2018 年 11 月 21 日

サービス＆セキュリティ株式会社 e-Gate センター

マクロレスファイルを用いた最新の攻撃手法

1 概要

様々なサイバー攻撃手法が日々生み出されている現在でも、攻撃者によって最もよく利用される侵入手口はメールを通じて Windows ユーザをマルウェアに感染させる手法です。IPA の選出する「情報セキュリティ 10 大脅威 2018 組織編」における第 1 位はここ数年「標的型攻撃」関連であり、その主な攻撃のきっかけはメールと言われています。

この時、攻撃者の狙いは主に以下の 2 つです。

- メール内のリンクをクリックさせ、マルウェア本体もしくはそのダウンローダーをダウンロードさせる。
- 添付した Word 文書や Excel ファイルなどに不正なコンテンツやマクロを埋め込み、それを実行させる。

一方で、通常マルウェアをダウンロード及び実行させるためには、ユーザの注意を潜り抜け、「マクロの有効化」といったいくつかの警告メッセージを許可させる必要があります。しかし、明らかに不自然な日本語で書かれたメールや、".exe"など典型的な怪しい拡張子のファイルは開かないという方も多いでしょう。

よって、攻撃者は見慣れない拡張子のファイルを利用するなど、ユーザをマルウェアに感染させるために様々な工夫を凝らしています。中でも、最近発見されたマクロ機能を使用しない(マクロレスな)手法は、警告メッセージが表示されない分ユーザが攻撃と気づかない可能性が高いため、特に注意が必要です。

今回は、マクロ実行の許可を必要としない最新の攻撃手法と、今年確認されているその他の攻撃例や悪用されやすい拡張子についてご紹介いたします。

2 マクロレスファイルを用いた最新の攻撃手法：「オンラインビデオの挿入」の利用

2.1 概要

10 月下旬、 Cymulate のセキュリティ研究チームによって、Word 文書のオンラインビデオ埋め込み機能を利用した手法が発見されました。本機能は、通常であれば YouTube などの動画を Word 文書内に埋め込むものですが、これを悪用することで、動画再生の代わりに攻撃者の任意の html や javascript を実行させることが可能となります。

注意すべき点として、この手法はマクロ機能を使用していないため「コンテンツの有効化」といった警告メッセージが表示されません。 すでに本機能を悪用した検体が確認されていますが、本記事掲載時点において Microsoft による対応の予定はないため、十分な注意が必要です。

【図 1】埋め込み動画（https://www.youtube.com/watch?v=ijD_ua13Vsc）の再生画面

2.2　攻撃の仕組み

“.docx” ファイルは実際にはテキストや書式設定などの各ファイルを圧縮した状態で保存されています。よって Word 文書をファイル解凍ツールで展開すると、通常の XML 形式のファイル等から構成されている様子を見ることができます。

展開後、word フォルダ内の document.xml を開くと、動画が含まれた iframe 要素を持つ embeddedHtml パラメータを確認することができます。

```
<a:extLst><a:ext uri="{28A0092B-C50C-407E-A947-70E740481C1C}"><a14:useLocalDpi
xmlns:a14="http://schemas.microsoft.com/office/drawing/2010/main" val="0"/></a:ext><a:ext uri="{C809E66F-F1BF-
436E-b5F7-EEA9579F0CBA}"><wp15:webVideoPr
xmlns:wp15="http://schemas.microsoft.com/office/word/2012/wordprocessingDrawing" embeddedHtml="&lt;iframe
id=&quot;ytplayer&quot; src=&quot;https://www.youtube.com/embed/ijD_ua13Vsc&quot; frameborder=&quot;0&quot;
type=&quot;text/html&quot; width=&quot;816&quot; height=&quot;480&quot; /&gt;" h="480" w="816"/></a:ext>
</a:extLst></a:blip><a:stretch><a:fillRect/></a:stretch></pic:blipFill><pic:spPr><a:xfrm><a:off x="0" y="0"/>
<a:ext cx="4572000" cy="3429000"/></a:xfrm><a:prstGeom prst="rect"><a:avLst/></a:prstGeom></pic:spPr></pic:pic>
```

【図 2】document.xml 内の embeddedHtml パラメータ

この iframe 要素を任意の html/javascript に書き換えることで、動画を再生しようとクリックしたユーザの環境で警告メッセージ無しにコードが実行されます。ここから攻撃者の用意した Web サイトにアクセスさせるなど、様々な悪用方法が考えられます。

【図 3】embeddedHtml パラメータ変更後の再生画面(変化が分かりやすいよう、Button を表示させています)

3 その他の攻撃例の紹介

3.1 ".lnk" ファイルや ".rtf" ファイルの利用：ファイルレスマルウェア

ファイルレスマルウェアは、昨年から流行しているマルウェア感染手法です。主に ".lnk" ファイルや ".rtf" ファイルを実行させることで、そこに埋め込まれたマクロから Windows の PowerShell コードを実行させます。

Windows の標準機能である PowerShell を用いているので従来のセキュリティ製品では検知されにくい特徴があります。

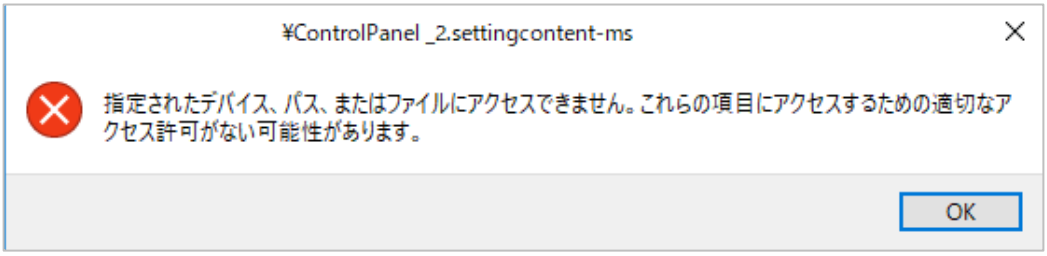
以前に弊社のグループ企業であるセキュアソフトのセキュリティニュースにおいて取り上げておりますので、詳しくはそちらをご参照ください。 https://www.securesoft.co.jp/news_mt/docs/TR17-12_20171129.pdf

3.2 ".SettingContent-ms" ファイルの利用

今年の 7 月、 ".SettingContent-ms" というファイル拡張子を利用した攻撃が可能であることが話題となりました。

".SettingContent-ms" ファイルは「設定」ページへのショートカットを作成する目的で使用されますが、中身の XML 形式のファイルを書き換えることで任意の PowerShell の実行などが可能になります。攻撃者は細工を施した当該ファイルを Word 文書に埋め込むなどして、マルウェアのダウンロードおよび実行を企図します。この攻撃はマクロ機能を使用していない点が特徴です。

なお、当該脆弱性（CVE-2018-8414）は Microsoft より更新プログラムが公開されており、Windows Update を実施している場合は正規のフォルダ以外から ".SettingContent-ms" ファイルを実行することができなくなっています。



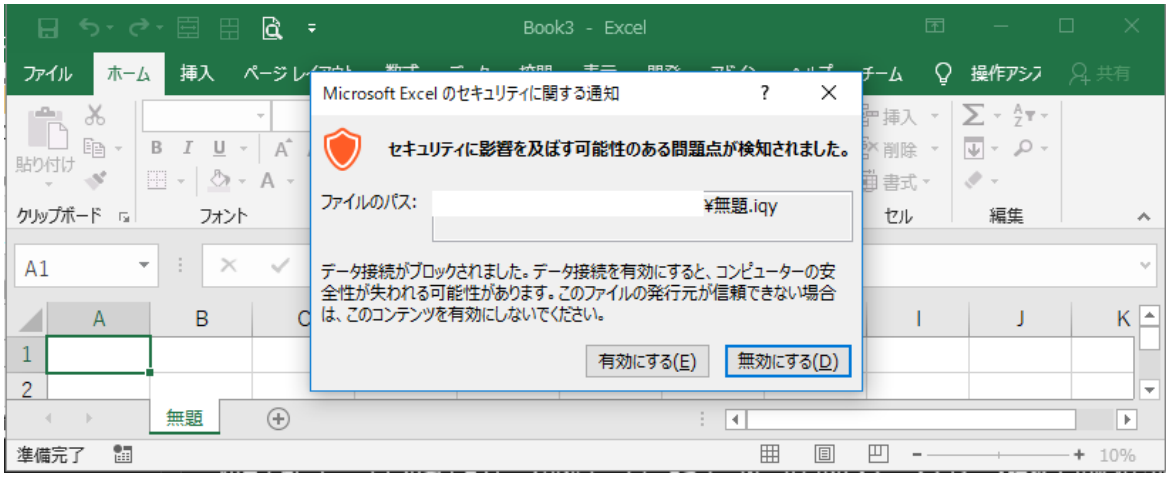
【図 4】正規のフォルダ以外から ".SettingContent-ms" ファイルを実行した際に表示されるエラーメッセージ

3.3 ".iqy" ファイルの利用

今年の 8 月には、".iqy" ファイルが添付された不審なメールが国内で確認されました。".iqy" ファイルは Microsoft Office クエリファイルのことで、Web サイトから Excel にデータを取り込む機能を持っています。

攻撃者はこのファイルを悪用し、ユーザが開くと Excel が起動し、マルウェアのダウンロードが行われるよう細工を施します。

なお、".iqy" ファイルを開く際と、コマンドプロンプト実行時の二回にわたり警告メッセージが表示されるため、気を付けていれば感染に至ることはありません。一方で、".iqy" ファイルでは「保護ビュー」が機能しないため、その点は注意が必要です。



【図 5】".iqy" ファイルを開いた際に表示されるメッセージ

また、拡張子 ".slk"のファイルにおいても「保護ビュー」を経ずに Excel を起動させる同様の手法が確認されています。

3.4 ".com" ファイルの利用

Cofense によると、10 月から拡張子 ".com" のファイルを使用したフィッシングメールが増加傾向にあると言います。 ".com" は MS-DOS において実行ファイルとして利用されていた拡張子の 1 つであり、互換性のため現在の Windows でも起動が可能となっています。ドメインで使用される ".com" (commercial) とは無関係のため、実行してしまわないようにしましょう。

4 共通する対策

- 不審なメールの添付ファイルは開かない。
- OS やアプリケーション、セキュリティ製品を常に最新の状態にする。
- 信頼できないメールに添付された Word 文書や Excel ファイルを開いた際、「保護ビュー」で閲覧する。
- マクロに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。
- 身に覚えのない警告メッセージが表示された際、警告の意味が分からない場合は操作を中断する。
- 本記事で紹介したような “.rtf” や” .iqy” といった拡張子ファイルを通常業務で使用しない場合、Word や Excel のセキュリティ機能でファイル制限をかけておく。

なお、このような対策を行っていたとしても、今後新たな手法が発見されたりメールや添付ファイルの文章が巧妙であったりする場合には、感染を許してしまうケースは発生するでしょう。

その際にマルウェアを検知・防御できるよう最新鋭のセキュリティ製品を導入し、適切に運用するとともに、いち早く感染に気付けるような監視体制を徹底しておくことが肝要です。

5 e-Gate の活用について

サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。SSK の総合セキュリティサービス「e-Gate」では、最新の分析システムを活用し精度の高い検知、また専任のアナリストによる分析を行っております。「e-Gate」のセキュリティ監視サービスをご活用頂くことにより迅速なセキュリティインシデント対応が可能となります。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター”この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

6 参考情報

- 独立行政法人情報処理推進機構（IPA）
  情報セキュリティ 10 大脅威 2018 組織編
  https://www.ipa.go.jp/files/000066223.pdf
  【参考資料】IQY ファイルを悪用する攻撃手口に関する注意点
  https://www.ipa.go.jp/files/000068065.pdf

- Cymulate
  Abusing Microsoft Office Online Video
  https://blog.cymulate.com/abusing-microsoft-office-online-video

- Microsoft
  CVE-2018-8414 | Windows Shell のリモートでコードが実行される脆弱性
  https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2018-8414/
  ※上記 URL の閲覧には利用規約への同意が必要です

- Cofense
  Phishing Emails with .COM Extensions Are Hitting Finance Departments
  https://cofense.com/phishing-emails-com-extensions-hitting-finance-departments/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp