悪意のある OneNote
サンプルのペイロードの傾向

概要

本稿は、攻撃者らが Microsoft OneNote
ファイルを悪用するさいに使う埋め込みペイロードの種類について取り上げます。私たちが WildFire から得た約 6,000 件の悪質な OneNote
サンプルを分析したところ、これらのサンプルにはフィッシングに似たテーマが存在することが明らかになりました。これらのサンプルでは、攻撃者らが、1 つ以上の画像を使ってユーザーに OneNote
ファイルをクリックまたは操作させようとします。その後、そうしたやり取りが埋め込まれた悪意のあるペイロードを実行します。

Office ではマクロがデフォルトで無効になっていますので、攻撃者らはほかの Microsoft
製品を使って悪意のあるペイロードを埋め込むようになってきました。この結果、悪意のある OneNote
ファイルの人気が高まっています。OneNote のデスクトップ アプリは Windows では Office 2019 および Microsoft 365
にデフォルトで含まれています。このため、誰かがうっかり OneNote ファイルを開くと、悪意のある OneNote
ファイルが読み込まれてしまうおそれがあります。

私たちは、攻撃者らが OneNote 内にテキストベースの悪意のあるスクリプトやバイナリー
ファイルを自由に埋め込めることを確認しました。これにより、従来のドキュメント内マクロに比べた柔軟性が高まります。

パロアルトネットワークスのお客さまは、以下の製品を通じて、上記の脅威からより強力に保護されています。

- WildFire を含むクラウド配信セキュリティサービスを有効にした次世代ファイアウォール
- WildFire を含むクラウド配信セキュリティ サービスを有効にした Prisma Access デバイス

- Cortex XDR および Cortex XSIAM
  エージェントは多層保護のアプローチにより、エクスプロイト後のアクティビティからの保護に役立ちます。
- Unit 42 のインシデント レスポンス チーム
  も、侵害を受けた場合の支援や、お客さまのリスク低減のための事前サイバーセキュリティ準備状況評価を行っています。

関連する Unit 42 のトピック	**Microsoft**, **Phishing**

背景

Microsoft OneNote は Microsoft Office スイートに含まれるデジタル ノートブックのアプリケーションです。OneNote ファイルにはメモを取るほかにもさまざまな種類の情報を保存することができます。

Microsoft OneNote には外部ファイルを埋め込むこともでき、ビデオや画像、さらにはスクリプトや実行可能ファイルなどのファイルも格納できます。ただし、Microsoft は特定の拡張子を持つ埋め込みオブジェクトのブロックを開始しています。このブロックの対象となるのは、Windows の Microsoft 365 上で実行されている OneNote ファイル内にあると危険と見なされる拡張子です。

それでも、攻撃者が悪意のあるペイロードを埋め込んで、オブジェクトを埋め込み機能を悪用することはよくあります。悪意のある OneNote サンプルは通常、画像やボタンを含む正当なノートのふりをします。

攻撃者らは画像でユーザーの注意を引き、それと知らずにボタンをクリックして悪意のあるペイロードを起動するのを待っています。ユーザーが正規ノート作成アプリケーションに寄せる信頼を逆手にとれることから、この手法はペイロード配信によく使われています。

図 1～3 は、さまざまな種類の埋め込み画像やボタンをもつ 3 種類の悪意のある OneNote サンプルを示しています。偽のボタンの上にマウス オーバーすると、OneNote ファイルに埋め込まれたペイロードの場所や種類を確認できます。

図 1 では、悪意のある OneNote サンプルが被害者に対し「保護されたドキュメントを表示するには [View] ボタンをクリックしてください」と要求しています。クリックすると悪意のある VBScript ファイルが実行されます。

画像 1 は、内容の一部をモザイクで処理してある Microsoft OneNote ページのスクリーンショットです。
Image not found or type unknown
図 1. 悪意のある VBS が埋め込まれた OneNote サンプル

同様に、図 2 と図 3 も偽のボタンを含む悪意のある OneNote ドキュメントを示したものです。それぞれ、埋め込まれた EXE ペイロードや Office 97-2003 ペイロードを被害者が実行するように仕向けています。

画像 2 は Microsoft OneNote のスクリーンショットです。青色の「CLICK TO VIEW DOCUMENT (クリック
Image not found or type unknown
図 2. 悪意のある EXE ファイルが埋め込まれた OneNote サンプル

画像 3 は、内容の一部をモザイクで処理してある Microsoft OneNote ページのスクリーンショットです。
Image not found or type unknown
図 3. 悪意のある Office 97-2003 ファイルが埋め込まれた OneNote サンプル

方法論

前述のように、攻撃者は主に OneNote ファイルを悪意のあるペイロードの配信に悪用します。これを行うにあたり、彼らは次のような特定のペイロードの種類をいくつか埋め込む傾向があります。

- JavaScript
- VBScript
- PowerShell
- HTML アプリケーション (HTA)

ファイルの種類こそ異なりますが、これらのペイロードは多くの場合、似たような振る舞いを呈し、似たような悪意のある目標の達成を狙っています。ただし、攻撃の全体像や感染チェーンについてはすでに悪意のある OneNote 添付ファイル についての記事で取り上げているので、ここで詳しくは触れません。

悪意のある OneNote ファイルであることを示す明らかな兆候は、埋め込みオブジェクトの存在です。無害な OneNote ファイルにも埋め込みオブジェクトが含まれる場合はありますが、悪意のある OneNote ファイルの場合、ほぼ必ずといってよいほど埋め込みオブジェクトが含まれています。

Microsoft によると、OneNote に埋め込まれたファイルは、特定のグローバル一意識別子 (GUID) タグで始まります。

- {BDE316E7-2665-4511-A4C4-8D4D0B7A9EAC}

この GUID は、FileDataStoreObject オブジェクトの存在を示しています。この GUID

の後ろには、埋め込まれたファイルのサイズが続きます。

実際の埋め込みファイルは、前述の GUID タグの 20

バイト後から始まり、定義されたサイズと同じ長さを持ちます。その例を下の図 4 に示します。

- 1 つめの赤い四角形は埋め込みオブジェクトの GUID タグを表しています。
- 2 つめの赤い四角形は、埋め込まれたオブジェクトのサイズを示しています。
- 3 つめの赤い四角形は、実際の埋め込みオブジェクトを表しています。

画像 4 は、OneNote ファイルに埋め込まれたオブジェクトです。3 つの異なる領域を赤でかこって強調表
Image not found or type unknown
図 4. OneNote ファイル内の埋め込みオブジェクトの識別

ペイロードの種類と平均サイズの分布

図 5 に示すように、攻撃者は主に次の 7 種類のファイルを OneNote ペイロードに使います。

- PowerShell
- VBScript
- Batch
- HTA
- Office 97-2003
- EXE
- JavaScript (このファイルタイプが最もよく使われる)

画像 5 は、悪意のあるファイル内のペイロードの種類を示す円グラフです。最も多いのは JavaScript で
Image not found or type unknown
図 5. 悪意のある OneNote ファイルに埋め込まれたペイロードの種類の分布

図 6 に示すように、私たちは各ペイロードの種類のサイズも抽出して記録しました。

図 6 は、ペイロードの種類の分布をサイズ別に示した棒グラフです。EXE のサイズが 1,000 KB を超えてお
Image not found or type unknown
図 6. 悪意のある OneNote
サンプル内で見つかったペイロードの平均サイズ。ペイロードの種類別にグループ
化したもの

EXE や Office 97-2003 などの大きなバイナリー埋め込みペイロードの方が高機能ですが、OneNote
サンプルの全体サイズが大きくなることから、攻撃者にはあまり使われない傾向があります (図 5 参照)。攻撃者は、ファイル
サイズ全体が小さいことを好む傾向があります。マルウェアのサイズが小さいほど電子メールの添付ファイルなどの一般的なマル
ウェア配信メカニズムに組み込みやすくなりますし、疑われにくくもなるためです。

上の図 6 に示すように、埋め込まれた悪意のある EXE ファイルと Office 97-2003
ファイルのペイロードは大きくなる傾向があり、埋め込まれた悪意のある HTA ファイルと JavaScript
ファイルは小さくなる傾向があります。

悪意のある OneNote サンプルでの画像の存在

悪意のある OneNote
ルアーを作成する攻撃者は、ボタンのように見える画像を使って、ユーザーをだまして有害なペイロードを起動させます。私たち
は悪意のある OneNote サンプルごとにペイロードの種類別に画像数をマッピングし、画像数の中央値を計算しました。

データセット内の 6,000 個のサンプルを分析したところ、悪意のある OneNote サンプルのうち 3 つを除くすべて (99.9%)
に、少なくとも 1 つの画像が含まれていることがわかりました。ほぼすべてのサンプルに少なくとも 1
つの画像が含まれているということで、OneNote
のサンプルは主にフィッシングの手段として使われているという仮説を確認できます。

図 7 は、ペイロードの種類ごとの画像数の中央値が 2
であることを示しています。たとえば攻撃者は、偽のボタンに加えて偽の「安全な」ドキュメント
バナーなどの目をひく画像を使い、フィッシング キャンペーンの信憑性を高めることができます (図 3 など)。

画像 7 は、さまざまなペイロードの種類ごとの画像数の中央値を示す棒グラフです。JavaScript、Power
Image not found or type unknown
図 7. OneNote
マルウェアに埋め込まれたさまざまなペイロードの種類の画像数の中央値をペイロ

ードの種類別にグループ化したもの

上のグラフは、悪意のある OneNote サンプルのペイロードには通常 2 ～ 3
枚の画像が含まれていて、一部はドキュメントの信憑性を高める用途に、一部は偽ボタンとして使われていることを示しています
。

埋め込まれた EXE ペイロードの分析

私たちはこれまでの研究で PowerShell や HTA など、より一般的で人気のあるペイロードの種類を含む OneNote
サンプルを調査してきましたが、EXE のペイロードにはあまり注目を払っていませんでした。そこで本セクションでは、EXE
のペイロードが埋め込まれた OneNote サンプルを分析したいと思います。

以下のペイロードは、次の SHA256 ハッシュを持つ OneNote サンプルから抽出されたものです。

- `d48bcca19522af9e11d5ce8890fe0b8daa01f93c95e6a338528892e152a4f63c`

このペイロード自体は次の SHA256 ハッシュを持っています。

- `92d057720eab41e9c6bb684e834da632ff3d79b1d42e027e761d21967291ca50`

図 8 は、この EXE ペイロードを IDA Pro
で分析した結果を示したものです。この中にはいくつかのコードブロックが見つかりました。これは多くの場合、ここで相手にし
ているのがシェルコードであることを示します。

私たちの仮説は、プロセス環境ブロック (PEB) と右回転 (ROR) 命令を指し示す GS:60
の存在によって確認されました。これは、このマルウェアが関数に動的アドレス解決を使い、関数識別にハッシュを使っている
ことを示しています。

画像 8 は、EXE ペイロードを逆アセンブラーの IDA Pro で開いた図です。赤い四角形は、アーキテクチャ
Image not found or type unknown
図 8. EXE ペイロードを IDA で開いたところ

このシェルコードの目的を理解し、動的にロードしていたライブラリーを識別するため、私たちは x64dbg
デバッガーでこれを開きました。次に、ループ内で `loc_140004021`
という関数ブロックを繰り返し呼び出している関数にブレークポイントを設定します (図 9)。

画像 9 は、動的にロードされた関数を強調表示しているスクリーンショットです。青い矢印が灰色でハイ
Image not found or type unknown

図 9. 動的にロードされた関数を識別するためにブレークポイントを設定したところ

これにより、`WSAStringToAddressA` 関数 (図 10 参照) と `WSASocketW` 関数 (図 11 参照)
を組み合わせて、このシェルコードがネットワーク ソケットを確立し、データ送受信を試みていることが明らかになります。

画像 10 は、RSI レジスターで強調表示された記録された関数 WSAStringToAddressA のスクリーンショッ
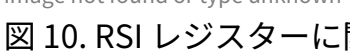
図 10. RSI レジスターに関数名 `WSAStringToAddressA` が記録されている

画像 11 は、RSI レジスターで強調表示された、記録された関数 WSASpclertW のスクリーンショットです

図 11. RSI レジスターに関数名 `WSASpclertW` が記録されている

攻撃者のマシンへの接続に最もよく使われる種類のシェルコードはリバース TCP シェルです。そこで私たちは、`ws2_32.dll`
内にブレークポイントを設定して (図 12 参照)、connect
関数が呼び出されるかどうかを判断することにしました。もしそうなら、この関数に渡される引数を抽出できます。これらの引数
には、ペイロードが接続を試みる IP アドレスやポート番号が含まれることがよくあります。

画像 12 は、ws2_32.dll のブレークポイントのスクリーンショットです。左ペインの行が灰色でハイライ

図 12. `ws2_32.dll`の関数 connect にブレークポイントを設定

予想した通り、このシェルコードは connect 関数の呼び出しで停止しました。RDX レジスターの値をダンプすると、
`sockaddr_in` 構造体の内容を識別できました (図 13)。

画像 13 は sockaddr_in の内容のスクリーンショットです。スクリーンショットの左下には赤い四角のハ

図 13. `sockaddr_in` 構造体の内容をダンプしたところ

次に私たちは、Python スクリプトを書き、上記で特定した `sockaddr_in` 構造体の内容をアンパックしました (図 14)。

画像 14 は、sockaddr_in の内容をアンパックする Python コードのスクリーンショットです。

図 14. `sockaddr_in` 構造体の内容を解凍する Python スクリプト

上記の Python スクリプトを実行すると、図 15 に示した出力が得られます。ここからは、攻撃者がポート番号 4444 でローカル
マシン (攻撃者がコントロールしているマシンの可能性あり) に接続していることがわかります。

画像 15 は、IP アドレスとポート (画像の 2 行目と 3 行目) を含む Python スクリプトの実行結果のスクリ


図 15. このペイロードが接続している IP
アドレスとポート

結論

私たちは、攻撃ベクトルとしての OneNote
は、当初考えていたよりも汎用性が高いという結論に達しました。スクリプトベースのダウンローダーに加え、実行可能形式のペイロードを含めることもできますし、ほかの多くのファイル タイプと同様にラテラルムーブにも使えます。

OneNote ファイル内に悪意のあるペイロードを埋め込む場合、攻撃者は主に JavaScript、PowerShell、Batch、VBScript
を利用しますが、実行可能ファイルや Office 97-2003 ファイルなどのバイナリー ペイロードを目的達成に使うこともあります。

こうした攻撃からユーザーを保護するため、組織側は OneNote
ファイル内に埋め込まれた危険な拡張子を持つペイロードのブロックを検討してもよいでしょう。さらに言うなら、クリックする前にボタンや画像を上にマウスオーバーしてみて、OneNote ファイルに埋め込まれたペイロード
ファイル名や拡張子を確認し、リスクを抑えることをユーザーの皆さんにはお勧めします。

パロアルトネットワークスのお客さまは、以下の製品を通じて、上記の脅威からより強力に保護されています。

- WildFire を含むクラウド配信セキュリティサービスを有効にした次世代ファイアウォール
- WildFire を含むクラウド配信セキュリティ サービスを有効にした Prisma Access デバイス
- Cortex XDR および Cortex XSIAM
  エージェントは多層保護のアプローチにより、エクスプロイト後のアクティビティからの保護に役立ちます。
- Unit 42 のインシデント レスポンス チーム
  も、侵害を受けた場合の支援や、お客さまのリスク低減のための事前サイバーセキュリティ準備状況評価を行っています。

IoC (侵害指標)

以下は、本校の調査中に発見された OneNote ファイルとペイロードのファイル ハッシュを含む Github
リポジトリへのリンクです。

- 悪意のある OneNote ファイルとペイロードの 11,226 個の SHA256 ハッシュ – GitHub
- OneNote ファイルの SHA256 ハッシュとペイロードの SHA256 ハッシュの対応 – GitHub

追加リソース

- The Adventures of Malicious OneNote Attachments in Cortex XDR Land – パロアルトネットワークス Unit 42
- Microsoft OneNote File Format – Microsoft