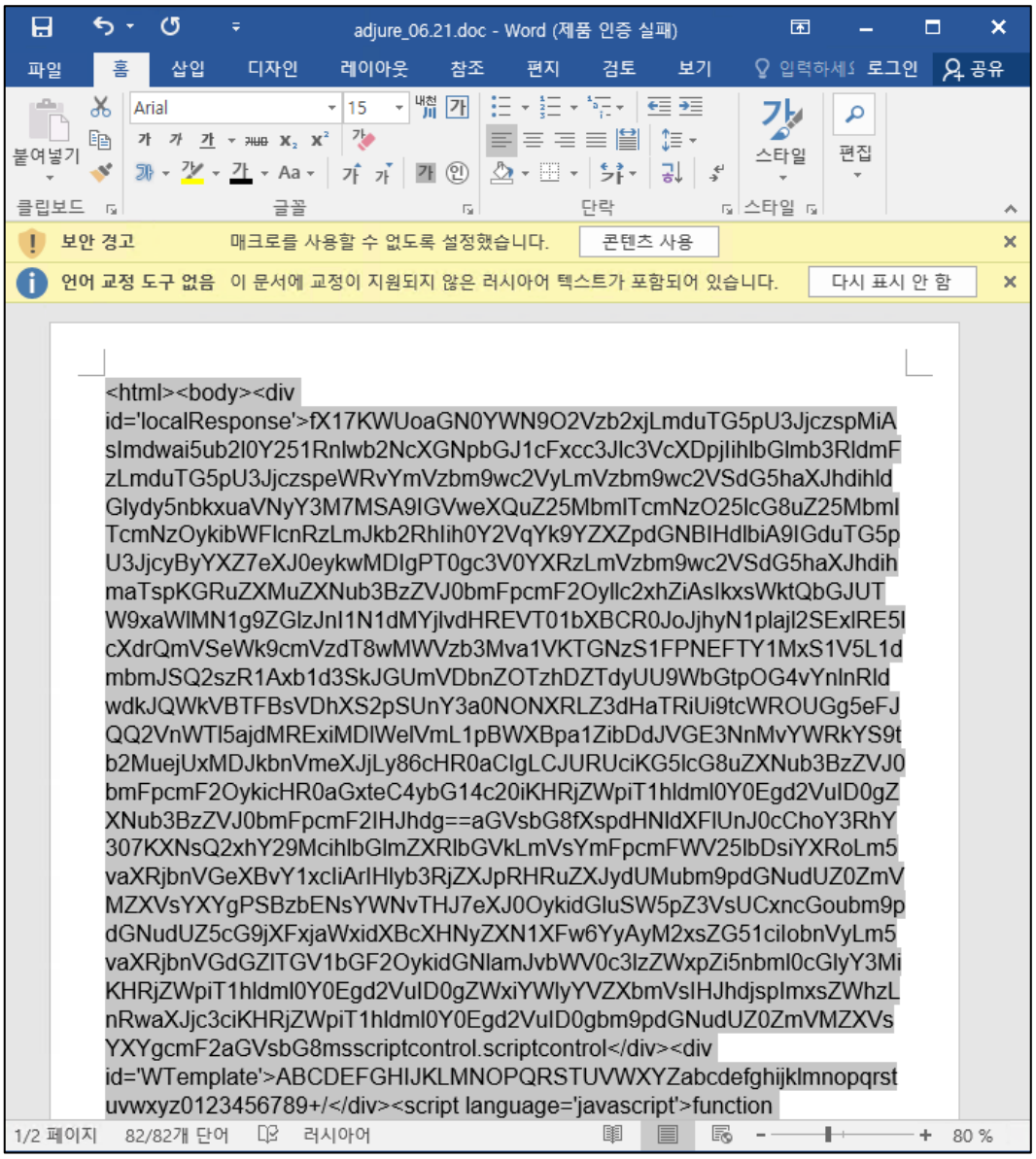
HTA ファイルは、インターネットブラウザ上のセキュリティポリシーによる影響を受けないため、信頼できないプログラムも実行することが可能だ。その上、パワーシェル (PowerShell) も利用できることから、攻撃者らはこの HTA ファイルを頻繁に悪用している。



[図3] TA551 タイプの Word ファイル本文

TA551 タイプの Word ファイルは、[図3] のように、マクロの有効化を誘導する画像を単独で挿入している点が主な特徴として挙げられる。2020年から確認されている TA551 タイプの Word ファイルのほとんどに、類似した画像が使われてきた。

マクロの有効化を誘導する画像ファイルを消してみると、白色フォントでデータが隠されていることが確認できる。フォント設定を変更すると、[図4] のように HTML のソースコードが表示される。このデータは、Word 文書内のマクロが動作した際、ローカル経路にダウンロードされる HTA ファイルの内容である。



[図4] 不正 Word ファイル内に隠された HTML ソースコード

マクロコードが動作すると、文書全体の内容をもとに HTA ファイルが作成され、その後 explorer.exe は mshta.exe を介し、この HTA ファイルを実行する。

[図5] RAPIT (マルウェア自動分析インフラ) のプロセスツリー

アンラボの RAPIT インフラからプロセスツリー (工程順序) を確認してみると、mshta.exe プロセスによる HTA ファイルの実行後、「jpg 拡張子ファイル」がダウンロードされ、rundll32.exe にロードすることで実行に及んでいることがわかる。実際は、HTA スクリプトの実行によりアクセスする URL から DLL 実行ファイル (Portable Executable) がダウンロードされるのだが、その際「.dll 拡張子」

を直接使用せず、「jpg 拡張子」を使用していることが確認できた。

これは、実行ファイルをダウンロードする際に、疑わしい行為として遮断されないための措置であると推測できる。こうした手法は、TA551 タイプの Word 文書に共通して用いられていた。

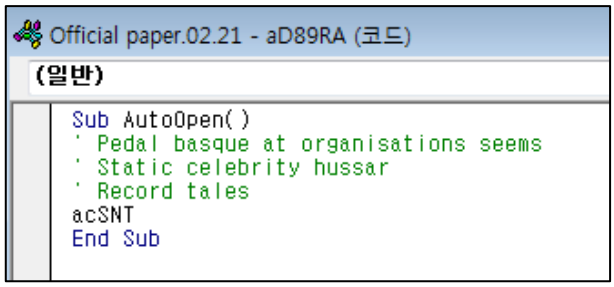
動作方式の変化

前述した不正 Word 文書を大きな枠組みで見た場合、動作過程にそれほど顕著な変化はない。しかし、マクロの動作過程には 2 種類の変形があることがわかった。それは、「VBA マクロコードおよび HTA ファイルの変形」と、「配布段階の拡張による最終マルウェアの種類の変化」である。

中でも、VBA マクロコードの形式は、これまでも頻繁に変形していることが確認されている。HTA ファイルのデータ自体が、Word 本文ではなく VBA マクロ内に存在する事例も報告されている。また、HTA ファイルの作成過程を飛ばし、Installer DLL のダウンロードに即座に移るケースもあった。ここからは、これまで配布されてきた TA551 タイプの Word ファイルのうち、確認できた変形タイプを 1 つずつ見ていこう。

1. VBA マクロコードおよび HTA ファイルの変形

2021年の初めに配布された不正 Word 文書を調査してみると、攻撃者は VBA マクロコードのユーザー定義フォームを悪用していた。これは、Word 本文内のデータを利用し、HTA ファイルを作成していた従来の方式とは多少異なる。



[図6] 2021年 2月に配布された不正 VBA コード

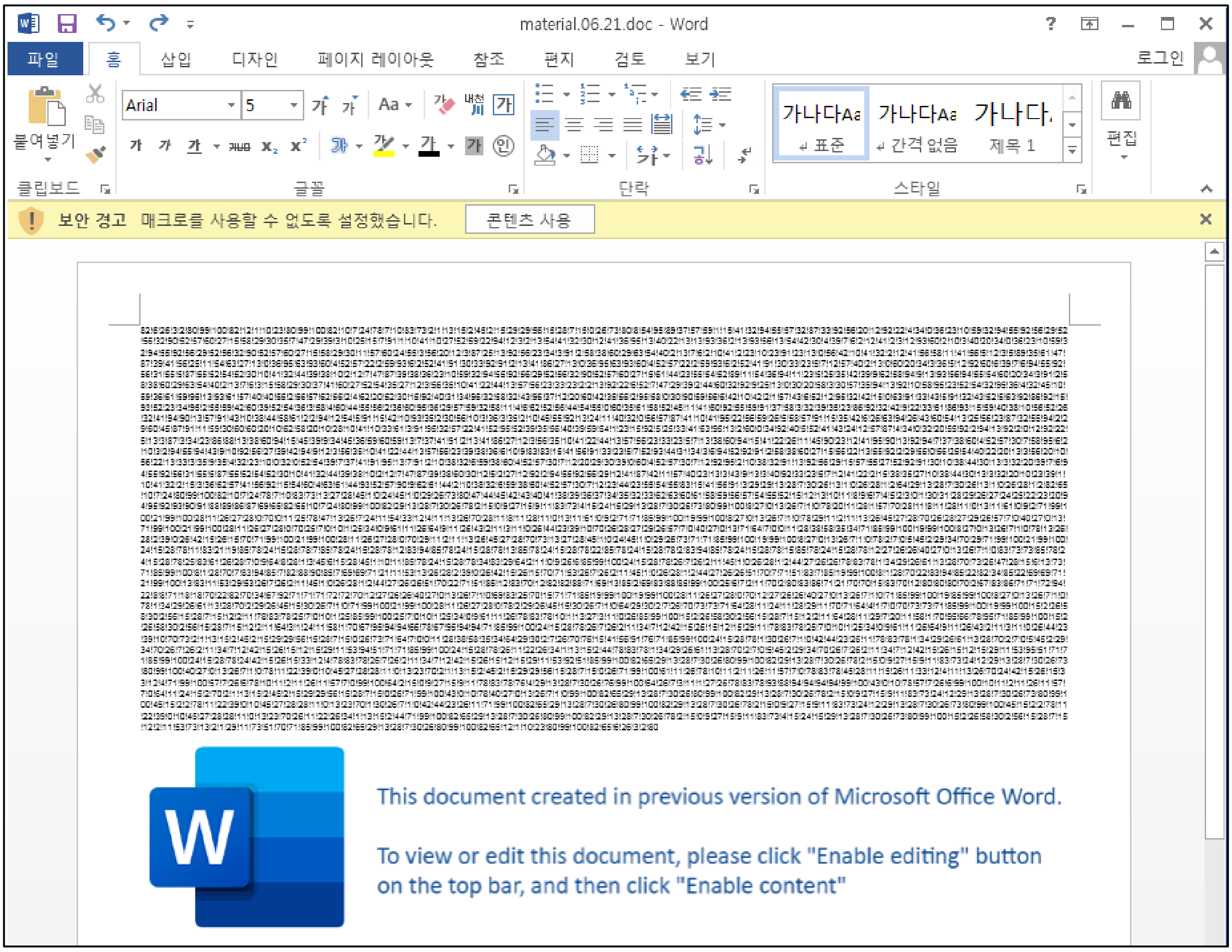
また、編集設定に制限がかけられていたことも、従来の方式とは異なる点である。これは、「マクロ有効化の誘導画像」が挿入された画像であることに気づかれにくくするため、意図的に制限したものと推測される。

全般的なエンコード過程に関しては、難読化などの複雑な手法は使われていなかった。攻撃者は基本的に、VBA マクロコードのユーザー定義フォームやモジュールを利用しており、それぞれに含まれるデータに対し、XOR 演算と ASCII コードの変換方式を主に使用していた。しかし、時期によって VBA マクロコードに使用可能な複数のエンコード方式が交互に使用されたり、また以前の手法と混用するケースなどもあり、それぞれ TA551 タイプの特徴が現れていた。これは、攻撃者がアンチウイルス製品による検知を迂回するため、配布時期によって継続的に変形を加えていたものと推測できる。

2021年 3月に確認された不正 Word 文書は、Ursnif マルウェアを配布するため、HTA データが VBA コード内に存在するタイプである。特定関数を用い、HTA ファイルに含まれるデータを配列形式で保存していた。しかし、この時期に配布された Word ファイルは、誤って作成されたマクロコードにより正常に実行しなかった。

2021年 7月に配布された不正 Word 文書は、難読化した HTA データが用いられていた。本文内のデータがエンコードされており、マクロコードも基本的な演算を経てデコードされるよう製作されていた。関連データは、[図7] のように、マクロの有効化を誘導する画像の

後ろに隠されている。



[図 7] マクロ有効化を誘導する画像の後ろに隠されたテキスト

マクロコードの動作過程で作成された HTA ファイル内のデータを、コード内容の意図通りにデコードする際、追加でマルウェアのダウンロード URL と、ローカル保存経路などが明示される。配布過程で確認されたサンプルを追跡調査してみると、「http://[ドメイン]/adda/~」のような方式で、path の最初のコードがかなりの長期間、統一性を保って維持していることが判明した。また、ダウンロードされる DLL ファイルは、2021年 7月当時、Trickbot マルウェアとして動作していたことも確認されている。

この他にも、こうした動作過程で、マクロのセキュリティ設定を変更するため、HTA ファイルを作成せずにレジストリキーを登録し、VBA コードを直接実行するタイプも報告されている。

上記で述べた不正 VBA マクロタイプ以外にも、多数の変形ファイルが存在する可能性もある。従来のエンコードとデータ隠匿方式を混用するケースもあり、より複雑な形に変化し続けていることが確認できる。

2. 最終段階で配布されるマルウェア種類の変化

2020年下半期に確認された TA551 タイプの Word ファイルは、主に IcedID と Qakbot マルウェアを配布していた。しかし、2021年下半期を過ぎた辺りから、配布されるマルウェアの種類が増加した。その上、マルウェアを直接配布していた手口から、様々な段階を経てマルウェアをダウンロードする手法へと変化していった。

2021年上半期までに収集された TA551 タイプの Word ファイルは、HTA スクリプトコードにエンコードされている URL を介し、マルウェアを直接ダウンロードしていた。当時、主にダウンロードされていたマルウェアは、Qakbot、Bokbot、Ursnif、Trickbot などのバンキング型マルウェアだった。

さらに、Word のマクロ動作過程にて、2 種類のマルウェアがダウンロードされる事例も多数報告されている。

[図8] マルウェアの追加ダウンロード過程

2021年 9月に確認された TA551 タイプは、HTA スクリプトコードにエンコードされている URL を介し、BazarLoader DLL ファイルをダウンロードしていた。BazarLoader DLL とは、メモリ上で backdoor (バックドア) をダウンロードし、正常なプロセスにインジェクションするマルウェアである。その後、C2 にアクセスすることで Trickbot のようなマルウェアも追加でダウンロードしていた。

またアンラボは、TA551 や Kimsuky タイプ以外にも、外部 (External) とのアクセス機能を悪用した不正 Word 文書や、Emotet マルウェアを配布する不正 Word 文書タイプも確認している。

結論

攻撃者は、以前より不正 Word 文書を利用した攻撃を仕掛け続けている。アンラボは今回、TA551 攻撃グループが使用する 不正 Word 文書の動作過程と、主な特徴に焦点を当て整理した。こうした脅威は、Word ファイルだけに限らず、多種多様なタイプの不正 Word 文書を用い、絶えず変形を加えながら配布されているため、格別の注意が求められる。

不正 Word 文書は、そのほとんどがメールを介して配布されている。従って、ユーザーは出所不明のメールを閲覧する際、警戒を怠ってはならない。また、V3 をはじめとするセキュリティ製品のアップデートを最新状態に保ち、マルウェアへの感染を事前に遮断できるよう注意を払う必要がある。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)