ZLAB

Malware Analysis Report: Bad Rabbit

Malware Analysts:

Antonio Pirozzi
Antonio Farina
Luigi Martire

CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

31/10/17

Table of Contents

CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Introduction

Recently a new ransomware, called BadRabbit, infected systems in many countries, most of in East Europe, such as Ukraine and Russia. The malware was not totally new, it seems to be an evolution of the old NotPetya ransomware for some aspects, including:

- The behavior after the reboot with a particular ransom note.
- The spreading capability through lateral movements that relies on the SMB protocol and exploits a vulnerability based on vulnerability MS17-010.

There are also many differences with NotPetya, including, a more sophisticated behavior and the fixing of coding errors that transform NotPetya from a ransomware to a wiper, through the ad-hoc encrypting library “DiskCryptor”, for this purpose. These aspects suggest that the malware is a pure and correctly developed ransomware. Although there are some discrepancies:

- The onion site indicated in the ransom note, “caforssztxqzf2nm[.]onion”, one the day after the initial infection, was no longer reachable. This implies that victims cannot pay the ransom to decrypt their files. But it’s strange that the onion site could be taken down so rapidly from authorities and it’s more probable that it could be taken down by the authors themselves.
- Most of the compromised websites belong to restaurants, hotels and “house rental” services.
- Most of the infected systems were in Ukraine, for example at the Odessa airport and Kiev metro. The targets are the same places previously targeted by NotPetya hackers.

These reasons make think that the malware isn’t a wiper for the design, but so de facto, because of the impossibility to pay the ransom and that the malware was written by the same authors of NotPetya and to be its evolution.

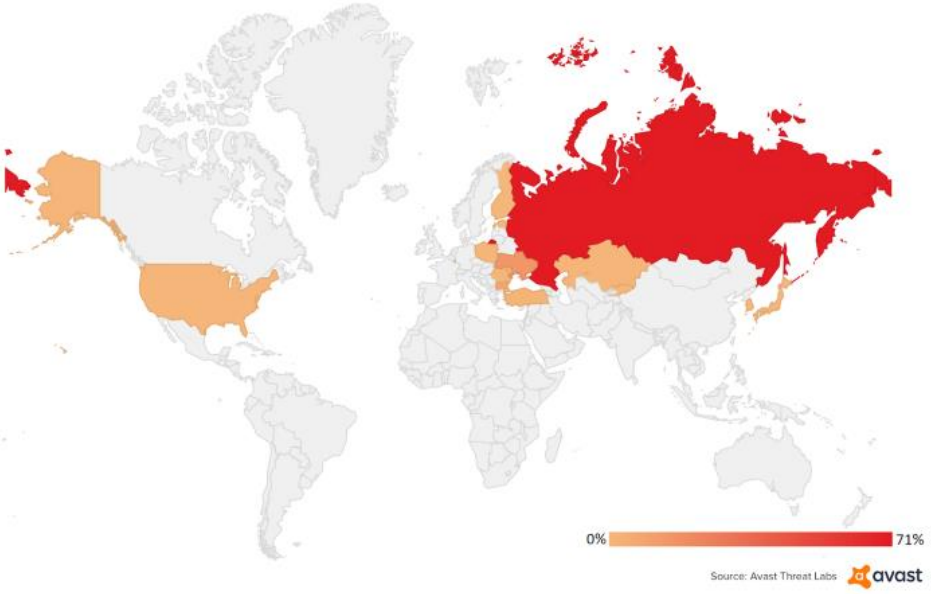

Figure 1 - BadRabbit infection map (Source Avast)

Basic Static Analysis

Dropper

Filename: “install_flash_player.exe”

MD5	fbbdc39af1139aebba4da004475e8839
SHA-1	de5c8d858e6e41da715dca1c019df0bfb92d32c0
SHA-256	630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da
File Size	431.5 KB
Icon	

Table 1 - Generic Info about Bad Rabbit's dropper

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	11987	12288	6.58	098c323b1a59bcf15c1feb8055e58931
.rdata	16384	12330	12800	7.18	9cc3629beb9d1f37932d860de2e3a4f5
.data	32768	828	512	0.18	4e5d61b2bd73632f0225e39a2e2c5144
.rsrc	36864	28808	29184	4.2	256c5e23a9ad8a276128f84017b2d79d
.reloc	69632	590	1024	3.29	26cd68101ade4e5f70ab3cd5f35e0ad5

Table 2 - Info about Bad Rabbit's dropper Sections

“infpub.dat”

Filename: “infpub.dat”

MD5	1d724f95c61f1055f0d02c2154bbccd3
SHA-1	79116fe99f2b421c52ef64097f0f39b815b20907
SHA-256	579fd8a0385482fb4c789561a30b09f25671e86422f40ef5cca2036b28f99648
File Size	401.1 KB

Table 3 - Generic info about "infpub.dat"

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	49107	49152	6.57	f277e74393ce6a5225228d538d794067
.rdata	53248	23803	24064	6.34	50eb2a2b07fa914ce2e9d3f470796e41
.data	77824	21360	2560	6.3	14a2ecc6822bbedc01d209e8b3f541c4
.rsrc	102400	316928	316928	7.99	49761becfc454de3506c3fa2b11cfbc9
.reloc	421888	3472	3584	5.77	0b73b18ff226349be058ad09669b00b0

Table 4 - Info about "infpub.dat" sections

“discpi.dat”

Filename: “dispcpi.dat”

MD5	b14d8faf7f0cbcfad051cefe5f39645f
SHA-1	afeee8b4acff87bc469a6f0364a81ae5d60a2add
SHA-256	8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93
File Size	139.5 KB

Table 5 - Generic info about "discpi.dat"

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	71754	72192	6.58	0fa851de532b3dd96e1578a1fe912cea
.rdata	77824	16444	16896	4.83	e69552feb958791e5d7283cd1e9f0b0b
.data	98304	220460	6656	4.2	dc53a4c1670b55450713e13adc573c51
.rsrc	319488	39724	39936	6.17	538045e89d3956ece75779bbffedb57f
.reloc	360448	5846	6144	4.5	664441acad88cda5370381c965d187ab

Table 6 - Info about "dispci.dat" sections

Compromised sites

academicnet.ro	bizzzarttattoo.ro
ace-economiesociala.ro	brixongroup.ro
activedoctors.org	btfprotect.ro
adlibri.ro	memorialulrevolutiei.ro
adrianadanaila.com	sosta.ro
adventistbruxelles.org	stas2015.ro
aetm.ro	toppromotions.ro
afaceri-poligrafice.ro	
alegedorna.ro	
alinabercu.com	
amenajari-locuinte.ro	
amicos.ro	
ampgrup.ro	
andra-cretu.com	
andreevents.ro	
anvelopeiarna-autocenter.ro	
anvelope-service.ro	
anvelopevara-autocenter.ro	
apimond.ro	
aquamundus.ro	
aquariusconsult.com	
archivumka.ro	
armoniacenter.com	
artbodyspa.ro	
arvar.ro	
asatm.ro	
aspirelo.ro	
athenee-palace.ro	
atv-funtrans.ro	
avocatiinbraila.ro	
avocatiinbrasov.ro	
avocatiinbucuresti.ro	
axiautoonline.ro	
axiservice.ro	
http://balcoane.ro	
bbooster.ro	
bcarhitectura.ro	
birou-avocatura.com	
bizo.ro	

Table 7 - List of compromised sites

Behavioral Analysis

Distribution

The attack vector used by Bad Rabbit hackers is drive-by download attack. Attackers compromised popular websites, related to restaurants, hotels and “house rental” services, they injected a malicious JavaScript in their HTML body or in one of their .js file.JavaScrupt was used to redirect visitors to 1dnscontrol[.]com. At the time of the analysis, the site which was hosting the malicious file is no longer reachable. The script was used to download the ransomware using a POST request to the static IP address (185.149.120[.]3).

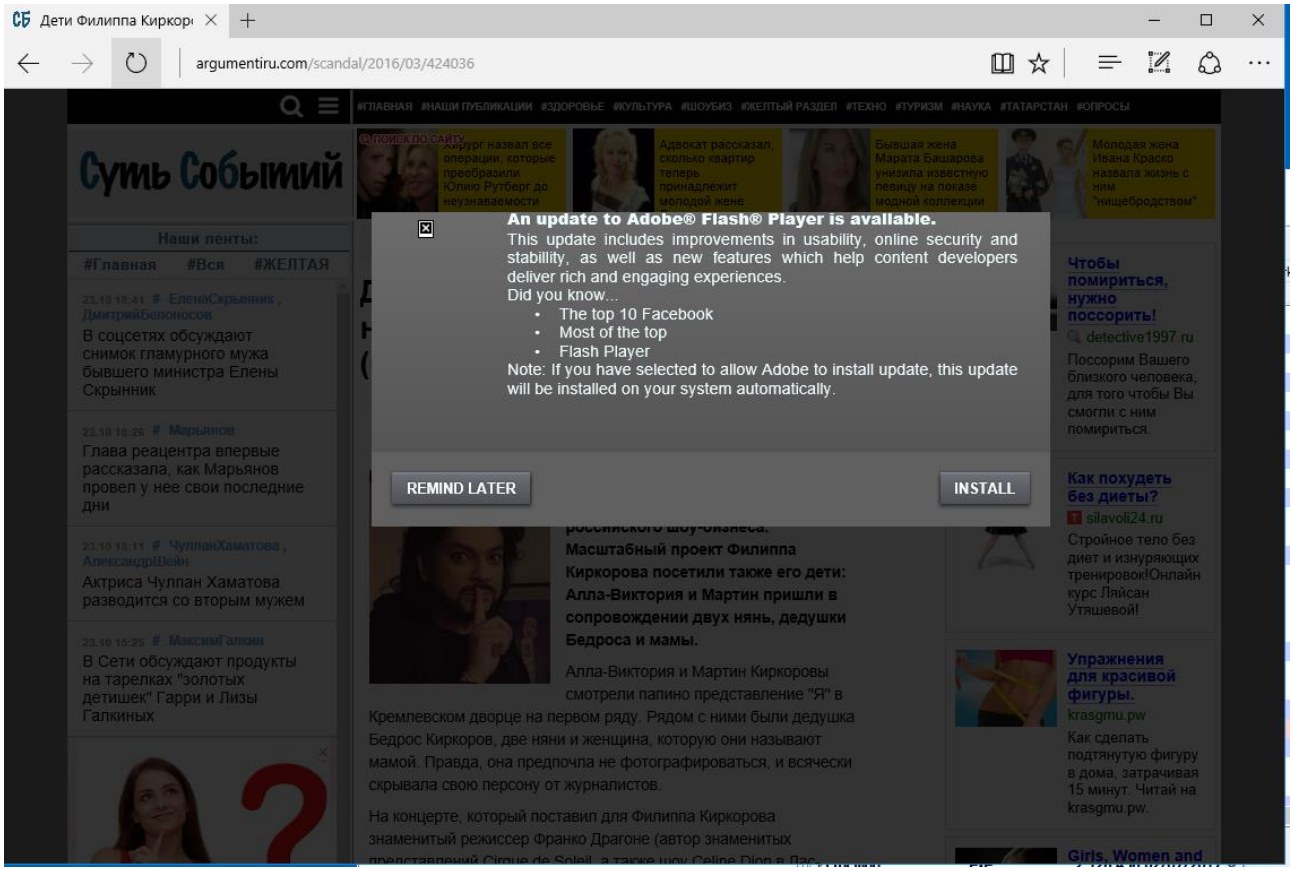

Figure 2 - Fake Adobe Flash Update

All the compromised sites present a screen similar to legit pop-up window of Adobe Flash update. The users download from the malicious site the “install_flash_player.exe” file, which is actually the dropper of Bad Rabbit (the users have to launch the executable to start the infection, otherwise nothing happens).
When the user executes the file, the Bad Rabbit’s infection starts and, after a series of operations, the system will reboot and display the ransom note.

Execution

When the infection is ready to go, the dropper file extracts some files:

- “C:\Windows\infpub.dat”
- “C:\Windows\cscc.dat”
- “C:\Windows\dispci.exe”
- “C:\Windows\[xxxx].tmp”

Once the files are extracted, the “infpub.dat” file is executed through the command:

"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"

This process can be considered as the “controller” of the malware, it controls every action of the ransomware. When the “infpub.dat” is loaded in memory, it deletes itself from the disk remaining only in memory.

Figure 3 - Some actions of "infpub.dat"

The purposes of “infpub.dat” are substantially three:

- To infect other machines on the subnetwork
- To schedule the reboot the execution of “discpi.exe” executable at the startup
- To encrypt the user files

The infection of the other machines is performed harvesting the password stored on the victim’s host with a custom version of Mimikatz tool (extracted in this case in the temporary file EC95.tmp). Together to a hard-coded wordlist of credentials (Table 8), the malware tries to get the access to the other hosts in the network in order to transfer the malicious file to them. If the transfer is completed, it uses EternalRomance, which is a remote code execution attack to exploit CVE-2017-0145, in order to launch the executable just transferred.

Usernames	Passwords
Administrator	Administrator
Admin	administrator
Guest	Guest
User	guest
User1	User
user-1	user
Test	Admin
root	adminTest

buh	test
boss	root
ftp	123
rdp	1234
rdpuser	12345
rdpadmin	123456
manager	1234567
support	12345678
work	123456789
other user	1234567890
operator	Administrator123
backup	administrator123
asus	Guest123
ftpuser	guest123
ftpadmin	User123
nas	user123
nasuser	Admin123
nasadmin	admin123Test123
superuser	test123
netguest	password
alex	111111
	55555
	77777
	777
	qwe
	qwe123
	qwe321
	qwer
	qwert
	qwerty
	qwerty123
	zxc
	zxc123
	zxc321
	zxcv
	uiop
	123321
	321
	love
	secret
	sex
	god

Table 8 - Hardcoded wordlist of credentials

Concurrently to the spread, “infpub.dat” schedules two tasks:

- Reboot after about 20 minutes
- Execute “dispci.exe” at the startup

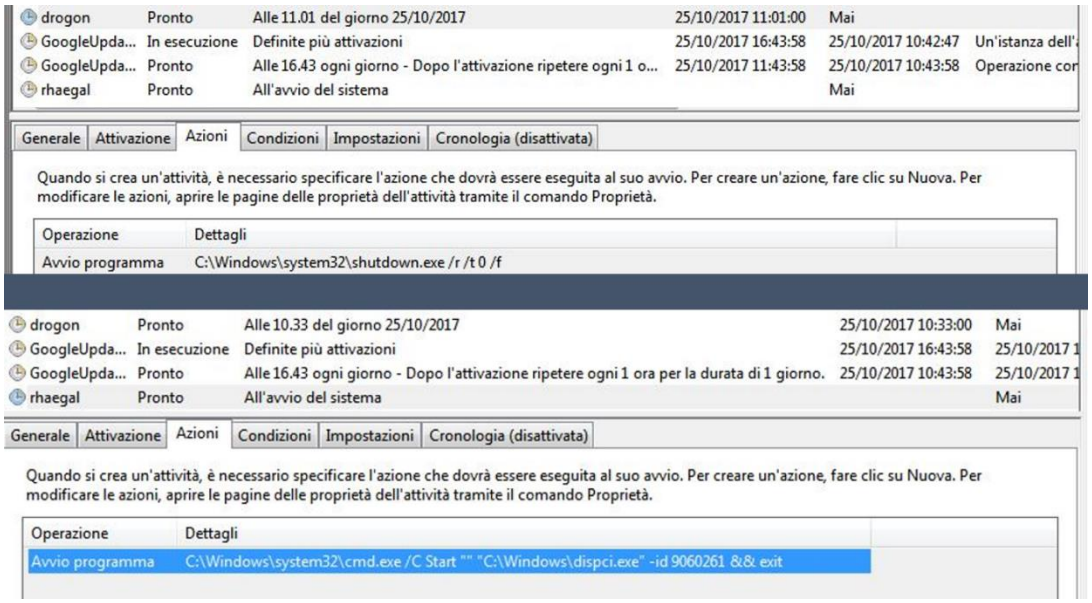

Figure 4 - Scheduled tasks

Moreover, the ransomware cyphers the user files using the open source library “DiskCryptor” hidden in the “cscc.dat” file. The malware excludes from the encryption the files contained in the following folders:

```
.data:10013014                                        ; "\\Windows"
.data:10013018                 dd offset aProgramFiles ; "\\Program Files"
.data:1001301C                 dd offset aProgramdata  ; "\\ProgramData"
.data:10013020                 dd offset aAppdata      ; "\\AppData"
```

Figure 5 - Folders excluded by the encryption

The malware cyphers only the file having one of the following extension:

```
.rdata:10011130 a_3ds_7z_accdb_:                      ; DATA XREF: sub_100059B1+46↑o
.rdata:10011130                                       ; .data:10013028↓o
.rdata:10011130                 unicode 0, <.3ds.7z.accdb.ai.asm.asp.aspx.avhd.back.bak.bmp.brw.c.cab>
.rdata:10011130                 unicode 0, <.cc.cer.cfg.conf.cpp.crt.cs.ctl.cxx.dbf.der.dib.disk.djvu>
.rdata:10011130                 unicode 0, <.doc.docx.dwg.eml.fdb.gz.h.hdd.hpp.hxx.iso.java.jfif.jpe.>
.rdata:10011130                 unicode 0, <jpeg.jpg.js.kdbx.key.mail.mdb.msg.nrg.odc.odf.odg.odi.odm>
.rdata:10011130                 unicode 0, <.odp.ods.odt.ora.ost.ova.ovf.p12.p7b.p7c.pdf.pem.pfx.php.>
.rdata:10011130                 unicode 0, <pmf.png.ppt.pptx.ps1.pst.pvi.py.pyc.pyw.qcow.qcow2.rar.rb>
.rdata:10011130                 unicode 0, <.rtf.scm.sln.sql.tar.tib.tif.tiff.vb.vbox.vbs.vcb.vdi.vfd>
.rdata:10011130                 unicode 0, <.vhd.vhdx.vmc.vmdk.vmsd.vmtm.vmx.vsdx.vsv.work.xls.xlsx.x>
.rdata:10011130                 unicode 0, <ml.xvd.zip.>,0
```

Figure 6 - Extensions of the files cyphered by the malware

After the first reboot, the “discpi.exe” executable is launched on the startup: this process is launched before the user logon and starts with its malicious actions.

The objectives of “discpi.exe” are two:

- Modify the original MBR
- Schedule a new reboot

The modification of the MBR happens overwriting the first sector. Unlike Petya and NotPetya, which have a defined and standard scheme for the structure of their microkernel, Bad Rabbit’s MBR jumps to a location variable for each infection. This position is related probably to the disk sector containing the files extracted by the dropper.

After the second reboot the Bad Rabbit’s ransom note is displayed:

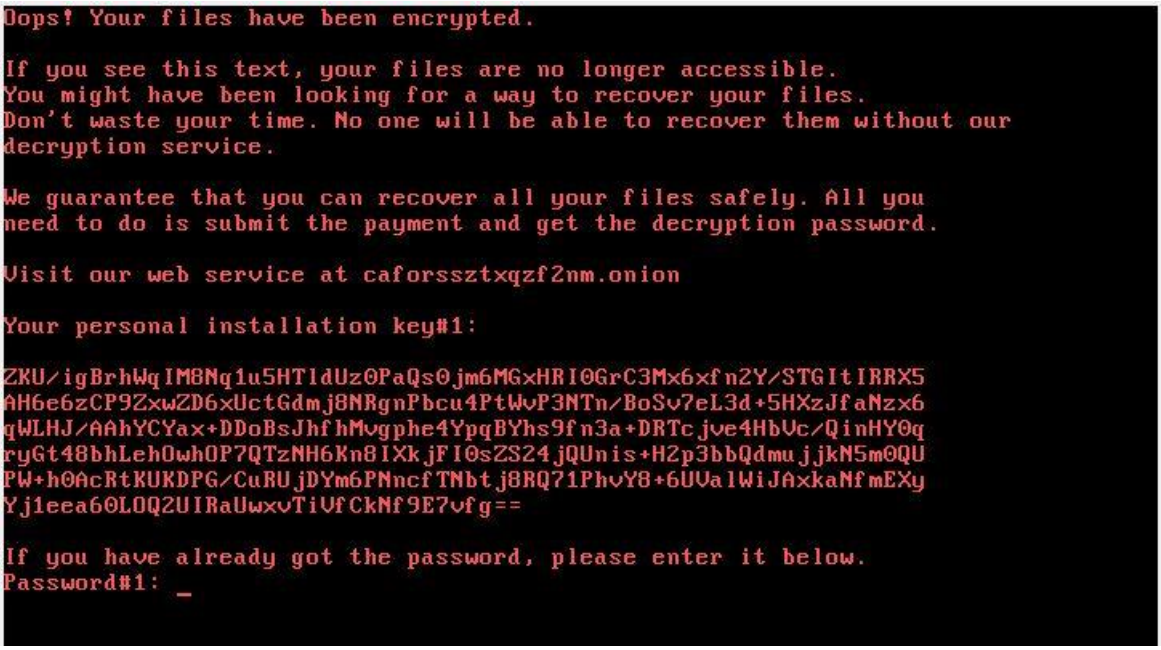

Figure 7 - Ransom note displayed

We synthetize the complete behavior of the malware in the following scheme:

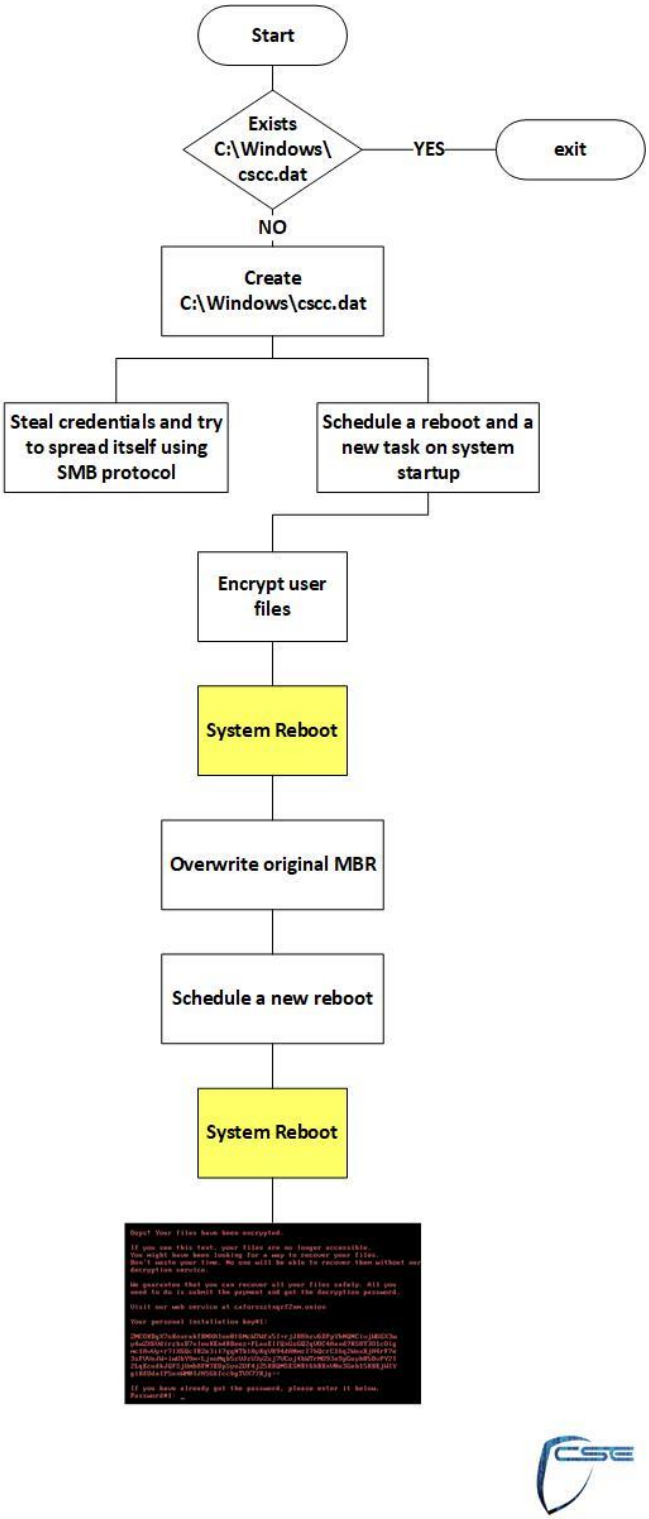

Figure 8 – Bad Rabbit's complete behavior

Advanced Analysis

Through the advanced analysis we consolidated the information gathered in the previous research and we found the kill-switch of the malware: when the dropper executes itself, it first checks the existence of the file “C:\Windows\cscc.dat” that includes the “DiskCryptor” library. If the file already exists, the malware doesn’t show its behavior terminating itself. This is confirmed in the code:

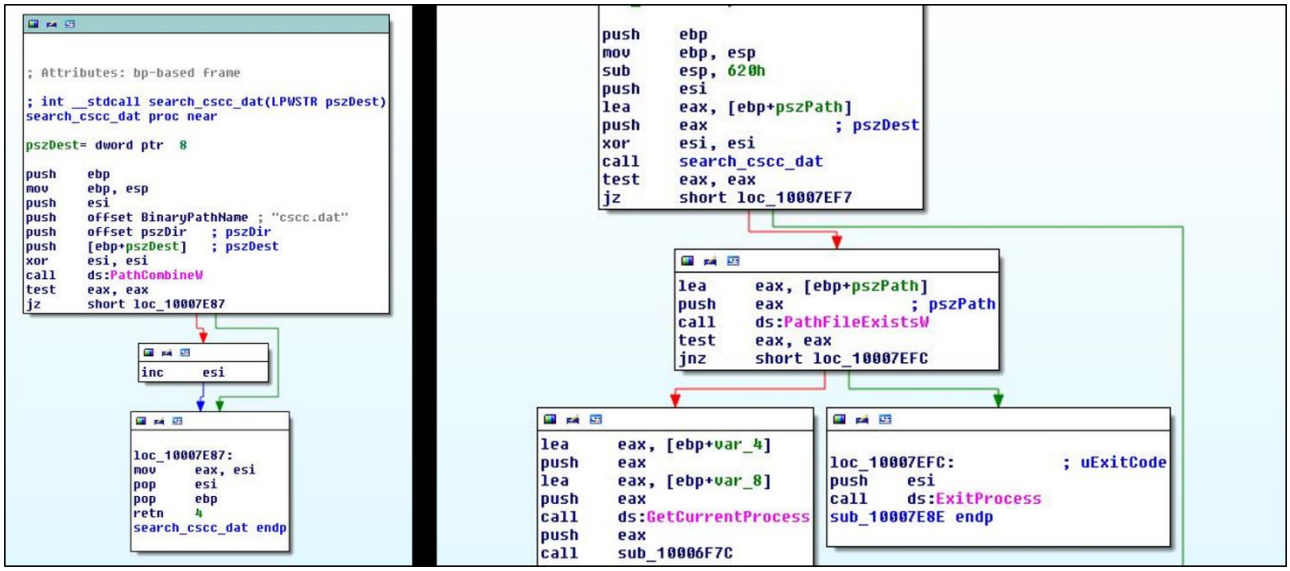

Figure 9 – Killswitch

We can confirm what the Cisco Talos team have discovered: the malware uses the EternalRomance exploit for its lateral movements. We found, using IDA, the section in which BadRabbit chooses the appropriate payload to include in EternalRomance exploit:

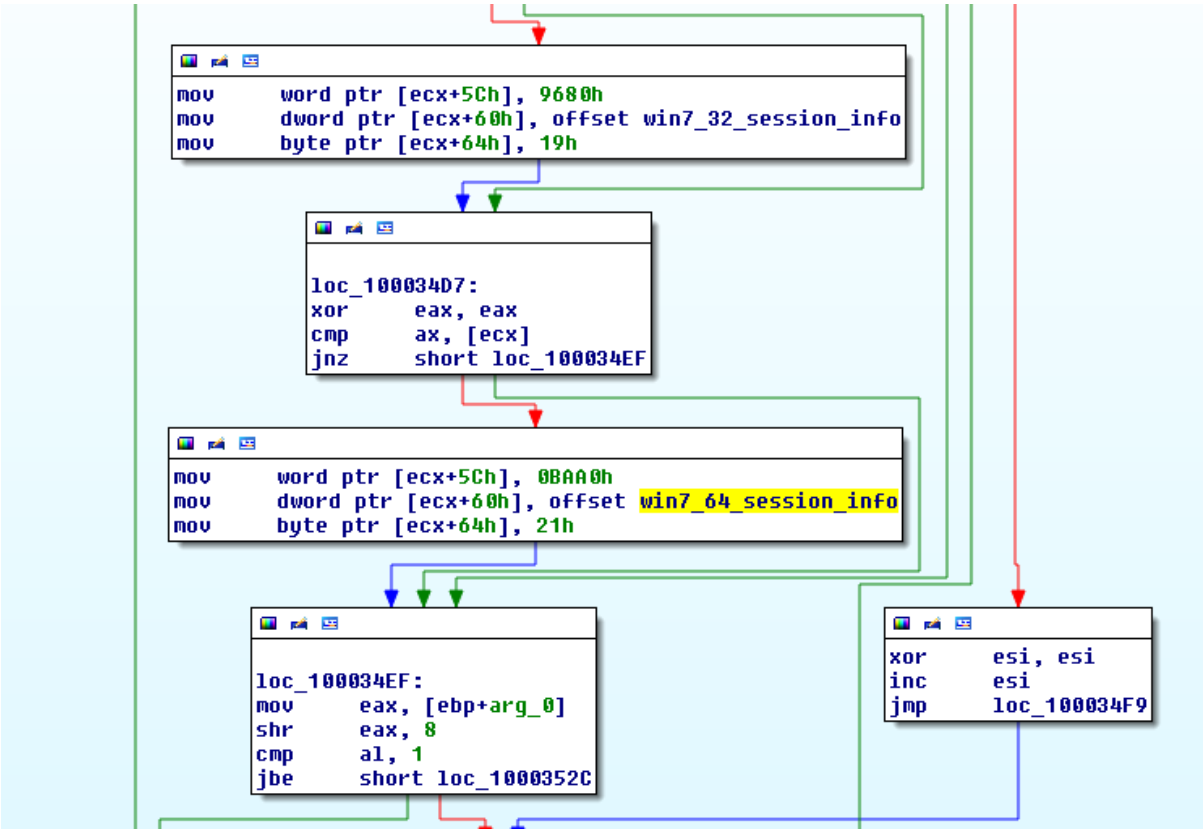

Figure 10 - Choice of EternalRomance payload

Yara Rules

```
import "pe"

rule BadRabbit_dropper {

	meta:
		description = "Yara Rule for Bad Rabbit dropper identification"
		author = "CSE CybSec Enterprise - Z-Lab"
		last_updated = "2017-10-31"
		tlp = "white"
		category = "informational"

	strings:
		// Flash string
		$flash = "Flash" wide

		// File infpub extracted
		$a = "C:\\Windows\\infpub.dat" wide
		$b = "infpub.dat" wide

		// Execution of infpub.dat
		$c = "%ws C:\\Windows\\%ws,#1 %ws" wide

	condition:
		all of them and
```

```
            pe.version_info["ProductName"] contains "Installer/Uninstaller"

}

rule BadRabbit_infpub {

      meta:
            description = "Yara Rule for Bad Rabbit infpub.dat file"
            author = "CSE CybSec Enterprise - Z-Lab"
            last_updated = "2017-10-31"
            tlp = "white"
            category = "informational"

      strings:

            // Task commands
            $a = "schtasks /Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR \"%ws /C
Start \\\"\\\" \\\"%wsdispci.exe\\\" -id %u && exit" wide

            //lateral movement instruction
            $b = "%ws\\admin$\\%ws" wide

            //part of public key
            $key =
"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5clDuVFr5sQxZ+feQlVvZcEK0k4uCSF5SkOkF9A3tR
6O" wide

      condition:
            all of them

}

rule BadRabbit_DiskCryptor_client {

      meta:
            description = "Yara Rule for Bad Rabbit dispci.exe file"
            author = "CSE CybSec Enterprise - Z-Lab"
            last_updated = "2017-10-31"
            tlp = "white"
            category = "informational"

      strings:

            // PhysicalDrive path
            $a = ".\\PhysicalDrive%d" wide

            // GameOfThrones Strings
            $b = "viserion" wide
            $c = "drogon" wide
            $d = "rhaegal" wide

      condition:
            all of them and
            pe.version_info["ProductName"] contains "GrayWorm" and
            pe.version_info["LegalCopyright"] contains "http://diskcryptor.net"

}
```

CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com