June 2017

## イントロダクション

Petya ランサムウェアの最新の猛威により、6 月 27 日以降、広範な産業分野に渡ってかなりの数の組織が影響を受けている。ウクライナの複数施設、スペイン、オランダ、イギリスなど、多くの被害組織が公開情報で確認されている。この被害は、2017 年 5 月に同様に驚異的なスピードで世界中の広範な組織を席巻した WannaCry の大流行を思い起こさせる。

このランサムウェアは若干異質であり、管理者権限で乗っ取った場合はシステムのマスターブートレコードを暗号化し、通常の一般ユーザー権限の場合はシステムの特定ファイルを暗号化するなど、複数のレイヤに渡る攻撃を試みる。また、できる限り多くのシステムに確実に感染するために、いくつかの異なる方法を使う。

## 戦略的な推奨事項

ランサムウェアは企業ネットワークを標的に開発されており、亜種が増加するにつれ、その脅威は流行の一途をたどっている。しかし企業には、こうしたインシデントを防ぎ、被害発生時のシステムへの影響を最小化したうえで、迅速かつ効率的に修復することができる実践的な方法がある。以下は、IT 運用やセキュリティに関する主な対策である。

- **堅固な事業継続計画および実施** - 個人のユーザシステムおよび基幹サーバは、バックアップから早急に修復することができることを確認するとともに、システムの使用できない状態を回避するため、企業によって準備すべきデータの時間軸にバックアップの頻度が合致していることを確認する。
- **危機およびインシデントへのレスポンス計画および演習実施** - 従業員および優先度の高いインシデントの管理責任者は、ランサムウェアのイベントに対する企業の取り組みを整備するための正式な手順、そして従業員や顧客に対してサービスを回復させる能力があることを確認する。
- **強固なセキュリティ対策ポリシーおよびユーザー意識** -電子メールのゲートウェイやネットワーク境界の管理を強化し、頑強な啓発活動を通して用心深い従業員を育成し、最も悪用される感染経路であるフィッシングを介したランサムウェアが自社の IT 環境に侵入するのを防ぐ。
- **厳密なパッチおよび脆弱性管理** - 今回の攻撃で悪用された脆弱性は、すでに Microsoft が 3 月にリリースした緊急パッチを介して周知されている。そして、確固たる脆弱性管理プログラムは攻撃の可能性を低下させる助けとなる。

## 優先的な推奨事項および注記

- 上層部はデスクトップおよびサーバの IT 運用チームに対し、迅速に MS17-010 と Microsoft の 4 月および 5 月のセキュリティアップデートを装備するためのサポートを提供する
- 上層部はまた、IT 運用チームがセキュリティチームの要請に基づいて、脆弱なサービスの無効化と追加的な管理手法の設置のため、複数の IT 資産上のサービスを一時的に不能にさせる必要があるかもしれないことを理解する
    - IT チームが対策を実施したか、あるいは対策案をまとめたかを確認する
    - 外部の SMB アクセスを無効化する（ネットから/への 137, 139, 445 ポートを遮断する）
    - IT 資産全般にわたって SMBv1 ネットワーク共有プロトコルを無効化する
    - グループポリシー設定を使ってオフィス文書における証明書のないマクロの実行を無効化する（そし

て自社だけの合法的なマクロを認証する）

- システムに対する外部からのアクセスすべてに二要素認証を導入する（例えば、VPN と RDP）
- MS17-010 のセキュリティパッチが導入されていない全てのシステムを特定して企業のコアネットワークの接続から遮断し、コアネットワークに接続できるすべてのゲストネットワークをセグメント化する
- アンチウイルス製品のシグネチャを全社規模で強制的にアップデートする
- 他のシステムに感染が拡大しないよう、感染システムを早急に企業ネットワークから隔離する

- PwC は、命の危険がある場合を除き、ランサムウェアへの身代金の支払いを推奨しない。支払いに応じることは、ランサムウェアにさらなる資金を注ぎ、新たなランサムウェア技術やキャンペーンの開発を促すことになる。
- ・イギリスにおけるランサムウェアのインシデントは、ActionFraud に報告する。ActionFraud は National Cyber Security Centre、National Crime Agency、および地域の法執行機関と連携している。

## 技術分析

この最新ランサムウェアの初期の感染経路は、現在のところ判明していない。不正プログラムは実際、「Petya」および「Mischa」の統合されたものである。もし不正プログラムが管理者権限で起動した場合はマスターブートレコード（MBR）を暗号化するが、ディスク上のファイルは暗号化しない。MBR を暗号化する影響としては、ユーザーが通常の方法でシステムを再起動することができず、代わりに身代金メッセージを表示させることである。しかし、不正プログラムが一般権限で起動した場合、特定の拡張子（Appendix A）のファイルが暗号化される。これは、「Goldeneye」との組み合わせで知られている。

バイナリは 32 ビット DLL ファイルであり、以下の属性情報がある。

MD5:71b6a493388e7d0b40c83ce903bc6b04
SHA1:34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
Size: 362,360 bytes
Compiler: Microsoft Visual C/C++ 2010
Linker: Microsoft Linker 10

不正プログラムはまず始めに、オペレーティングシステムが 32 ビットか 64 ビットかを検証し、Windows の x64 バージョンが稼働していると検知した場合は 64 ビットの互換バージョンをドロップする。そのファイルはユーザーの AppData\Local\Temp directory に.tmp ファイルとして格納される。その属性情報は以下の通りである。

MD5:7e37ab34ecdcc3e77e24522ddfd4852d
SHA1:38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf
Size: 56320 bytes
Compiler: Microsoft Visual C/C++ 2010
Linker: Microsoft Linker 10

興味深いのは、最初のペイロードにおけるコンパイルされたタイムスタンプが 2017 年 6 月 18 日である一方、x64DLL のコンパイルされたタイムスタンプが 2017 年 6 月 6 日であることだ。我々の評価では、今回キャンペーンが、流行した 27 日から数週間前に遡って計画されてきた可能性が高い。

最初の DLL は下図の Figure 1 の通り、Microsoft Sysinternal ツール群からコピーされた 2010 年 4 月 27 日にサインされた無効なデジタル証明書を持っていた。

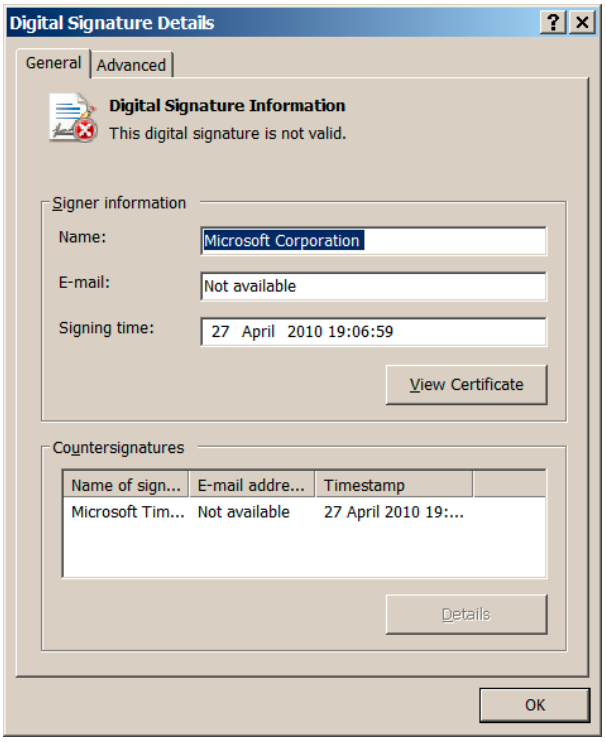


**Figure 1 - Microsoft からのものと主張するファイルの電子証明書**

最初のバイナリは DLL ファイルのため、rundll32.exe として起動されるべきであり、以下のコマンドによって起動することができる:

rundll32.exe perfc.dat #1

不正プログラムが一旦起動すれば、Figure 2 の通り以下のコマンドを実行する。

wevtutil cl Setup wevtutil cl System wevtutil cl Security
wevtutil cl Application
fsutil usn deletejournal /D C:

```
loc_1000811B:
mov     eax, [ebp+arg_0]
imul    eax, 0EA60h
push    eax             ; dwMilliseconds
call    ebx ; Sleep
movzx   eax, Filename
push    eax
lea     eax, [ebp+var_A18]
push    offset aWevtutilClSetu ; "wevtutil cl Setup & wevtutil cl System "...
push    eax             ; LPWSTR
call    ds:wsprintfW
xor     eax, eax
add     esp, 0Ch
mov     [ebp+var_21A], ax
push    3
lea     eax, [ebp+var_A18]
call    sub_100083BD
test    byte ptr dword_1001F144, 1
jz      short loc_10008114

; const WCHAR aWevtutilClSetu
aWevtutilClSetu:                        ; DATA XREF: perfc_1+34A↑o
                unicode 0, <wevtutil cl Setup & wevtutil cl System & wevtutil cl Secu>
                unicode 0, <rity & wevtutil cl Application & fsutil usn deletejournal>
                unicode 0, < /D %c:>,0
```

**Figure 2 -イベントログや USN ジャーナルを削除するコマンドの起動**

Wevutil は Microsoft のイベントログユーティリティであり、'cl'の引数はそれぞれセットアップログ、システムログ、セキュリティログ、アプリケーションログを削除する。これは、システム上における不正な活動を隠ぺいする目的で実施される。そして、システムの USN ジャーナルを削除して無効化するために、fsutil のコマンドを使って実行する。USN ジャーナルが無効化するということは、システムがボリューム対し、またはボリューム上のファイルに対して行われた追加変更を記録しないことを意味し、後日、任意の日付で成功裏にリカバリできる可能性を低下させる。

全てのコマンドが実行されたのち、タスクスケジューラが作成され、コマンド実行後 1 時間後にシステムの強制終了が実行されるようスケジュールされる。

dllhost.dat（MD5: aeee996fd3484f28e5cd85fe26b6bdcd）ファイルが%WINDIR%ディレクトリ内にドロップされる。同ファイルは実際、リモートシステムでコマンドを実行するために使われるツールであり、PSEXEC の一種である。これがネットワーク内に不正プログラムが拡散していく感染経路として使われている可能性が高い。我々は、以下のコマンドでサブネット全体をスキャンする証拠を確認している。

```
\\%\s\admin$
\\%\s\admin%w$
```

また、このランサムウェアが増殖するために、wmic が使われていると暗示される証拠もある。

```
wbem\wmic.exe %s /node:"%ws" /user:"%ws" /password:"%ws" process call create "C:\Windows\System32\rundll32.exe\"C:\Windows\%s\"
```

同サンプルはまた、最近の WannaCry の流行や EternalBlue によって攻撃される同様の脆弱性に悪用される 139 ポートおよび 445 ポート（SMB）をスキャンすることで、端末が稼働するサブネット全体を列挙する。

## インジケーター

以下のインジケーターが確認されている

*Filenames*:

dllhost.dat

*Hashes*:

71b6a493388e7d0b40c83ce903bc6b04
a1d5895f85751dfe67d19cccb51b051a
7e37ab34ecdcc3e77e24522ddfd4852d
e285b6ce047015943e685e6638bd837e
fe2c47fbb22139f790287272e9a9e365
e595c02185d8e12be347915865270cca

*Email*:

wowsmith123456@posteo[.]net

*Payment URL's*:

http://mischapuk6hyrn72.onion/
http://petya3jxfp2f7g3i.onion/
http://petya3sen7dyko2n.onion/
http://mischa5xyix2mrhd.onion/MZ2MMJ
http://mischapuk6hyrn72.onion/MZ2MMJ
http://petya3jxfp2f7g3i.onion/MZ2MMJ
http://petya3sen7dyko2n.onion/MZ2MMJ

*IDS Rules:*

alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /"; flow:established,from_client; urilen:1; content:"OPTIONS"; http_method; content:"DavClnt"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000199; rev:2017062701;)

alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"OPTIONS"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0- 9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000200; rev:2017062701;)

alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - PROPFIND /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"PROPFIND"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; content:"Depth: 0|0d 0a|"; http_header; content:"Content-Length: 0|0d 0a|"; http_header; pcre:"/^[0- 9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000201; rev:2017062701;)

※本文は、PwC 英国が発表した資料の抄訳です。英語の原文と翻訳内容に相違がある場合には原文が優先します。

## 付録 1 – ターゲットとなるファイルタイプ

| File Type | | | |
|---|---|---|---|
| .3ds | .dwg | .pst | .work |
| .7z | .eml | .pvi | .xls |
| .accdb | .fdb | .py | .xlsx |
| .ai | .gz | .pyc | .xvd |
| .asp | .h | .rar | .zip |
| .aspx | .hdd | .rtf | |
| .avhd | .kdbx | .sln | |
| .back | .mail | .sql | |
| .bak | .mdb | .tar | |
| .c | .msg | .vbox | |
| .cfg | .nrg | .vbs | |
| .conf | .ora | .vcb | |
| .cpp | .ost | .vdi | |
| .cs | .ova | .vfd | |
| .ctl | .ovf | .vmc | |
| .dbf | .pdf | .vmdk | |
| .disk | .php | .vmsd | |
| .djvu | .pmf | .vmx | |
| .doc | .ppt | .vsdx | |
| .docx | .pptx | .vsv | |

## About PwC

PwC Japan グループでは、クライアントの課題解決のために、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、そして税務、法務において、国内およびグローバルにおける複雑な経済環境で活躍される皆様に、きめ細かなサービスを提供しています。

サイバーセキュリティに関する
ご相談／お問い合わせ先はこちらまで

» Mail: JP_Cons_pcs.info@pwc.com

**PwC サイバーサービス合同会社**
〒104-0061 東京都中央区銀座 8-21-1
住友不動産汐留浜離宮ビル
Tel：03-3546-8480
http://www.pwc.com/jp/cybersecurity

**www.pwc.com/jp**