< WannaCry ランサムウェアリサーチレポート>

WannaCry の不正ファイルを検出できるように作成された YARA Rule では、次のように exe、bat、vbs のルールが存在します。
(YARA は、文字列やバイナリパターンに基づいてマルウェアを検出し、これらのマルウェアを分類することができるツールであり、製品に適用して使用している企業は、VirusTotal と FireEye があります)

EXE

```
rule WannaCry_Ransomware_Gen {
   meta:
      description = "Detects WannaCry Ransomware"
      author = "Florian Roth (based on rule by US CERT)"
      reference = "https://www.us-cert.gov/ncas/alerts/TA17-132A"
      date = "2017-05-12"
      hash1 = "9fe91d542952e145f2244572f314632d93eb1e8657621087b2ca7f7df2b0cb05"
      hash2 = "8e5b5841a3fe81cade259ce2a678ccb4451725bba71f6662d0cc1f08148da8df"
      hash3 = "4384bf4530fb2e35449a8e01c7e0ad94e3a25811ba94f7847c1e6612bbb45359"
   strings:
      $s1 = "__TREEID__PLACEHOLDER__" fullword ascii
      $s2 = "__USERID__PLACEHOLDER__" fullword ascii
      $s3 = "Windows for Workgroups 3.1a" fullword ascii
      $s4 = "PC NETWORK PROGRAM 1.0" fullword ascii
      $s5 = "LANMAN1.0" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 5000KB and all of them
`
```

BAT

```
rule WannCry_BAT {
   meta:
      description = "Detects WannaCry Ransomware BATCH File"
      author = "Florian Roth"
      reference = "https://goo.gl/HG2j5T"
      date = "2017-05-12"
      hash1 = "f01b7f52e3cb64f01ddc248eb6ae871775ef7cb4297eba5d230d0345af9a5077"
   strings:
      $s1 = "@.exe\">> m.vbs" ascii
      $s2 = "cscript.exe //nologo m.vbs" fullword ascii
      $s3 = "echo SET ow = WScript.CreateObject(\"WScript.Shell\")> " ascii
      $s4 = "echo om.Save>> m.vbs" fullword ascii
   condition:
      ( uint16(0) == 0x6540 and filesize < 1KB and 1 of them )
}
```

VBS

```
rule WannCry_m_vbs {
   meta:
      description = "Detects WannaCry Ransomware VBS"
      author = "Florian Roth"
      reference = "https://goo.gl/HG2j5T"
      date = "2017-05-12"
      hash1 = "51432d3196d9b78bdc9867a77d601caffd4adaa66dcac944a5ba0b3112bbea3b"
   strings:
      $x1 = ".TargetPath = \"C:\\@" ascii
      $x2 = ".CreateShortcut(\"C:\\@" ascii
      $s3 = " = WScript.CreateObject(\"WScript.Shell\")" ascii
   condition:
      ( uint16(0) == 0x4553 and filesize < 1KB and all of them )
}
```

以下は、WannaCry ランサムウェアの感染、対象拡張子、拡散方法などをリサーチした資料です。

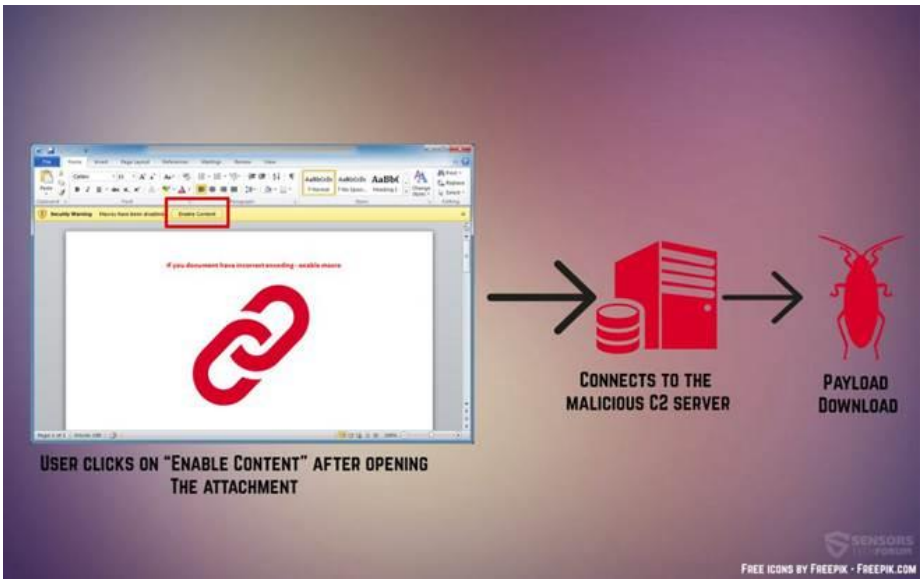
1. 感染

A. MS17-010 パッチが適用されていない Windows で、ETERNALBLUE と命名されたマルウェアが実行される

i. マルウェアは、以下のような経路で感染または流入することがある。

1. Torrent Web Site、Fake Updates ファイルまたは Fake Setups 実行ファイルを通した感染
2. 電子メールの添付ファイルで流入(Java Script、実行ファイル、**マルウェアマクロが入っている文書ファイル**)

A.マルウェアマクロが入っている文書ファイルを実行する場合、下記のような段階でマルウェアをダウンロードして実行する



B.マルウェアの動作方式

i. Program Data フォルダ内に tasksche.exe ファイルを作成するか、Windows フォルダの中に任意の文字フォルダを作成して、mssecsvc.exe と tasksche.exe を生成

ii. Icacls./grant Everyone：F/T/C/Q コマンドを実行し、全てのファイルに対する全ての権限を付与

iii.下の Windows System Process を終了

1. Mysqld.exe
2. Sqlwriter.exe
3. Sqlserver.exe
4. MSExchange
5. Microsoft.Exchange

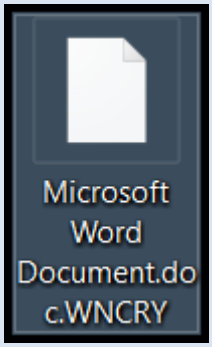
iv. Windowsレジストリを編集して、システムがブーティングする時にファイルの暗号化を開始する

1. HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩
2. HKCU₩Software₩WanaCrypt0r₩
3. HKCU₩Software₩WanaCrypt0r₩wd
4. HKCU₩Control Panel₩Desktop₩Wallpaper

C. 感染後、以下のような画面を表示し、BitCoin支払いを要求する。

2. 対象拡張子

A. 179 個のファイルタイプを WNCRY 拡張子で暗号化し、代表的な拡張子は以下の通り。

i. Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi) ii. Less common and nation-specific office formats (.sxw, .odt, .hwp) iii. Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv) iv. Emails and email databases (.eml, .msg, .ost, .pst, .edb) v. Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd) vi. Developers' sourcecode and project files (.php, .java, .cpp, .pas, .asm) vii. Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes) viii. Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd) ix. Virtual machine files (.vmx, .vmdk, .vdi)	

3. 拡散方法

A. Windows の SMB(Server Message Block)実現の脆弱性を使用して拡散する