pandasecurity.com

Bad Rabbit report

Panda Security

26/10/2017

Technical Analysis of 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

We're looking at a ransomware that is very similar to NotPetya. One of the main differences, besides not using the EternalBlue exploit, is in the way it encrypts the disk.

In the case of NotPetya, it restarted the computer and used a false chkdsk that was executed when starting the system, which then went on to encrypt the disk. This was done before starting Windows with a modified Master Boot Record (MBR). This process has disappeared from Bad Rabbit. Instead, they use a "dispci.exe" program for encryption, which makes use of the "cscc" driver. This driver is not malware, but rather a legitimate application (**https://diskcryptor.net/wiki/FAQ**) used in this case to encrypt the victim's disk.

According to what we've been able to observe until present, compromised web pages were used as an entry vector, posing as a Flash Player update. The user has to download and execute the file. Once executed, it extracts the file in C:\Windows\infpub.dat. In reality, the file is a dll, and it is executed through the following command: rundll32.exe C:\Windows\infpub.dat,#1 15

From this point on, infopub.dat will carry out all the following actions:

1. Checks for certain running programs using hashes. We've found values for:

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

Depending on what processes it finds, it carries out corresponding actions. This behavior is similar to **NotPetya**.

2. Extracts the driver with the name "cscc.dat". This driver is not malware, but rather a legitimate application used in this case by ransomware for encryption.

3. Extracst the dispci.exe file and schedules a task to be executed at the next reboot:

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

4. Installs the “cscc.dat” driver as a service.

```
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. Programs a task to restart the system:

```
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. Moves laterally to infect other machines on the network, using the same techniques as the previous version but this time without EternalBlue. The infection process is the following:

a. Launches a version of MIMIKATZ to obtain credentials.

b. Performs an enumeration using its own code to obtain credentials for the processes executed in the system.

c. With the obtained credentials it tries to connect to the shared resources of other machines. In addition, attempts a brute force entry with a hardcoded dictionary of credentials.

d. If it gets access, it copies the bug itself and installs it on the system.

7. Encrypts the files on the hard drive. The affected extensions are:

```
                        ; .data:0f693028↓o
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. Finally, it reboots the system.

As we mentioned above, it is basically the same as NotPetya, but now it is the program “dispci.exe” which will be executed after rebooting and which will perform the encryption of the disk and modify the MFT so that on the next boot it shows the same Petya message and asks for the password to boot the system. This password only allows the computer to start up. Once it starts up, the files that were encrypted will still be encrypted.

We will keep you informed with continuous updates on our support page providing any new details relating to Bad Rabbit.