Introduction

Malware forensic analysis provides the ability to analyze and understand the operation of malicious code (Trojans, viruses, rootkits, etc.) to assess the damage caused and assess the intentions and attacker capabilitie (Or-Meir et al., 2019). Knowing the structure, operation, and interaction of malware will provide valuable information, not only for the design and development of countermeasures effective but also to help identify the source of an attack and assess the detection capacity of the organization's systems at the time of taking the necessary and appropriate response actions.

Two malware analysis procedure are followed in this paper. The static analysis that involves analyzing malware at rest incorporates tools including virustotal, PEview, PEStudio, PEiD, and strings.exe. Dynamic analysis involves analysis while the malware executes. The tools involved include Wireshark, ProcMon, Process Explorer, Regshot, and Fakenet.

Static analysis

Virustotal

The file was uploaded to the virustotal.com to check if the malware was malicious or not. 53 out of 69 antivirus engines flagged the file as malicious as shown in the figure below

				- 00
53	() 53 security vendors and 1 sandbox flagged this file as malicious			C 🔛
2 2 Community √ Score	1679b0861649d92456b21600281e3be7169e955830319e7168063ab76379 Synaptics.exe bobsoft @etect-debug-environment @rect-cpu-clock-access long-sleeps		4.43 MB 2021-12-31 16:24:46 UTC Size 6 days ago	exe exe
DETECTION	DETAILS RELATIONS BEHAVIOR COMMUNITY			
Acronis (Static ML)	① Suspicious	Ad-Aware	Dropped:Trojan.GenericKD.3794	0051
AhnLab-V3	Win32/Zorex.X1799	ALYac	() Dropped:Trojan.GenericKD.3794	0051
Antiy-AVL	() Trojan/Generic.ASMacro.5657	Arcabit	() HEUR.VBA.Trojan.d	
AVG	() Other:Malware-gen [Trj]	Avira (no cloud)	() WORM/Dldr.Agent.gqrxn	
BitDefender	Dropped:Trojan.GenericKD.37940051	BitDefenderTheta	() Al:Packer.F5AF03D517	
CAT-QuickHeal	W32.Delf.NB4	Comodo	() Virus.Win32.Agent.DE@74b38h	
CrowdStrike Falcon	() Win/malicious_confidence_100% (D)	Cybereason	() Malicious.55e064	
Cylance	① Unsafe	Cynet	() Malicious (score: 100)	
Cyren	() W32/Backdoor.OAZM-5661	DrWeb	() Trojan.DownLoader22.9658	

The following hash values were identified

MD5 ff7276155e0641b40dfc36e1cf315d70

SHA-12fd07b03fda2bf8bc43cd9ea9446ea40aa10b24a

SHA-256 1679b086f649d92456b2f60028fe3be7169e955830319e7f68063ab76379a37e

Basic Properti	ies 🛈									
MD5	ff7276155e0641b40dfc36e1cf315d70									
SHA-1	2fd07b03fda2bf8bc43cd9ea9446ea40aa10b24a									
SHA-256	1679b086f649d92456b2f60028fe3be7169e955830319e7f68063ab76379a37e									
Vhash	0460866d5c0d5c051565503162z41z32z13z1035z23z40305bz									
Authentihash	0f3320d3dbdb717b5fb287667a64e346487899addb592df1af902b2ad647fb9a									
Imphash	332f7ce65ead0adfb3d35147033aabe9									
SSDEEP	98304:8nsmtk2aN+hfTKQGEpz3xjlZwZC2vJhdO6qTrELwRxNjuAAPgg/ut9OQ9iAm/53X:SLM+hfzzxUJhdOLTrELwRxNjuAAPgg/F									
TLSH	T1BD265BF1BDA14462C6131630783DEA78A9FFADA01B34478B529EF9582F323C708E9557									
File type	Win32 EXE									
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit									
TrID	Win32 Executable Borland Delphi 7 (62.2%)									
TrID	Windows Control Panel Item (generic) (18.4%)									
TrID	Windows ActiveX control (10.9%)									
TrID	InstallShield setup (4%)									
TrID	Win32 Executable Delphi generic (1.3%)									
File size	4.63 MB (4858880 bytes)									
PEiD packer	BobSoft Mini Delphi -> BoB / BobSoft									

From the figure above it is also identified that the file type is win32 EXE and its size is 4.83 MB. The PEiD packer indicates that the file is packed.

The file makes some network communication as it contacts 5 domains, 2 URLs, and 6 IP addresses as shown in the figure below

DETECTION	DETAILS RE	LATIONS BEHAVIOR	COMMUNITY	
Contacted URLs	0			(
Scanned	Detections	Status	URL	
2022-01-06	3 / 93	200	http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978	
2021-12-31	0 / 93	200	http://pki.goog/gsr1/gsr1.crt	
Contacted Domain	s (i)			l
Domain	Detections	Created	Registrar	
xred.mooo.com	4 / 90	2000-03-24	Domain.com, LLC	
freedns.afraid.org	2/90	1999-09-21	ENOM, INC.	
pki.goog	0 / 90	2016-06-13	Charleston Road Registry Billable	
docs.google.com	0 / 90	1997-09-15	MarkMonitor Inc.	
arc.msn.com	0 / 90	1994-11-10	MarkMonitor Inc.	
Contacted IP Addre	esses (1)			
IP	Detections	Autonomous System	Country	
69.42.215.252	0 / 90	17048	US	
216.239.32.29	0 / 90	15169	US	
224.0.0.252	0 / 90	-	e de la construcción de la constru	
142.250.81.206	0 / 90	15169	US	
108.177.127.101	0 / 90	15169	US	
20.82.209.183	0/90	8075	IE	

PEiD

Since virustotal.com indicated that the file is packed, PEiD was used to confirm that. It was identified the malware is packed with Borland Delphi 6.0 - 7.0 as shown in the figure below

🌃 PEiD ∨0.	95			_		×
File: C:\Us	ers\Windows10\[Desktop\FlyerSMT_H	V_2\FlyerS	MT_HV≬	FlyerSM	
Entrypoint:	0009AB80	EF	Section:	CODE		>
File Offset:	00099F80	Fi	rst Bytes:	55,8B,	EC,83	>
Linker Info:	2.25	Su	ubsystem:	Win32	GUI	>
Borland Del	phi 6.0 - 7.0					
Multi Scan	Task Viewer	r Options	Abo	ut	Exi	t
Stay on	top				**	->

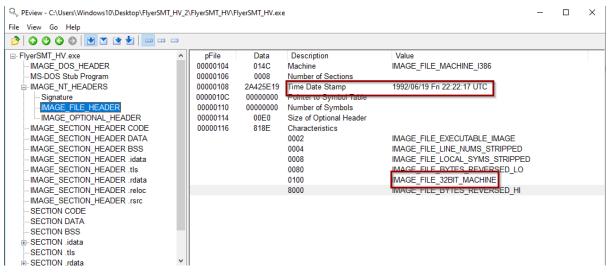
Strings

The strings of interest are as shown in the figure below

Administrator: Command Prompt @3@ kernel32.dll DeleteCriticalSection LeaveCriticalSection EnterCriticalSection InitializeCriticalSection VirtualFree VirtualAlloc LocalFree LocalAlloc GetVersion GetCurrentThreadId GetThreadLocale GetStartupInfoA GetLocaleInfoA GetCommandLineA FreeLibrary ExitProcess WriteFile UnhandledExceptionFilter RtlUnwind RaiseException GetStdHandle user32.dll GetKeyboardType MessageBoxA advapi32.dll RegQueryValueExA RegOpenKeyExA RegCloseKey kernel32.dll TlsSetValue TlsGetValue TlsFree TlsAlloc LocalFree LocalAlloc kernel32.dll UnmapViewOfFile OpenFileMappingA MapViewOfFile CloseHandle user32.dll UnhookWindowsHookEx SetWindowsHookExA PostMessageA CallNextHookEx KBHks.dll HookOff HookOn

PEView

PEView was used to gain the header information of the malware. It was identified that the malware Time Date Stamp was 1992/06/19 Fri 22:22:17 UTC. The malware runs in 32 bit machine as shown in the figure below.



The malware has the following imports

C PEview - C:\Users\Windows10\Desktop\FlyerSMT_HV_2\FlyerSMT_HV\FlyerSMT_HV.exe

File View Go Help								
2 0 0 0 0 1 0 0 0 0								
	pFile	Data	Description	Value				
IMAGE_DOS_HEADER	0009D000	00000000	Import Name Table RVA					
MS-DOS Stub Program	0009D004	00000000	Time Date Stamp					
	0009D008	00000000	Forwarder Chain					
IMAGE_SECTION_HEADER CODE	0009D00C	000A0964	Name RVA	kernel32.dll				
IMAGE_SECTION_HEADER DATA	0009D010	000A01CC	Import Address Table RVA					
IMAGE_SECTION_HEADER BSS	0009D014	00000000	Import Name Table RVA					
IMAGE_SECTION_HEADER .idata	0009D018	00000000	Time Date Stamp					
IMAGE_SECTION_HEADER .tls	0009D01C	00000000	Forwarder Chain					
IMAGE_SECTION_HEADER .rdata	0009D020	000A0CCA	Name RVA	user32.dll				
IMAGE_SECTION_HEADER .reloc	0009D024	000A0290	Import Address Table RVA					
IMAGE_SECTION_HEADER .rsrc	0009D028	00000000	Import Name Table RVA					
SECTION CODE	0009D02C	00000000	Time Date Stamp					
SECTION DATA	0009D030	00000000	Forwarder Chain					
SECTION BSS	0009D034	000A0D10	Name RVA	advapi32.dll				
SECTION .idata	0009D038	000A02A4	Import Address Table RVA					
IMPORT Directory Table	0009D03C	00000000	Import Name Table RVA					
IMPORT Address Table	0009D040	00000000	Time Date Stamp					
IMPORT Hints/Names & DLL Names	0009D044	00000000	Forwarder Chain					
SECTION .tls	0009D048	000A0D50	Name RVA	oleaut32.dll				
SECTION .rdata	0009D04C	000A02B4	Import Address Table RVA					
SECTION .reloc	0009D050	00000000	Import Name Table RVA					
SECTION .rsrc	0009D054	00000000	Time Date Stamp					
	0009D058	00000000	Forwarder Chain					
	0009D05C	000A0D98	Name RVA	kernel32.dll				
	0009D060	000A02C4	Import Address Table RVA					
	0009D064	00000000	Import Name Table RVA					
	0009D068	00000000	Time Date Stamp					
	0009D06C	00000000	Forwarder Chain					
	0009D070	000A0DE4	Name RVA	advapi32.dll				
	0009D074	000A02D8	Import Address Table RVA					

PEStudio

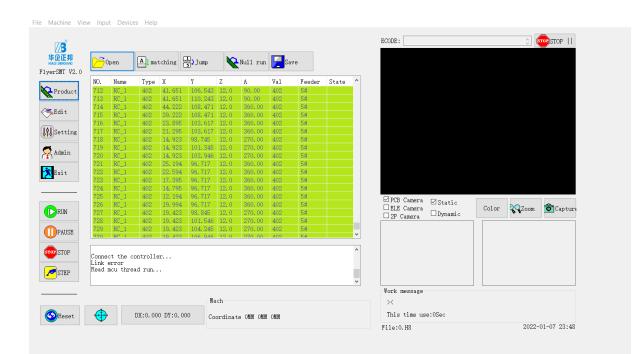
This tool was used to gain more information about the malware. The information gathered includes the indicators, the virustotal flags, and strings. Similar strings as indicated by the

strings.exe tool was identified. There were a total of 81 indicators of comprise, as shown in the figure below

settings about						
1 🗙 自 💡						
c:\users\windows10\desktop\flyersmt_hv_2\flyer	indicator (81)	detail	le			
- Jal indicators (81)	The file references string(s)	type: blacklist, count: 282				
Virustotal (53/69)	The file is scored by virustotal	score: 53/69				
 dos-header (64 bytes) dos-stub (192 bytes) 	The file contains another file	signature: executable, location: .rsrc, offset: 0x000B3614, size: 4087296				
dos-stub (192 bytes) ich-header (n/a)	The file contains another file	signature: executable, location: .rsrc, offset: 0x00499418, size: 15360				
 > file-header (Jun, 1992) 	The file contains another file	signature: PKZIP, location: .rsrc, offset: 0x0049D788, size: 18387 type: blackist, count: 19 urt: 127.0.0.1 urt: http://freedns.afraid.org/api/laction=getdyndns8xsha=a30fa98efc092684e8d1c5cff797bcc613				
 optional-header (GUI) 	The file imports symbol(s)					
directories (5)	The file references a URL pattern					
sections (files)	The file references a URL pattern					
libraries (12) *	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSVIVsOGIEVGxuZVk&export=download				
functions (161) *	The file references a URL pattern	url: https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1				
exports (n/a)	The file references a URL pattern	url: http://xred.site50.net/syn/SUpdate.ini				
••• tis-callbacks (n/a)	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download				
.NET (n/a)	The file references a URL pattern	url: https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1				
resources (executable) *	The file references a URL pattern	url: http://xred.site50.net/syn/Synaptics.rar				
abc strings (28367)	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSTmIVYkxhSDg5TzQ&export=download				
-🏦 debug (n/a)	The file references a URL pattern	url: https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1				
📲 manifest (n/a)	The file references a URL pattern	url: http://xred.site50.net/syn/SSLLibrary.dll				
version (1.0.0.0)	The file references file extensions like a Ransomware Wiper	count: 34				
certificate (n/a)	The file references a URL pattern	url: 2.0.0.0				
overlay (n/a)	The file contains another file	signature: unknown, location: .rsrc, offset: 0x000B35C0, size: 68				
	The file contains another file	signature: Delphi, location: .rsrc, offset: 0x000B3604, size: 16				
	The file contains another file	signature: unknown, location: .rsrc, offset: 0x00499414, size: 3				
	The file contains another file	signature: Delphi, location: .rsrc, offset: 0x0049D018, size: 1612				
	The file contains another file	signature: Delphi, location: .rsrc, offset: 0x0049D664, size: 339				
	The file-ratio of the resource(s) is high	ratio: 85.46 %				
	The file references blacklist library(ies)	count: 3				

Dynamic analysis

Dynamic analysis involves the analysis of the malware while the program is running. It uses different tools in the process, including procmon, process explorer, and regshot, which are all run before the malware is run (Ucci et al., 2019). Stimulation of the network by fakenet makes the malware run so that the analyst comprehends the analysis of what it does in the. Malware is also analyzed through regshot in the registry files, where the shots are taken simultaneously and compared. When the malware is run, a graphical user interface pops as shown in the figure below



Regshot

This tool allows an analyst to take two snapshots of the registry. The first snapshot is takes before the malware is executed and the second is taken after the malware is executed. The comparison of two snapshots helps the analyst identify the changes the malware makes in the registry, giving more indication as to what the malware is capable of, in case there is any files that are dropped or modified. The malware accesses the registry and makes different actions including deleting registry keys, adding values, and modifying values. There was a total of 221 changes made on the registry as shown in the figure below

	;
File Edit Format View Help	
<pre>Will(S-1-5-21-2081364252-1438397395-3132659045-1002_classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-143897395-3132659045-1002_classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-143897395-3132659045-1002_classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-143897395-3132659045-1002_classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-143897395-3132659045-1002_classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-143897395-3132659045-1002_classe\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUJ HKU\S-1-5-21-2081364252-143897395-3132659045-1002_classe\Local Settings\Software\Microsoft\Windows\LurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppData\Microsoft.Windows\KurrentVersion\AppModel\SystemAppDa</pre>	I_cw5n1ł I_cw5n1ł I_cw5n1ł I_cw5n1ł I_cw5n1ł I_cw5n1ł I_cw5n1ł I_cw5n1ł I_cw5n1ł (AUI\App (AUI\App 00 00 (00 (0))))))))))
Total changes: 221	
<	2
Ln 428, Col 35 100% Windows (CRLF) UTF-8	

Comparing the two snapshots, it was identified that the malware accesses the Current User Hive.

Process Explorer

Process Explorer tool gives access to the information when the malware executes. It offers a range of functionalities that are important to analyze the file (Chakkaravarthy et al., 2019). It was identified that the malware initiates a child process and then it kills the parent process. The child process was running with PID 5436. The color in the tool indicated that the malware is its process and is not packed. When verifying the signature, it was identified that the malware did not have any signature assigned to it as shown in the figure below. It means that the file has a malicious activity.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer		
Registry		2,956 K	37,924 K	72					
System Idle Process		60 K	8 K	0					
🗉 🔳 System	< 0.01	200 K	140 K	4					
Interrupts	< 0.01	0 K	0 K		Hardware Interrupts and DPCs				
smss.exe		1,060 K	856 K	336					
Memory Compression		2,072 K	263,508 K	1412					
Csrss.exe		1,548 K	4,444 K	432					
🗉 🔳 wininit.exe		1,332 K	5,732 K	500					
Csrss.exe	< 0.01	1,632 K	4,564 K	508					
🗉 🔳 winlogon.exe		2,440 K	9,216 K	564					
fontdrvhost.exe		3,740 K	8,608 K	716					
dwm.exe	1.54	67,088 K	102,636 K	900					
explorer.exe	< 0.01	52,724 K	134,168 K	2972	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows		
SecurityHealthSystray.exe		1,648 K	8,760 K	5648	Windows Security notificatio	Microsoft Corporation	(Verified) Microsoft Windows		
💑 VBoxTray.exe	< 0.01	2,356 K	9,804 K	5748	VirtualBox Guest Additions Tr	. Oracle Corporation	(Verified) Oracle Corporation		
OneDrive.exe		18,624 K	27,752 K		Microsoft OneDrive	Microsoft Corporation	(Verified) Microsoft Corporation		
Regshot-x64-ANSI.exe		158,104 K	11,360 K	1628					
💭 procexp64.exe	< 0.01	22,416 K	41,408 K			Sysintemals - www.sysinter	. (Verified) Microsoft Corporation		
Procmon64.exe		4,992 K	16,264 K	440	Process Monitor	Sysintemals - www.sysinter	. (Verified) Microsoft Corporation		
Procmon64.exe	< 0.01	266,564 K	197,676 K	5476					
🖃 🔳 FakeNet.exe		4,760 K	11,100 K	2896					
conhost.exe		6,912 K	18,488 K	3716					
ipconfig.exe		532 K	2,268 K	5660					
GoogleCrashHandler.exe		1,728 K	276 K	5460					
GeogleCreekHandlerC1.exe	-	1,910 K	332 K	5400					
cache_FlyerSMT_HV.exe	1.54	148,220 K	29,428 K		FlyerSMT	编写者:黄新建	(No signature was present in the subject) 编写者:黄新建		
Synaptics.exe		3,736 K	17,460 K	1460					

Procmon

This tool shows the real-time process activities, registry, and file systems. Similar to other malware dynamic analysis tools, ProcMon was executed before malware execution. The malware was filtered using the PID from process explorer and analysis was done to check the registry activities, file activities, and process/thread activities. After filtering the activities, it was identified that the malware's parent PID is 6492 as shown in the figure below. The malware accessed different files including

Proce	ess Monitor - Sysin	ternals:	www.sysinternals	s.com						- T X
File Ed	dit Event Filter	Tools	s Options He	lp			Event Properties			- 🗆
∋ 🖫] 🖸 🗔 🚺	ז ג	7 💋 🎯 🛃	品 🔗 P 기 📰 🖬	🖵 🕫 🔼		🔗 Event	Process	Stack	
lime	Process Name	PID	Operation	Path	Result	Detail	Date:	1/7/2022 11:45:3	3.7158342 PM	
1:45:	cache_FlyerS	5436	Process Start		SUCCESS	Parent PID: 6492,	Thread:	5624		
	cache_FlyerS		C Thread Create		SUCCESS	Thread ID: 1400				
	cache_RyerS			C:\Users\Windows10\Desktop\FlyerSM		Image Base: 0x4f0	Class:	Process		
1:45:	cache_RyerS		c [©] Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc	Operation:	Process Start		
			c₿Load Image	C:\Windows\SysWOW64\ntdl.dll	SUCCESS	Image Base: 0x76f				
	cache_FlyerS			C:\Windows\Prefetch\CACHE_FLYE			Result:	SUCCESS		
1:45:			📑 RegOpenKey	HKLM\System\CurrentControlSet\Contr.		Desired Access: Q	Path:			
			📑 RegOpenKey	HKLM\System\CurrentControlSet\Contr.		Desired Access: Q	Duration:	0.0000000		
	cache_FlyerS					Length: 80	Duration:	0.0000000		
1:45:	cache_FlyerS		RegCloseKey	HKLM\System\CurrentControlSet\Contr.						•
			📑 RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con		Desired Access: Q	Parent PID:		6492	
			📑 RegOpenKey	HKLM\System\CurrentControlSet\Contr.			Command line		C:\Use	s\Windows10\Desktop\FlyerSMT_HV_2\FlyerSMT_HVcache_FlyerSMT_HV.exe"
:45:	cache_FlyerS	5436	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con		Desired Access: Q	Current directo	ry:	C:\User	s\Windows10\Desktop\FlyerSMT_HV_2\FlyerSMT_HV\
			RegOpenKey	HKLM\System\CurrentControlSet\Contr.		Desired Access: Q	Environment:			
			RegQueryValue) Length: 24			=::=::\	
:45:	cache_FlyerS		RegCloseKey	HKLM\System\CurrentControlSet\Contr.						RSPROFILE=C:\ProgramData
			CreateFile	C:\Windows	SUCCESS	Desired Access: E				TA=C:\Users\Windows10\AppData\Roaming
	cache_FlyerS			C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffc				onProgramFiles=C:\Program Files (x86)\Common Files
:45:			c [©] Load Image	C:\Windows\System32\wow64win.dll	SUCCESS NAME NOT FOUND	Image Base: 0x7ffc				onProgramFiles(x86)=C:\Program Files (x86)\Common Files
	cache_FlyerS			C:\Windows\System32\wow64log.dll						onProgramW6432=C:\Program Files\Common Files
	cache_FlyerS			C:\Windows	SUCCESS	Desired Access: R				JTERNAME=DESKTOP-M7BIIGE
:45:	cache_FlyerS	5436	QueryNameInfo.		SUCCESS	Name: \Windows			ComSp	ec=C:\Windows\system32\cmd.exe
45			RegOpenKey	C:\Windows		Destruct Assessed D			DriverD	lata=C:\Windows\System32\Drivers\DriverData
1:45:	 cache_Hyer5 cache Flver5 			HKLM\Software\Microsoft\Wow64\x86 HKLM\SOFTWARE\Microsoft\Wow64\		Desired Access: R			FPS_BR	OWSER_APP_PROFILE_STRING=Internet Explorer
				HKLM\SOFTWARE\Microsoft\Wow64\ HKLM\SOFTWARE\Microsoft\Wow64\		Type: REG_SZ, Le				OWSER_USER_PROFILE_STRING=Default
1:45:	 cache_HyerS cache FlyerS 		Regulery value	HKLM\SOFTWARE\Microsoft\Wow64\ HKLM\SOFTWARE\Microsoft\Wow64\		type. neu_52, Le				DRIVE=C:
1:45	. cache FlyerS		celload Image	C:\Windows\System32\wow64cpu.dl	SUCCESS	Image Base: 0x76f				PATH=\Users\Windows10
	cache_RyerS			C: \Windows \System 32 \Wow64cpu.dll HKLM\System \CurrentControlSet \Contr.		Desired Access: Q				APPDATA=C:\Users\Windows10\AppData\Local
1:45:	Cache RyerS		RegOpenKey	HKLM\System\CurrentControlSet\Contr. HKLM\System\CurrentControlSet\Contr.		Desired Access: Q				ISERVER=\\DESKTOP-M7BIIGE
1:45	. cache RyerS		RegSetInfoKey	HKLM\System\CurrentControlSet\Contr. HKLM\System\CurrentControlSet\Contr.		KeySetInformation				ER_OF_PROCESSORS=1
			RegQueryValue							ve=C:\Users\Windows10\OneDrive
1:45:	cache_RyerS		RegCloseKey	HKLM\System\CurrentControlSet\Contr. HKLM\System\CurrentControlSet\Contr.		Longar. oo				ndows_NT
1:45:			RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Cont HKLM\SYSTEM\CurrentControlSet\Con		Desired Access: Q				:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\Sys
		5450	regopenney	internor or enrichtenteontoldet con	and their a structure	Deared racess. G			PATHEX	(T=.COM:.EXE:.BAT:.CMD:.VBS:.VBE:.JS:.JSE:.WSF:.WSH:.MSC

Wireshark

Wireshark was used to analyze the communication of the malware. It was identified that there is a traffic communication between the source, 10.0.2.15, and the destination, 69.42.215.252.

It initiates a http get method when it gets the dynamic DNS and sends to

http://freedns.afraid.org/ as shown in the figure below.

No.	Time	Source	Destination	Protocol	Length Info				
Г	3281 278.805972	10.0.2.15	69.42.215.252	TCP	66 60670 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1				
	3282 279.112265	69.42.215.252	10.0.2.15	TCP	60 80 \rightarrow 60670 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460				
	3283 279.112351	10.0.2.15	69.42.215.252	TCP	54 60670 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0				
+	3284 279.116030	10.0.2.15	69.42.215.252	HTTP	208 GET /api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978 HTTP/1.1				
	3285 279.116400	69.42.215.252	10.0.2.15	TCP	60 80 → 60670 [ACK] Seq=1 Ack=155 Win=65535 Len=0				
+	3286 279.455448	69.42.215.252	10.0.2.15	HTTP	297 HTTP/1.1 200 OK (text/html)				
	3287 279.455504	10.0.2.15	69.42.215.252	TCP	54 60670 → 80 [ACK] Seq=155 Ack=244 Win=65535 Len=0				
	3327 309.472689	69.42.215.252	10.0.2.15	TCP	60 80 → 60670 [FIN, ACK] Seq=244 Ack=155 Win=65535 Len=0				
L	3328 309.472759	10.0.2.15	69.42.215.252	TCP	54 60670 → 80 [ACK] Seq=155 Ack=245 Win=65535 Len=0				
> Frame 3284: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{A4015D42-371B-4DA7-9EBC-D87192671FCF}, id 0 > Ethernet II, Src: PcsCompu f1:a5:cd (08:00:27:f1:a5:cd), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)									
			2.15, Dst: 69.42.215.2						
			: 60670, Dst Port: 80,		Ack: 1, Len: 154				
	ypertext Transfer								
>	GET /api/?action	n=getdyndns&sha=a30fa9	08efc092684e8d1c5cff79	7bcc6135	62978 HTTP/1.1\r\n				
	User-Agent: MyAp	p\r\n							
	Host: freedns.at	fraid.org\r\n							
	Cache-Control: r	no-cache\r\n							
	\r\n								
	[Full request UF	RI: http://freedns.afr	raid.org/api/?action=g	etdyndns	<u>&sha=a30fa98efc092684e8d1c5cff797bcc613562978]</u>				
	[HTTP request 1/	/1]							
	[Response in fra	ame: 3286]							

Conclusion

The malware analysis presented in this paper has involved static analysis, dynamic analysis, and reverse engineering. The static analysis helped to gather information about the malware when it was at rest. The hash values, flags from antivirus engines, the header information, and the strings of interest are some of the information gathered from the static analysis. Dynamic analysis was used to gather more information about the malware. In the dynamic malware analysis, the malware was analyzed while running. Before its execution, the corresponding tools including regshot, ProcMon, Process explorer, fakenet, and Wireshark were set. The process explorer and procmon helped to know that the malware created a child process and then killed the process. It was also identified that the file did not have the signature but had the company name, and the path, confirming that it is a suspicious file from a legitimate organization. The regshot helped in getting the two snapshots of the registry, one before execution and one after malware execution. Therefore, it can be concluded that the file analyzed contains a trojan spyware which creates a child process that kills the original file when run. The malware collects user information and sends it to http://freedns.afraid.org/.

To remove the malware, follow the following steps

- 1. Start the PC in safe mode by opening system configuration, navigating to boot and then safe boot.
- 2. Show hidden files and folders from control panel
- 3. Remove all files from startup since it may contain autorun apps with trojans

- 4. Modify regedit file in the folder RUN
- 5. Clean the Temp folder
- 6. Start windows normally

References

- Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys (CSUR)*, *52*(5), 1-48.
- Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Computers & Security*, 81, 123-147.
- Chakkaravarthy, S. S., Sangeetha, D., & Vaidehi, V. (2019). A Survey on malware analysis and mitigation techniques. *Computer Science Review*, *32*, 1-23.