IIT KANPUR

Indian Institute of Technology, Kanpur

Project 3

Problem Statement :-

Run and analyze files on cuckoo that are marked as malware and those marked as benign applications. Inspect the reports generated by cuckoo on each individual malware and then answer the questions in a typed (using MS word or latex) form, generate a pdf file and upload it on Talent Sprint Portal.

Abhishek Verma

NAMING CONVENTION FOLLOWED-

Sample No.	**Time of execution**	**Actual file Name**	**Status**	**Analysis Score**
1	2020-11-07 17:42	01_VirusShare_0a426257e0f45255f4a7366c6e0a309e(Malware-1)	reported	score: 5.2
2	2020-11-07 17:43	02_VirusShare_0b109c1cb3f6ae1eb5c8d415e9643c07(Malware-2)	reported	score: 3
3	2020-11-07 17:45	03_VirusShare_3d2ec4d503e282cc0db13d662b92c5e8(Malware-3)	reported	score: 5.2
4	2020-11-07 17:46	04_VirusShare_4c2fdd9f819d6b551df945c6bf5faec7(Malware-4)	reported	score: 5.2
5	2020-11-07 17:48	05_VirusShare_8acf123b9576b7e76c930637ab67f43b(Malware-5)	reported	score: 5.2
6	2020-11-07 17:49	06_VirusShare_65b23015f3b67ec35381c0fff4209b21(Malware-6)	reported	score: 5.2
7	2020-11-07 17:51	07_VirusShare_085de2518f08f8541d71b5e7fead31b4(Malware-7)	reported	score: 5.2
8	2020-11-07 17:52	08_VirusShare_427a1136e5e470964ec6aa3a7bd991f8(Malware-8)	reported	score: 5.2
9	2020-11-07 17:54	09_VirusShare_0611ee394f9c236fc5b3197b8c1f3691(Malware-9)	reported	score: 5.2
10	2020-11-07 17:57	10_VirusShare_d8ecc13aba2945c22e6a6f92a26d7e01(Malware-10)	reported	score: 3.2

11	2020-11-07 18:31	1-(Benign -1)	reported	score: 0.6
12	2020-11-07 18:35	2-(Benign -2)	reported	score: 4
13	2020-11-07 18:37	3-(Benign -3)	reported	score: 0
14	2020-11-07 18:38	4-(Benign -4)	reported	score: 0.4
15	2020-11-07 18:41	5-(Benign -5)	reported	score: 1.8
16	2020-11-07 18:43	7-(Benign -6)	reported	score: 0
17	2020-11-07 18:45	8-(Benign -7)	reported	score: 4
18	2020-11-07 18:47	10-(Benign -8)	reported	score: 0
19	2020-11-07 18:50	19-(Benign -9)	reported	score: 2.4
20	2020-11-07 18:53	BDUSBImmunizerLauncher.exe(Benign -10)	reported	score: 4

Q1. From the reports on the malware – do you see one or more malware trying to detect that it is being executed on a virtual machine? What are the indications you are finding – which makes you believe it (they) is (are) trying to detect whether it is running on a VM?

A1.

Sl. No.	Malware Sample	Parameter 1- Virtual Machines	Parameter 2- Global Memory	Parameter 3- Virtual Interfaces	Parameter 4- Registry keys
1	Malware 01	Yes	Yes	Yes	No
2	Malware 02	Yes	Yes	No	No
3	Malware 03	Yes	Yes	Yes	No
4	Malware 04	Yes	Yes	Yes	No
5	Malware 05	Yes	Yes	Yes	No
6	Malware 06	Yes	Yes	Yes	No
7	Malware 07	Yes	Yes	Yes	No
8	Malware 08	Yes	Yes	Yes	No
9	Malware 09	Yes	Yes	Yes	No
10	Malware 10	No	No	No	Yes

Parameter 1: WMI query to identify virtual machines (Select * from Win32_ComputerSystem)

Parameter 2: GlobalMemoryStatusEx

Parameter 3: GetAdaptersAddresses

Parameter 4: Registry Keys

1) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions

2) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VBoxGuest

----

Q2. Count the number of files created by each malware and add them up as count1. Count the number of files created by the benign applications, and add them up as count 2? Do you see any marked difference between count1 and count2? Explain

A2.

Sl. No	**Malware Sample**	**No. of Files created**
01	Malware 01, Malware 03, Malware 04, Malware 05, Malware 06, Malware 07, Malware 08, Malware 09	**11 Files created for each**
02	Malware 02	**14**
03	Malware 10	**00**
Total(Count 1)		**102**

Sl. No.	**Benign Sample**	**No. of Files created**
01	Benign 01	**01**
02	Benign 02	**12**
03	Benign 03	**00**

04	Benign 04	**01**
05	Benign 05	**01**
06	Benign 06	**00**
07	Benign 07	**05**
08	Benign 08	**00**
09	Benign 09	**02**
10	Benign 10	**07**
Total(Count 2)		**29**

The remarkable difference between the count for files created by malwares (Count 1) and files created by Benign binaries (Count 2) can be attributed to the fact that in the first stage of infection itself , most malware installer either install a dropper (which later executes to unpack the malicious binary thus increasing the number of files) or a downloader (in case which it downloads these malicious files from the internet) thus adding to the count.

Another reason could be that most malware authors today follow an approach to either install the malware in one go or do not install in order to avoid corrupted installation (bad sectors, etc.). They follow something called atomicity while writing malware (acquire a write lock , write everything in tmp , copy from temp).This results in a bunch of malware files in temp directory as we observed.

Also if the temp files are present then they can use these files to resume the installation in case there is a crash during the write operation on malware.(Recovery from crash during write).

Q3. Count the number of files deleted by each malware and add them up as count3. Count the number of files created by the benign applications, and add them up as count 4? Do you see any marked difference between count3 and count 4? Explain.

A3.

Sl. No	**Malware Sample**	**No. of Files deleted**
01	Malware 01, Malware 03, Malware 04, Malware 05, Malware 06, Malware 07, Malware 08, Malware 09	**04 Files deleted for each**
02	Malware 02	**04**
03	Malware 10	**00**
Total(Count 3)		**36**

Sl. No.	**Benign Sample**	**No. of Files deleted**
01	Benign 01	**01**
02	Benign 02	**05**
03	Benign 03	**00**
04	Benign 04	**01**
05	Benign 05	**00**
06	Benign 06	**00**
07	Benign 07	**04**

08	Benign 08	**00**
09	Benign 09	**00**
10	Benign 10	**01**
Total(Count 4)		**12**

Possibly the malware executor does so to hide the traces or to avoid giving undue suspicion to end-user that some malicious program has been installed on his/her system. Although all these steps are generally followed after successful installation of the malicious program in the system.

Q4. Count the number of files written to by each malware and add them up as count5. Count the number of files written to by the benign applications, and add them up as count 6? Do you see any marked difference? Explain.

A4.

Sl. No.	Malware Sample	No. of Files Written
1	Malware 01	**10**
2	Malware 02	**12**
3	Malware 03	**10**
4	Malware 04	**10**
5	Malware 05	**10**
6	Malware 06	**10**
7	Malware 07	**10**
8	Malware 08	**10**

9	Malware 09	**10**
10	Malware 10	**0**
Total(Count5)		**92**

Sl. No.	**Malware Sample**	**No. of Files Written**
1	Benign 01	**1**
2	Benign 02	**11**
3	Benign 03	**0**
4	Benign 04	**0**
5	Benign 05	**0**
6	Benign 06	**0**
7	Benign 07	**4**
8	Benign 08	**0**
9	Benign 09	**1**
10	Benign 10	**5**
Total(Count6)		**22**

The malware sample have written to more files as opposed to benign files , since malwares create a lot of temp files as explained above (following the principle of atomic write)

Q5. Which category of files (malware or benign) are creating more directories?

A5.

Sl. No.	Malware Sample	No. of Directories Created
1	Malware 01	**4**
2	Malware 02	**4**
3	Malware 03	**4**
4	Malware 04	**4**
5	Malware 05	**14**
6	Malware 06	**4**
7	Malware 07	**4**
8	Malware 08	**4**
9	Malware 09	**4**
10	Malware 10	**0**
Total(Count7)		**46**

Sl. No.	Malware Sample	No. of Directories Created
1	Benign 01	**0**
2	Benign 02	**9**
3	Benign 03	**1**
4	Benign 04	**0**

5	Benign 05	**0**
6	Benign 06	**0**
7	Benign 07	**1**
8	Benign 08	**0**
9	Benign 09	**0**
10	Benign 10	**1**
Total(Count 8)		**12**

Malwares have created more directories.

--

Q6. While category of files (malware or benign) opened more registry keys?

A6.

Sl. No.	Malware Sample	No. of Registry keys Opened
01	Malware 01	504
02	Malware 02	283
03	Malware 03	503
04	Malware 04	504
05	Malware 05	503
06	Malware 06	503
07	Malware 07	503
08	Malware 08	503
09	Malware 09	504
10	Malware 10	10
Total		4320

Sl. No.	Benign Sample	No. of Registry keys Opened
01	Benign 01	03
02	Benign 02	494
03	Benign 03	229
04	Benign 04	31
05	Benign 05	32
06	Benign 06	00
07	Benign 07	13
08	Benign 08	00
09	Benign 09	944
10	Benign 10	163
Total		1909

The malwares opened more registry key.

Q7. Are any of the files trying to resolve any URL names to IP addresses? If so, which category (malware or benign) are they?

A7.

Sl. No.	Malware Sample	Resolve URL names to IP
01	Malware 01, Malware 03, Malware 04, Malware 05, Malware 06, Malware 07, Malware 08, Malware 09,	04 each ("dtrack.secdls.com", "api.v2.secdls.com", “wpad”, “Cuckoo2-PC”)

		(Of which the first two appear to be genuine URLs and the other two simply appear in the section of resolving URLs)
02	Malware 02	00 (As per Cuckoo analysis Results) (However further analysis indicate other domain(s) as well viz. “ocsp.thawte.com “)
03	Malware 10	00 (As per Cuckoo analysis Results) (However further analysis indicate other domain(s) as well viz. “report.179q1793my9cei9q.com “ and “report.93m7g3i7931q9w17yw1.com”)

Sl. No.	**Benign Sample**	**Resolve URL names to IP**
01	Benign 01	00
02	Benign 02	02 ("dl.mycommerce.com", "cdn.simtel.net")
03	Benign 03	00
04	Benign 04	00
05	Benign 05	00
06	Benign 06	00
07	Benign 07	00
08	Benign 08	00
09	Benign 09	00
10	Benign 10	01 (“ labs.bitdefender.com")

More malwares as opposed to benign files try to resolve URLs to IP Address. Under the resolve host classification, we see urls , the hostname and reference to wpad (The Web Proxy Auto-Discovery Protocol is a method used by clients to locate the URL of a configuration file using DHCP and/or DNS discovery methods).

Q8. Which category of files on average imported more DLLs? What APIs are being imported and exported (make two lists – one combined list for all DLLs and imported functions by malware files, and another combined list of all DLLs and imported functions by benign files)? Make some observations on the differences between the two lists.

A8.

Sl. No.	Malware Sample	No. of DLLs imported
01	Malware 01	102
02	Malware 02	18
03	Malware 03	103
04	Malware 04	105
05	Malware 05	103
06	Malware 06	104
07	Malware 07	104
08	Malware 08	103
09	Malware 09	103
10	Malware 10	15

Sl. No.	Benign Sample	No. of DLLs imported
01	Benign 01	05
02	Benign 02	77
03	Benign 03	25
04	Benign 04	09
05	Benign 05	15
06	Benign 06	00
07	Benign 07	10
08	Benign 08	00

09	Benign 09	51
10	Benign 10	44

The malware samples have imported more dlls viz. Microsoft.mshtml.dll, RpcRtRemote.dll, ws2_32.dll ,etc. (a list of dlls used is given below) .The malware samples have mostly used DLLs present in the temp folder which may indicate a DLL hi-jacking too.

Distinct Malware DLLs

SL No.	Malware Dll
1	C:\\Windows\\system32\\pnrpnsp.dll
2	DNSAPI.dll
3	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\diasymreader.dll
4	UxTheme.dll
5	C:\\Windows\\system32\\ole32.dll
6	dwmapi.dll
7	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System.Drawing\\dbfe8642a8ed7b2b103ad28e0c96418a\\System.Drawing.ni.dll
8	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System.Configuration\\bc09ad2d49d8535371845cd7532f9271\\System.Configuration.ni.dll
9	ImgUtil.dll
10	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\OLEAUT32.dll
11	PROPSYS.dll
12	C:\\Windows\\assembly\\GAC_MSIL\\System\\2.0.0.0__b77a5c561934e089\\rasapi32.dll
13	API-MS-WIN-Service-winsvc-L1-1-0.dll
14	advapi32.dll
15	ole32.dll
16	SHLWAPI.dll

17	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System.Management\\6f3b99ed0b791ff4d8aa52f2f0cd0bcf\\System.Management.ni.dll
18	C:\\Windows\\System32\\mswsock.dll
19	SHELL32.dll
20	CFGMGR32.dll
21	C:\\Windows\\assembly\\GAC_MSIL\\System\\2.0.0.0__b77a5c561934e089\\winhttp.dll
22	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System.Xml\\461d3b6b3f43e6fbe6c897d5936e17e4\\System.Xml.ni.dll
23	urlmon.dll
24	ntdll
25	apphelp.dll
26	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\Gdiplus.dll
27	kernel32.dll
28	oleaut32.dll
29	ntdll.dll
30	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\ole32.dll
31	C:\\Windows\\system32\\napinsp.dll
32	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\culture.dll
33	cryptsp.dll
34	WININET.dll
35	API-MS-Win-Core-LocalRegistry-L1-1-0.dll
36	user32
37	MLANG.dll
38	rtutils.dll
39	IPHLPAPI.DLL
40	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\Accessibility\\9859a6e0562f64eacfb8ad76f260a2d6\\Accessibility.ni.dll
41	RASAPI32.dll

42	oleacc.dll
43	profapi.dll
44	comctl32.dll
45	VERSION.dll
46	C:\\Windows\\assembly\\GAC\\Microsoft.mshtml\\7.0.3300.0__b03f5f7f11d50a3a\\Microsoft.mshtml.dll
47	RpcRtRemote.dll
48	C:\\Windows\\assembly\\GAC_MSIL\\System.Windows.Forms\\2.0.0.0__b77a5c561934e089\\uxtheme.dll
49	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\\\wminet_utils.dll
50	C:\\Windows\\SysWOW64\\oleaut32.dll
51	user32.dll
52	ws2_32.dll
53	gdi32.dll
54	iphlpapi
55	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\mscorjit.dll
56	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\mscorlib\\62a0b3e4b40ec0e8c5cfaa0c8848e64a\\mscorlib.ni.dll
57	mshtml.dll
58	SspiCli.dll
59	C:\\Windows\\assembly\\GAC_MSIL\\System.Windows.Forms\\2.0.0.0__b77a5c561934e089\\oleacc.dll
60	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs3A06.tmp
61	sensapi.dll
62	C:\\Windows\\assembly\\GAC_MSIL\\System\\2.0.0.0__b77a5c561934e089\\ws2_32.dll
63	NSI.dll
64	C:\\Windows\\system32\\NLAapi.dll
65	SXS.DLL
66	SETUPAPI.dll

67	IEFRAME.dll
68	gdiplus.dll
69	kernel32
70	credssp.dll
71	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System.Windows.Forms\\3afcd5168c7a6cb02eab99d7fd71e102\\System.Windows.Forms.ni.dll
72	C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System\\9e0a3b9b9f457233a335d7fba8f95419\\System.ni.dll
73	C:\\Windows\\WinSxS\\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\\gdiplus.dll
74	C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\mscorwks.dll
75	ntmarta.dll
76	C:\\Windows\\assembly\\GAC_MSIL\\System.Windows.Forms\\2.0.0.0__b77a5c561934e089\\comctl32.dll
77	API-MS-WIN-Service-Management-L1-1-0.dll
78	rasadhlp.dll
79	dnsapi
80	RASMAN.DLL
81	winhttp.dll
82	API-MS-Win-Security-SDDL-L1-1-0.dll
83	DHCPCSVC.DLL
84	RPCRT4.dll
85	C:\\Windows\\System32\\winrnr.dll
86	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\shell32.dll
87	mscoree.dll
88	ws2_32
89	C:\\Windows\\system32\\Msimtf.dll
90	NETMSG
91	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\nsb6DAB.tmp\\nsExec.dll

92	SHFOLDER
93	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\nsb6DAB.tmp\\System.dll
94	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs90F0.tmp
95	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs3E9A.tmp
96	C:\\Windows\\syswow64\\MSCTF.dll
97	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs34E6.tmp
98	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs5FED.tmp
99	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs6443.tmp
100	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs53C8.tmp
101	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\dfs777D.tmp
102	msvcrt.dll
103	PSAPI.DLL

Distinct Benign DLLs

Sl No.	Benign - DLL
1	dwmapi.dll
2	version.dll
3	C:\\Program Files (x86)\\Common Files\\microsoft shared\\ink\\tiptsf.dll
4	C:\\Windows\\system32\\dsrole.dll
5	C:\\Windows\\system32\\uxtheme.dll
6	IEFRAME.dll
7	DHCPCSVC.DLL
8	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\2LOC.dll

9	C:\\Windows\\system32\\pnrpnsp.dll
10	mshtml.dll
11	C:\\Windows\\System32\\mswsock.dll
12	apphelp.dll
13	rasadhlp.dll
14	kernel32.dll
15	comdlg32.dll
16	oledlg.dll
17	C:\\Windows\\system32\\ole32.dll
18	AUDIOSES.DLL
19	C:\\Program Files\\Internet Explorer\\ieproxy.dll
20	shlwapi.dll
21	C:\\Windows\\system32\\napinsp.dll
22	iphlpapi
23	wdmaud.drv
24	sensapi.dll
25	msacm32.drv
26	API-MS-WIN-Service-Management-L2-1-0.dll
27	C:\\Windows\\system32\\WINMM.dll
28	API-MS-WIN-Service-Management-L1-1-0.dll
29	API-MS-Win-Security-SDDL-L1-1-0.dll
30	urlmon.dll
31	C:\\Windows\\syswow64\\MSCTF.dll
32	WININET.dll
33	dnsapi
34	Secur32.dll
35	OLEAUT32.DLL

36	API-MS-WIN-Service-winsvc-L1-1-0.dll
37	IPHLPAPI.DLL
38	DNSAPI.dll
39	ole32.dll
40	ws2_32
41	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\2ENU.dll
42	USER32.dll
43	Comctl32.dll
44	wscapi.dll
45	IMM32.dll
46	RASMAN.DLL
47	rtutils.dll
48	C:\\Windows\\SysWOW64\\oleaut32.dll
49	midimap.dll
50	MMDEVAPI.DLL
51	API-MS-Win-Core-LocalRegistry-L1-1-0.dll
52	uxtheme.dll
53	profapi.dll
54	SHELL32.dll
55	RPCRT4.dll
56	RASAPI32.dll
57	C:\\Windows\\System32\\winrnr.dll
58	C:\\Windows\\system32\\NLAapi.dll
59	SXS.DLL
60	WINMM.dll
61	CFGMGR32.dll
62	GDI32.dll

63	MLANG.dll
64	WINSPOOL.DRV
65	ADVAPI32.dll
66	SETUPAPI.dll
67	WS2_32.dll
68	oleacc.dll
69	C:\\Windows\\system32\\ntshrui.dll
70	C:\\PROGRA~2\\MICROS~1\\Office12\\GR469A~1.DLL
71	PROPSYS.dll
72	C:\\Windows\\system32\\EhStorShell.dll
73	CRYPTSP.dll
74	WINTRUST.dll
75	WindowsCodecs.dll
76	netutils.dll
77	MSImg32.dll
78	gdi32
79	Kernel32
80	vb6stkit.dll
81	shell32
82	C:\\Windows\\system32\\user32.dll
83	API-MS-Win-Security-LSALookup-L1-1-0.dll
84	C:\\Windows\\system32\\advapi32.dll
85	C:\\Windows\\system32\\cabinet.dll
86	C:\\Windows\\system32\\version.dll
87	C:\\Windows\\system32\\kernel32.dll
88	advapi32
89	C:\\Program Files (x86)\\Windows Defender\\mpclient.dll

90	LINKINFO.dll
91	C:\\Windows\\system32\\DUser.dll
92	MsftEdit.dll
93	msls31.dll
94	ntdll.dll
95	slc.dll
96	ntmarta.dll
97	SHDOCVW.dll
98	C:\\Windows\\SysWOW64\\actxprxy.dll
99	comctl32
100	UIAutomationCore.dll
101	msctf.dll
102	C:\\Windows\\system32\\xmllite.dll
103	XmlLite.dll
104	DUser.dll
105	DUI70.dll
106	ntshrui.dll
107	winhttp.dll
108	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\BDUSBImmunizerLauncherENU.dll
109	SspiCli.dll
110	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\BDUSBImmunizer\\WSUtils.dll
111	credssp.dll
112	C:\\Windows\\system32\\dwmapi.dll
113	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\BDUSBImmunizer\\bdnimbus.dll
114	C:\\Users\\cuckoo2\\AppData\\Local\\Temp\\BDUSBImmunizerLauncherLOC.dll