Informe Bad Rabbit
Panda Security

26 de octubre de 2017

Análisis Técnico de Bad Rabbit

Calle Santiago de Compostela, 12 1ª plta
48003 Bilbao, Vizcaya. Spain

Crta. de la Coruña, km 17,800
28231 Las Rozas, Madrid. Spain

Estamos ante un ransomware muy parecido al NotPetya. Una de las principales diferencias, además de no usar el exploit EternalBlue, es que han cambiado la forma de cifrar el disco.

Antes, tras reiniciar el ordenador, usaban un chkdsk falso que se ejecutaba al iniciar el sistema y acababa cifrando el disco. Esto se llevaba a cabo antes de iniciar Windows con un Master Boot Record (MBR) modificado. Esto ha desaparecido de Bad Rabbitt, lo que utilizan para cifrar es un programa "dispci.exe", que hace uso el driver "cscc". Este driver no es malware, se trata de una aplicación legítima (**https://diskcryptor.net/wiki/FAQ**) utilizada en este caso para cifrar el disco de la víctima.

Por lo que hemos observado hasta el momento, el vector de entrada es a través de páginas web comprometidas, haciéndose pasar por una actualización del Flash Player. Es el propio usuario el que tiene que descargarse y ejecutar el fichero. Una vez ejecutado, extrae el fichero en C:\Windows\infpub.dat -en realidad el ficheros es una dll- y lo ejecuta con el siguiente comando: rundll32.exe C:\Windows\infpub.dat,#1 15

A partir de este momento infpub.dat será el que realice todas las acciones:

1) Comprueba la existencia de ciertos programas en ejecución, la comprobación la hace mediantes hashhemos encontrado los valores para:

- mfevtps.exe -> 0xC8F10976
- McTray.exe -> 0x923CA517
- mcshield.exe ->0xE5A05A00
- dwwatcher -> 0x4A241C3E
- dwarkdaemon.exe -> 0x966D0415
- dwengine.exe -> 0xE2517A14
- dwservice.exe -> 0xAA331620

Dependiendo de qué procesos encuentre, realiza unas u otras acciones. Esto mismo lo hacía también **NotPetya**.

2. Extrae el driver con el nombre "cscc.dat", este driver no es malware, es una aplicación legítima usada en este caso por el ransomware para cifrar.

3. Extrae el fichero dispci.exe y genera una tarea programada que se ejecuta en el siguiente reinicio:

- chtasks /Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR “C:\Windows\system32\cmd.exe /C Start \”\” \”C:\Windows\dispci.exe\” -id 2213133121 && exit”

4. Instala el driver “cscc.dat” como servicio en el sistema:

```
loc_6F68138E:                           ; CODE XREF: CreaServicio+19↑j
                push    edi
                push    esi             ; lpPassword
                push    esi             ; lpServiceStartName
                push    offset Dependencies ; "FltMgr"
                push    esi             ; lpdwTagId
                push    offset Data     ; "Filter"
                push    offset BinaryPathName ; "cscc.dat"
                push    3               ; dwErrorControl
                push    esi             ; dwStartType
                push    1               ; dwServiceType
                push    0F01FFh         ; dwDesiredAccess
                push    offset DisplayName ; "Windows Client Side Caching DDriver"
                push    offset ServiceName ; "cscc"
                push    ebx             ; hSCManager
                call    ds:CreateServiceW
```

5. Crea una tarea programada para reiniciar el sistema:

```
pMore = 's';
v10 = 'h';
v11 = 'u';
v12 = 't';
v13 = 'd';
v14 = 'o';
v15 = 'w';
v16 = 'n';
v17 = '.';
v18 = 'e';
v19 = 'x';
v20 = 'e';
v21 = ' ';
v22 = '/';
v23 = 'r';
v24 = ' ';
v25 = '/';
v26 = 't';
v27 = ' ';
v29 = ' ';
v30 = '/';
v31 = 'f';
v32 = 0;
v28 = '0';
if ( PathAppendW(&Buffer, &pMore) )
{
  wsprintfW(&v6, L"schtasks /Create /SC once /TN drogon /RU SYSTEM /TR \"%ws\" /ST %02d:%02d:00", &Buffer, v4, v3);
  v0 = CreaProceso(&v6, 0);
}
```

6. Realiza el movimiento lateral para infectar otras maquinas de la red, utiliza las mismas técnicas que la versión anterior pero esta vez NO tiene ETERNALBLUE implementado, la forma de infección es la siguiente:

a. Lanza una versión de MIMIKATZ para obtener credenciales

b. Realiza una enumeración mediante código propio para obtener credenciales de los procesos ejecutados en el sistema

c. Con las credenciales obtenidas intenta conectarse a los recursos compartidos de otras máquinas, además hace fuerza bruta con un diccionario de credenciales que tiene hardcodeado.

d. Si consigue acceso copia el propio bicho y lo instala en el sistema.

7. Realiza un cifrado de los archivos del disco duro la extensiones afectadas son:

```
unicode 0, <.3ds.7z.accdb.ai.asm.asp.aspx.avhd.back.bak.bmp.brw.c.cab>
unicode 0, <.cc.cer.cfg.conf.cpp.crt.cs.ctl.cxx.dbf.der.dib.disk.djvu>
unicode 0, <.doc.docx.dwg.eml.fdb.gz.h.hdd.hpp.hxx.iso.java.jfif.jpe.>
unicode 0, <jpeg.jpg.js.kdbx.key.mail.mdb.msg.nrg.odc.odf.odg.odi.odm>
unicode 0, <.odp.ods.odt.ora.ost.ova.ovf.p12.p7b.p7c.pdf.pem.pfx.php.>
unicode 0, <pmf.png.ppt.pptx.ps1.pst.pvi.py.pyc.pyw.qcow.qcow2.rar.rb>
unicode 0, <.rtf.scm.sln.sql.tar.tib.tif.tiff.vb.vbox.vbs.vcb.vdi.vfd>
unicode 0, <.vhd.vhdx.vmc.vmdk.vmsd.vmtm.vmx.vsdx.vsv.work.xls.xlsx.x>
unicode 0, <ml.xvd.zip.>,0
```

8. Y finalmente reinicia el sistema

Como decíamos al inicio, básicamente es lo mismo que NotPetya, pero que ahora es el programa “dispci.exe” el que se ejecutará tras el reinicio y es el que realizará el cifrado del disco y modificará la MFT para que en el siguiente arranque muestre el mensaje típico de Petya y pida la contraseña para arrancar el sistema. Esta contraseña solo permite arrancar, una vez arrancado los ficheros que fueron cifrados seguirán cifrados.

Para tu información, mantendremos constantemente actualizada nuestra web de soporte con todos los detalles del ciberataque Bad Rabbit