

## Part 2

# Basic Dynamic Analysis

What happens to our file system and registry if we run the malware.  
Can we detect any network traffic?

Keywords: Registry, files, network

# Warning

Caution! Caution!

Live Malware!

Caution! Caution!

# Basic Dynamic Analysis

**Lets run the malware and  
see what happens!**

- Also known as: Behavioral Analysis
- Interact with malware
- Help to find more IoC's

# Why Dynamic Analysis?

- Basic Static Analysis may have reached a dead-end:
  - Obfuscation
  - Packing
  - Tried all static analysis techniques
- Basic Dynamic Analysis
  - Efficient way to identify malware functionality
  - **What does it (malware) do?**

# Generic Procedure

## 5 Step Procedure:

1. Activate monitoring tools
2. Run malware
3. Terminate malware
4. Pause monitoring tools
5. Examine logs

**NB! Start and finish with clean image**

# Challenge 2

Use information available through basic dynamic analysis techniques to strengthen/reject your hypothesis about the purpose/functionality of the sample, based upon IoC's in registry, file and network activity

# Basic Dynamic Analysis

- Look for IoC in
    - Registry (e.g. Regshot and/or Process Monitor)
    - File (e.g. Regshot and/or Process Monitor)
    - Network Activity (e.g. wireshark)
- 1) Regshot
  - 2) Process Monitor
  - 3) Wireshark

# Regshot

Follow my demo



# Regshot suggested approach

- Clean img
- Open Process hacker and Regshot
- Unpack malware (pw – infected)
- Regshot: first shot (NB! Scan dir)
- Run spybot.exe as administrator
- wuaumqr.exe should start up
- After "some time" terminate wuaumqr.exe
- Regshot: 2 shot
- Regshot: Compare
  
- Variations:
  - Include Keyboard activity (look at keylog.txt)
  - Start twice, look at name

# Regshot results

## Files added

- C:\windows\system32\kazaabackupfiles\... (x14)
- C:\windows\system32\keylog.txt
- C:\windows\system32\wuaumqr.exe

## Folders added:

- C:\windows\system32\kazaabackupfiles

**Keys** added (not easy to detect until you see folder name added)

- ... \KAZAA
- ... \KAZAA\LocalContent

# Registry

```

7 -----
8 Keys added: 2
9 -----
10 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\KAZAA
11 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\KAZAA\LocalContent
12
13 -----
14 Values added: 9
15 -----
16 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Winsock driver: 77 75 61 75 6D 71 72 2E 65 78 65 00 78 78 78 00 23 7C 2D 7C 78 58 78 7C 2D 7C 00 78 54 72 69 70 6C 65 78 00 0A 00
    00 00 57 69 6E 73 6F 63 6B 20 64 72 69 76 65 72 00 00 53 00 00 00 6B 72 6E 65 6C 00 78 58 78 20 2D 20 54 72 69 70 6C 65 20 54 68 72 65 61 74 20 2D 20 78 58 78 00 01 00 00 00 14 3D
    41 00 05 3D 41 00 00 00 00 0B 1A 00 00 0A 1A 00 00 09 1A 00 00 08 1A 00 00 6B 65 79
17 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:Hfref\ERZ\Orfxgbc\fclo
    bg.rkr: 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF
    FF FF FF B0 03 0B 63 C3 DF D4 01 00 00 00 00
18 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\Microsoft\Windows\CurrentVersion\RunOnce\Winsock driver: 77 75 61 75 6D 71 72 2E 65 78 65 00 78 78 78 00 23 7C 2D 7C 78
    58 78 7C 2D 7C 00 78 54 72 69 70 6C 65 78 00 0A 00 00 00 57 69 6E 73 6F 63 6B 20 64 72 69 76 65 72 00 00 53 00 00 00 6B 72 6E 65 6C 00 78 58 78 20 2D 20 54 72 69 70 6C 65 20 54 68
    72 65 61 74 20 2D 20 78 58 78 00 01 00 00 00 14 3D 41 00 05 3D 41 00 00 00 00 0B 1A 00 00 0A 1A 00 00 09 1A 00 00 08 1A 00 00 6B 65 79
19 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\REM\Desktop\spybot.exe: 53 41
    43 50 01 00 00 00 00 00 00 07 00 00 00 28 00 00 00 20 AE 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 05 51 00 00 00 97 5F D8 91 C9 9E CE 01 00 00 00 00 00 00 00 00 02 00
    00 00 28 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D1 20 01 00 00 00 00 00 01 00 00 00 01 00 00 00
20 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\REM\Desktop\spybot.exe.FriendlyAppName:
    "Generic Host Process for Win32 Services"
21 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\REM\Desktop\spybot.exe.ApplicationCompany:
    "Microsoft Corporation"
22 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001\Software\KAZAA\LocalContent\Dir0: 30 31 32 33 34 35 3A 43 3A 5C 57 69 6E 64 6F 77 73 5C 73 79 73 74 65 6D 33 32 5C 6B 61 7A 61 61
    62 61 63 6B 75 70 66 69 6C 65 73 5C 00 00 00 00 00 00 00 00 00 9C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\REM\Desktop\spybot.exe.FriendlyAppName: "Generic Host
    Process for Win32 Services"
24 HKU\S-1-5-21-1897952862-3656991677-1792418944-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\REM\Desktop\spybot.exe.ApplicationCompany: "Microsoft
    Corporation"
25

```



NTNU

```
C:\Users\REM\AppData
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
~res-x86.txt
656 -----
657 Files added: 18
658 -----
659 C:\Windows\Prefetch\SPYBOT.EXE-EBF4C71B.pf
660 C:\Windows\Prefetch\WUAUMQR.EXE-6198254D.pf
661 C:\Windows\System32\kazaabackupfiles\AVP_Crack.exe
662 C:\Windows\System32\kazaabackupfiles\DreamweaverMX_Crack.exe
663 C:\Windows\System32\kazaabackupfiles\EDU_Hack.exe
664 C:\Windows\System32\kazaabackupfiles\FlashFXP_Crack.exe
665 C:\Windows\System32\kazaabackupfiles\Generals_No-CD_Crack.exe
666 C:\Windows\System32\kazaabackupfiles\Norton_Anti-Virus_2002_Crack.exe
667 C:\Windows\System32\kazaabackupfiles\PlanetSide.exe
668 C:\Windows\System32\kazaabackupfiles\Porn.exe
669 C:\Windows\System32\kazaabackupfiles\Postal_2_Crack.exe
670 C:\Windows\System32\kazaabackupfiles\Red_Faction_2_No-CD_Crack.exe
671 C:\Windows\System32\kazaabackupfiles\Renegade_No-CD_Crack.exe
672 C:\Windows\System32\kazaabackupfiles\Sitebot.exe
673 C:\Windows\System32\kazaabackupfiles\Winamp_Installer.exe
674 C:\Windows\System32\kazaabackupfiles\zoneallarm_pro_crack.exe
675 C:\Windows\System32\keylog.txt
676 C:\Windows\System32\wuaumgr.exe
677
678 -----
679 Files [attributes?] modified: 8
680 -----
681 C:\Users\REM\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
682 C:\Users\REM\ntuser.dat.LOG1
683 C:\Windows\AppCompat\Programs\Amcache.hve.LOG1
684 C:\Windows\Prefetch\CONSENT.EXE-65F6206D.pf
685 C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG2
686 C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG2
687 C:\Windows\System32\config\DEFAULT.LOG2
688 C:\Windows\System32\config\SYSTEM.LOG2
689
690 -----
691 Folders added: 1
692 -----
693 C:\Windows\System32\kazaabackupfiles
694
```

# Files

















File Home Share View

← → ▾ ↑ This PC ▸ Local Disk (C:) ▸ Windows ▸ System32 ▸ kazaabackupfiles

- ★ Favorites
- Desktop
- Documents
- Downloads
- Recent places

- This PC
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)

Network

<input type="checkbox"/> Name	Date modified	Type	Size
 AVP_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 DreamweaverMX_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 EDU_Hack.exe	1/8/2014 8:52 PM	Application	44 KB
 FlashFXP_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 Generals_No-CD_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 Norton_Anti-Virus_2002_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 PlanetSide.exe	1/8/2014 8:52 PM	Application	44 KB
 Porn.exe	1/8/2014 8:52 PM	Application	44 KB
 Postal_2_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 Red_Faction_2_No-CD_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 Renegade_No-CD_Crack.exe	1/8/2014 8:52 PM	Application	44 KB
 Sitebot.exe	1/8/2014 8:52 PM	Application	44 KB
 Winamp_Installer.exe	1/8/2014 8:52 PM	Application	44 KB
 zoneallarm_pro_crack.exe	1/8/2014 8:52 PM	Application	44 KB



File Home Share View

This PC &gt; Local Disk (C:) &gt; Windows &gt; System32

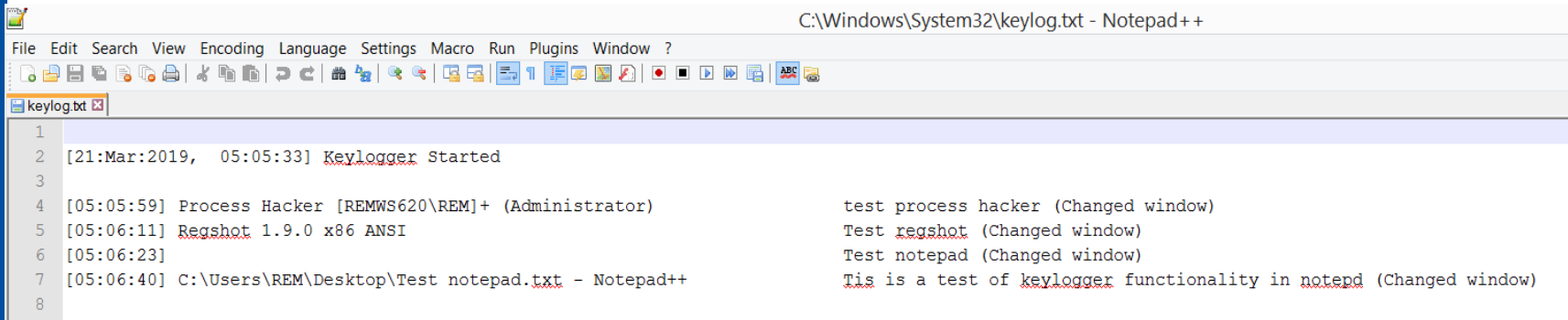
- ★ Favorites
- Desktop
- Documents
- Downloads
- Recent places

- This PC
  - Desktop
  - Documents
  - Downloads
  - Music
  - Pictures
  - Videos
  - Local Disk (C:)

- Network

<input type="checkbox"/>	Name	Date modified	Type	Size
<input type="checkbox"/>	kdnet.dll	8/22/2013 1:25 AM	Application extens...	82 KB
<input type="checkbox"/>	KdsCli.dll	8/21/2013 10:54 PM	Application extens...	69 KB
<input type="checkbox"/>	kdstub.dll	8/22/2013 1:25 AM	Application extens...	14 KB
<input type="checkbox"/>	kdusb.dll	8/22/2013 1:35 AM	Application extens...	39 KB
<input type="checkbox"/>	keepaliveprovider.dll	8/21/2013 10:46 PM	Application extens...	13 KB
<input type="checkbox"/>	kerberos.dll	9/21/2013 1:31 AM	Application extens...	739 KB
<input type="checkbox"/>	kernel.appcore.dll	8/22/2013 1:31 AM	Application extens...	30 KB
<input type="checkbox"/>	kernel32.dll	10/22/2013 2:14 A...	Application extens...	1,010 KB
<input type="checkbox"/>	KernelBase.dll	9/21/2013 5:14 AM	Application extens...	842 KB
<input type="checkbox"/>	kernelceip.dll	8/21/2013 11:55 PM	Application extens...	16 KB
<input type="checkbox"/>	KEY01.SYS	8/21/2013 9:42 PM	System file	9 KB
<input type="checkbox"/>	keyboard.drv	8/21/2013 9:42 PM	Device driver	9 KB
<input type="checkbox"/>	KEYBOARD.SYS	8/21/2013 9:42 PM	System file	9 KB
<input type="checkbox"/>	keyiso.dll	8/21/2013 10:48 PM	Application extens...	43 KB
<input checked="" type="checkbox"/>	keylog.txt	3/21/2019 4:18 AM	Notepad++ Docu...	1 KB
<input type="checkbox"/>	keymgr.dll	8/21/2013 11:26 PM	Application extens...	153 KB
<input type="checkbox"/>	klist.exe	8/22/2013 12:03 A...	Application	30 KB
<input type="checkbox"/>	kmddsp.tsp	8/22/2013 12:04 A...	TSP File	39 KB
<input type="checkbox"/>	KMSVC.DLL	8/21/2013 11:54 PM	Application extens...	74 KB

# Keylog.txt



```
C:\Windows\System32\keylog.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
keylog.txt
1
2 [21:Mar:2019, 05:05:33] Keylogger Started
3
4 [05:05:59] Process Hacker [REMWS620\REM]+ (Administrator) test process hacker (Changed window)
5 [05:06:11] Regshot 1.9.0 x86 ANSI Test regshot (Changed window)
6 [05:06:23] Test notepad (Changed window)
7 [05:06:40] C:\Users\REM\Desktop\Test notepad.txt - Notepad++ Tis is a test of keylogger functionality in notepad (Changed window)
8
```

# Changes filename

```

C:\Users\REM\AppData\Local\Temp\~res-x86.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
~res-x86.txt
00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 EC 56 69 C6 DF D4 01 00 00 00 00
1263
1264 -----
1265 Files added: 23
1266 -----
1267 C:\Windows\Prefetch\SPYBOT.EXE-EBF4C71B.pf
1268 C:\Windows\Prefetch\WUAUMQR.EXE-6198254D.pf
1269 C:\Windows\Prefetch\XUGWMPK.EXE-75008C3A.pf
1270 C:\Windows\Prefetch\ZZUMGOZ.EXE-D7EDB409.pf
1271 C:\Windows\System32\sru\SRU00053.log
1272 C:\Windows\System32\kazaabackupfiles\AVP_Crack.exe
1273 C:\Windows\System32\kazaabackupfiles\DreamweaverMX_Crack.exe
1274 C:\Windows\System32\kazaabackupfiles\EDU_Hack.exe
1275 C:\Windows\System32\kazaabackupfiles\FlashFXP_Crack.exe
1276 C:\Windows\System32\kazaabackupfiles\Generals_No-CD_Crack.exe
1277 C:\Windows\System32\kazaabackupfiles\Norton Anti-Virus_2002_Crack.exe
1278 C:\Windows\System32\kazaabackupfiles\PlanetSide.exe
1279 C:\Windows\System32\kazaabackupfiles\Porn.exe
1280 C:\Windows\System32\kazaabackupfiles\Postal_2_Crack.exe
1281 C:\Windows\System32\kazaabackupfiles\Red_Faction_2_No-CD_Crack.exe
1282 C:\Windows\System32\kazaabackupfiles\Renegade_No-CD_Crack.exe
1283 C:\Windows\System32\kazaabackupfiles\Sitebot.exe
1284 C:\Windows\System32\kazaabackupfiles\Winamp_Installer.exe
1285 C:\Windows\System32\kazaabackupfiles\zoneallarm_pro_crack.exe
1286 C:\Windows\System32\keylog.txt
1287 C:\Windows\System32\wuaumgr.exe
1288 C:\Windows\System32\xugwmpk.exe
1289 C:\Windows\System32\zzumgoz.exe
1290
  
```



C:\Windows\System32\keylog.txt - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

res-x86.bt keylog.txt

```
1
2 [21:Mar:2019, 05:14:40] Keylogger Started
3
4 [05:14:57] Process Hacker [REMWS620\REM]+ (Administrator)           First run (Changed window)
5
6 [21:Mar:2019, 05:15:07] Keylogger Started
7
8 [05:15:43] Process Hacker [REMWS620\REM]+ (Administrator)           Second run. Note filename has changed to zzumgoz.exe (Changed window)
9
10 [21:Mar:2019, 05:15:50] Keylogger Started
11
12 [05:16:09] Process Hacker [REMWS620\REM]+ (Administrator)           Third time> new filename again (Changed window)
13
```

# Process Monitor

Follow my demo

# Process Monitor suggested approach

- Clean img (unpack malware)
- Open Process Hacker
- Open Process Monitor, pause and clear
- Start Process monitor
- Run spybot.exe as administrator
- wuamqr.exe should start up (check Process Hacker)
- After "some time" stop Process Monitor first (avoid some noise)
- terminate wuamqr.exe
  
- Variations:
  - Include Keyboard activity (look at keylog.txt)
  - Start twice, look at name

# Making sense of ProcMon

- Suggested filters:
- Process Name is
  - wuamqr.exe
  - spybot.exe
- Operation is
  - WriteFile, (Create File)
    - Same as regedit
  - RegCreateKey, RegSetValue
    - Some activity
  - Process create, Process start, Process exit
    - Spybot starts from desktop, creates wuamqr.exe cmd line and starts it, then exits itself
  - Thread Creat, Thread exit
    - Spybot starts and exits 7 threads
    - Wuamqr starts 4 treads

# WriteFile

Process Monitor - C:\Program Files\Process Monitor\procmon\_event\_data.p...

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail	TID
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\wuauqmqr.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\zoneallarm_pro_crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\AVP_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Porn.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Norton_Anti-Virus_2002_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Generals_No-CD_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Renegade_No-CD_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Red_Faction_2_No-CD_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Postal_2_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\FlashFXP_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\DreamweaverMX_Crack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\PlanetSide.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Winamp_Installer.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\Sitebot.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\kazaabackupfiles\EDU_Hack.exe	SUCCESS	Offset 0, Length: 44...	1904
6:05:30...	spybot.exe	952	WriteFile	C:\Windows\System32\wuauqmqr.exe	SUCCESS	Offset 0, Length: 45...	1904
6:05:30...	wuauqmqr.exe	1752	WriteFile	C:\Windows\System32\keylog.txt	SUCCESS	Offset 0, Length: 48...	3612

Process Monitor Filter

Display entries matching these conditions:

Operation is CreateFile then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process N...	is	spybot.exe	Include
<input checked="" type="checkbox"/> Process N...	is	wuauqmqr.exe	Include
<input checked="" type="checkbox"/> Operation	is	WriteFile	Include
<input type="checkbox"/> Operation	is	CreateFile	Include
<input checked="" type="checkbox"/> Process N...	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	System	Exclude
<input checked="" type="checkbox"/> Operation	begins with	IRP_MJ_	Exclude

OK Cancel Apply

# Registry

Process Monitor - C:\Program Files\Process Monitor\procmon\_event\_data.pml

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail	TID
6:05:30...	spybot.exe	952	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	SUCCESS	Desired Access: Al...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Winsock driver	SUCCESS	Type: REG_SZ, Le...	1904
6:05:30...	spybot.exe	952	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Al...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Winsock driver	SUCCESS	Type: REG_SZ, Le...	1904
6:05:30...	spybot.exe	952	RegCreateKey	HKCU\SOFTWARE\KAZAA\LocalContent	NAME NOT FOUND	Desired Access: M...	1904
6:05:30...	spybot.exe	952	RegCreateKey	HKCU\SOFTWARE	SUCCESS	Desired Access: M...	1904
6:05:30...	spybot.exe	952	RegCreateKey	HKCU\Software\KAZAA	SUCCESS	Desired Access: M...	1904
6:05:30...	spybot.exe	952	RegCreateKey	HKCU\Software\KAZAA\LocalContent	SUCCESS	Desired Access: M...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\KAZAA\LocalContent\Dir0	SUCCESS	Type: REG_SZ, Le...	1904
6:05:30...	spybot.exe	952	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: R...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWO...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWO...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWO...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWO...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWO...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWO...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWO...	1904
6:05:30...	spybot.exe	952	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWO...	1904
6:05:30...	wuauqr.exe	1752	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	SUCCESS	Desired Access: Al...	3896
6:05:30...	wuauqr.exe	1752	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Al...	3896

Process Monitor Filter

Display entries matching these conditions:

Operation is RegSetValue then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/>	Process N...	spybot.exe	Include
<input checked="" type="checkbox"/>	Process N...	wuauqr.exe	Include
<input type="checkbox"/>	Operation	WriteFile	Include
<input type="checkbox"/>	Operation	CreateFile	Include
<input checked="" type="checkbox"/>	Operation	RegCreateKey	Include
<input checked="" type="checkbox"/>	Operation	RegSetValue	Include
<input checked="" type="checkbox"/>	Process N...	Procmon.exe	Exclude

OK Cancel Apply

# Process



Process Monitor - C:\Program Files\Process Monitor\procmon\_event\_data.pml

File Edit Event Filter Tools Options Help



Time o...	Process Name	PID	Operation	Path	Result	Detail	TID
6:05:30...	spybot.exe	952	Process Start		SUCCESS	Parent PID: 3068, Command line: "C:\Users\REM\Desktop\spybot.exe", Current direc...	1488
6:05:30...	spybot.exe	952	Process Create	C:\Windows\system32\wuauqm.exe	SUCCESS	PID: 1752, Command line: "C:\Windows\system32\wuauqm.exe"	1904
6:05:30...	wuauqm.exe	1752	Process Start		SUCCESS	Parent PID: 952, Command line: "C:\Windows\system32\wuauqm.exe", Current direct...	1904
6:05:30...	spybot.exe	952	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0312500 seconds, Kernel Time: 0.0937500 seconds, Privat...	3348

Process Monitor Filter

Display entries matching these conditions:

Operation is Process Exit then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process N...	is	spybot.exe	Include
<input checked="" type="checkbox"/> Process N...	is	wuauqm.exe	Include
<input type="checkbox"/> Operation	is	WriteFile	Include
<input type="checkbox"/> Operation	is	CreateFile	Include
<input type="checkbox"/> Operation	is	RegCreateKey	Include
<input type="checkbox"/> Operation	is	RegSetValue	Include
<input checked="" type="checkbox"/> Operation	is	Process Create	Include
<input checked="" type="checkbox"/> Operation	is	Process Start	Include
<input checked="" type="checkbox"/> Operation	is	Process Exit	Include
<input checked="" type="checkbox"/> Process N...	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	System	Exclude
<input checked="" type="checkbox"/> Operation	begins with	IRP_MJ_	Exclude

OK Cancel Apply

# Threads

Process Monitor - C:\Program Files\Process Monitor\procmon\_event\_data.pml

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail	TID
6:05:30...	spybot.exe	952	Thread Create		SUCCESS	Thread ID: 1904	1488
6:05:30...	spybot.exe	952	Thread Create		SUCCESS	Thread ID: 3348	36
6:05:30...	spybot.exe	952	Thread Create		SUCCESS	Thread ID: 3412	3348
6:05:30...	spybot.exe	952	Thread Create		SUCCESS	Thread ID: 868	1904
6:05:30...	spybot.exe	952	Thread Create		SUCCESS	Thread ID: 4036	1904
6:05:30...	spybot.exe	952	Thread Create		SUCCESS	Thread ID: 2600	1904
6:05:30...	spybot.exe	952	Thread Create		SUCCESS	Thread ID: 1328	36
6:05:30...	wuauqmgr.exe	1752	Thread Create		SUCCESS	Thread ID: 3244	1904
6:05:30...	spybot.exe	952	Thread Exit		SUCCESS	Thread ID: 1904, User Time: 0.0312500, Kernel Time: 0.0937500	1904
6:05:30...	spybot.exe	952	Thread Exit		SUCCESS	Thread ID: 4036, User Time: 0.0000000, Kernel Time: 0.0000000	4036
6:05:30...	wuauqmgr.exe	1752	Thread Create		SUCCESS	Thread ID: 1896	3244
6:05:30...	wuauqmgr.exe	1752	Thread Create		SUCCESS	Thread ID: 3896	3244
6:05:30...	wuauqmgr.exe	1752	Thread Create		SUCCESS	Thread ID: 3612	3244
6:05:30...	spybot.exe	952	Thread Exit		SUCCESS	Thread ID: 1328, User Time: 0.0000000, Kernel Time: 0.0000000	1328
6:05:30...	spybot.exe	952	Thread Exit		SUCCESS	Thread ID: 2600, User Time: 0.0000000, Kernel Time: 0.0000000	2600
6:05:30...	spybot.exe	952	Thread Exit		SUCCESS	Thread ID: 868, User Time: 0.0000000, Kernel Time: 0.0000000	868
6:05:30...	spybot.exe	952	Thread Exit		SUCCESS	Thread ID: 3412, User Time: 0.0000000, Kernel Time: 0.0000000	3412
6:05:30...	spybot.exe	952	Thread Exit		SUCCESS	Thread ID: 3348, User Time: 0.0000000, Kernel Time: 0.0000000	3348

Process Monitor Filter

Display entries matching these conditions:

Operation is Thread Exit then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/>	Process N...	spybot.exe	Include
<input checked="" type="checkbox"/>	Process N...	wuauqmgr.exe	Include
<input type="checkbox"/>	Operation	WriteFile	Include
<input type="checkbox"/>	Operation	CreateFile	Include
<input type="checkbox"/>	Operation	RegCreateKey	Include
<input type="checkbox"/>	Operation	RegSetValue	Include
<input type="checkbox"/>	Operation	Process Create	Include
<input type="checkbox"/>	Operation	Process Start	Include
<input type="checkbox"/>	Operation	Process Exit	Include
<input checked="" type="checkbox"/>	Operation	Thread Create	Include
<input checked="" type="checkbox"/>	Operation	Thread Exit	Include
<input checked="" type="checkbox"/>	Process N...	Procmon.exe	Exclude

OK Cancel Apply



# Write while Keylogger is active

Process Monitor - C:\Program Files\Process Monitor\procmo

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail	TID
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\wuauqr.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\zoneallarm_pro_cr...	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\AVP_Crack.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Porn.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Norton_Anti-Virus_2...	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Generals_No-CD...	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Renegade_No-CD...	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Red_Faction_2_No...	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Postal_2_Crack.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\FlashFXP_Crack.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\DreamweaverMX...	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\PlanetSide.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Winamp_Installer.e...	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\Sitebot.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\kazaabackupfiles\EMU_Hack.exe	SUCCESS	Offset 0, Length: 44...	3424
6:24:14...	spybot.exe	3612	WriteFile	C:\Windows\System32\wuauqr.exe	SUCCESS	Offset 0, Length: 45...	3424
6:24:14...	wuauqr.exe	416	WriteFile	C:\Windows\System32\keylog.bt	SUCCESS	Offset 0, Length: 48...	2336
6:24:26...	wuauqr.exe	416	WriteFile	C:\Windows\System32\keylog.bt	SUCCESS	Offset: 48, Length: 1...	2336
6:24:35...	wuauqr.exe	416	WriteFile	C:\Windows\System32\keylog.bt	SUCCESS	Offset: 151, Length: ...	2336

Process Monitor Filter

Display entries matching these conditions:

Operation is WriteFile then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process N...	is	spybot.exe	Include
<input checked="" type="checkbox"/> Process N...	is	wuauqr.exe	Include
<input checked="" type="checkbox"/> Operation	is	WriteFile	Include
<input checked="" type="checkbox"/> Process N...	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	System	Exclude
<input checked="" type="checkbox"/> Operation	begins with	IRP_MJ_	Exclude
<input checked="" type="checkbox"/> Operation	begins with	FASTIO_	Exclude

OK Cancel Apply

# Wireshark

Follow my demo

# Wireshark suggested approach

- Open remnux,
  - cd /etc/inetsim/
  - sudo leafpad inetsim.conf (setup)
  - Ping
  - sudo inetsim (start)
  - wireshark (start) and start capture
- On win7:
  - Clean img
  - Open cmd: ping remnux
  - Start Process Hacker
  - Run spybot.exe as administrator
  - wuaumqr.exe should start up (check Process Hacker)
  - After "some time" (> 60s) terminate wuaumqr.exe
- On remnux
  - Analyse wireshark pcap

# result

- TCP SYN to 209.126.201.20 port 6667
  - Retransmit twice
- TCP SYN to 209.126.201.22 port 6666
  - Retransmit twice
  - Repeat
- Guess: IRC
- Future work: Simulate the other end, test the protocol

2	0.966804	192.168.81.130	192.168.81.129	DNS	83	Standard query 0xf0b1	A	win8.ipv6.microsoft.com
4	0.967644	192.168.81.130	192.168.81.129	DNS	83	Standard query 0xf0b1	A	win8.ipv6.microsoft.com
6	0.968152	192.168.81.130	192.168.81.129	DNS	83	Standard query 0xf0b1	A	win8.ipv6.microsoft.com
8	0.968671	192.168.81.130	192.168.81.129	DNS	83	Standard query 0xf0b1	A	win8.ipv6.microsoft.com
10	0.969098	192.168.81.130	192.168.81.129	DNS	83	Standard query 0xf0b1	A	win8.ipv6.microsoft.com
12	4.167960	192.168.81.130	209.126.201.20	TCP	66	49164 > 6667 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
16	7.169261	192.168.81.130	209.126.201.20	TCP	66	[TCP Retransmission] 49164 > 6667 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
18	13.16970	192.168.81.130	209.126.201.20	TCP	62	[TCP Retransmission] 49164 > 6667 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1		
30	30.18573	192.168.81.130	209.126.201.22	TCP	66	49165 > 6666 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
32	33.18453	192.168.81.130	209.126.201.22	TCP	66	[TCP Retransmission] 49165 > 6666 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
34	39.20056	192.168.81.130	209.126.201.22	TCP	62	[TCP Retransmission] 49165 > 6666 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1		
36	43.83442	192.168.81.130	192.168.81.129	DNS	83	Standard query 0x826b	A	win8.ipv6.microsoft.com
38	43.83493	192.168.81.130	192.168.81.129	DNS	83	Standard query 0x826b	A	win8.ipv6.microsoft.com
40	43.83517	192.168.81.130	192.168.81.129	DNS	83	Standard query 0x826b	A	win8.ipv6.microsoft.com
42	43.83536	192.168.81.130	192.168.81.129	DNS	83	Standard query 0x826b	A	win8.ipv6.microsoft.com
44	43.83553	192.168.81.130	192.168.81.129	DNS	83	Standard query 0x826b	A	win8.ipv6.microsoft.com
58	56.21640	192.168.81.130	209.126.201.20	TCP	66	49166 > 6667 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
59	59.21591	192.168.81.130	209.126.201.20	TCP	66	[TCP Retransmission] 49166 > 6667 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
62	65.21639	192.168.81.130	209.126.201.20	TCP	62	[TCP Retransmission] 49166 > 6667 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1		

# Summary

- Registry
  - Activity, keys and values added and changed
  - Closer look, we could probably learn more
- Files
  - Files created and accessed
  - Wuaumqr.exe, keylog.txt, 14 .exe
- Processes and Threads
  - Created and started
- Network
  - IRC channel? Two IP adr