

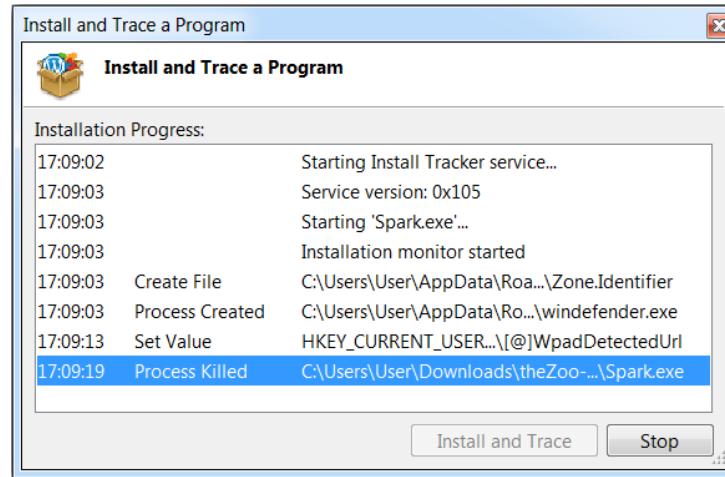
## Lab № 1

### Dynamic malware analysis

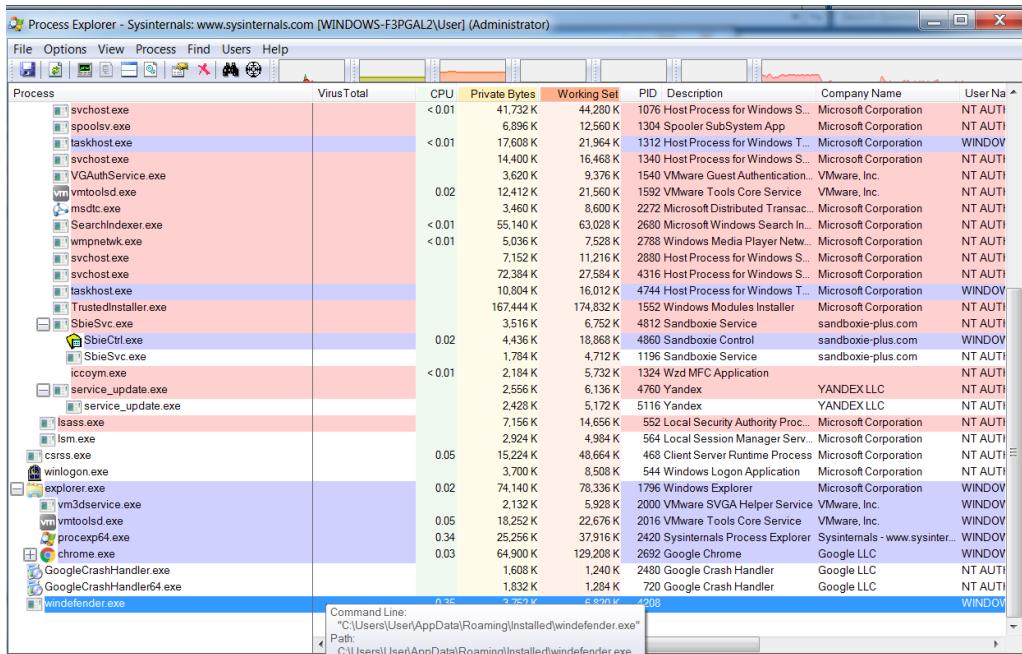
Sample 1: Alina Spark – PoS(point of sale)

Hash(SHA-1): 553d1afa824c34f348f8c53d1b043d3b671d946a

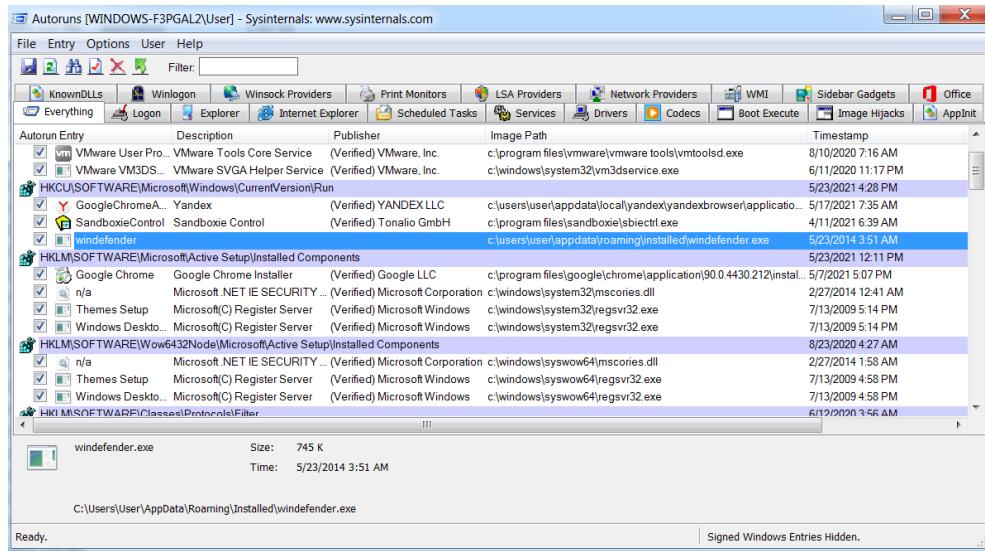
Running malware sample using Install&Trace shows steps completed by file during installation:



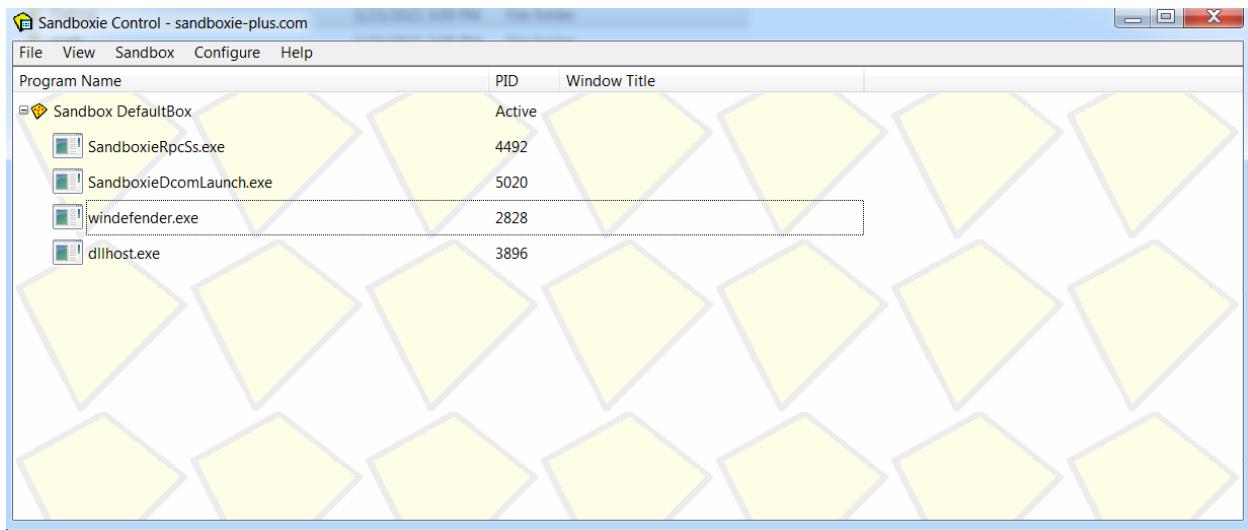
In "Process Explorer" window, we see file dropped running under the name "windefender.exe":



Dropped file also added to the *startup*:



Running into *sandboxie*:



## Sample 2: Nullsoft self-extracting archive

Hash(SHA-1): 7a60598b33ca31627ab3767c6359ce81f8938785

**Install and Trace a Program**

Installation Progress:

```

12:39:35 Starting Install Tracker service...
12:39:36 Service version: 0x105
12:39:36 Starting '065f50e43b6331130a7b0ac8de24f6e1df0fb00d5c101666f32f6d54e6bd9d83.exe'...
12:39:36 Installation monitor started
12:39:36 Create File C:\Users\user\AppData\Local\Temp\ns629.tmp
12:39:36 Create File C:\Users\user\AppData\Local\Temp\ns62A.tmp
12:39:36 Create Folder C:\Users\user\AppData\Local\Temp\ns62B.tmp
12:39:36 Create Folder C:\Users\user\AppData\Local\Temp\ns62B.tmp
12:39:36 Create File C:\Users\user\AppData\Local\Temp\8ySpitej62weui3
12:39:36 Create File C:\Users\user\AppData\Local\Temp\o9xc87gn7u
12:39:36 Create File C:\Users\user\AppData\Local\Temp\rcyqfd
12:39:36 Create File C:\Users\user\AppData\Local\Temp\ns62B.tmp\System.dll
12:39:37 Create Folder C:\Users\user\AppData\Roaming\auto
12:39:37 Create File C:\Users\user\AppData\Roaming\auto\dmpr.exe
12:39:37 Set Value HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\[@]=own
12:39:37 Process Created C:\Users\user\Downloads\065f50e43b6331130a7b0ac8de24f6e1df0fb00d5c101666f32f6d54e6bd9d83.exe
12:39:37 Process Killed C:\Users\user\Downloads\065f50e43b6331130a7b0ac8de24f6e1df0fb00d5c101666f32f6d54e6bd9d83.exe
12:39:37 Create Folder C:\Users\user\AppData\Roaming\84EA9F6-7868-49F8-8972-4A3A5D1326D2
12:39:37 Create File C:\Users\user\AppData\Roaming\84EA9F6-7868-49F8-8972-4A3A5D1326D2\run.dat
12:39:37 Create Folder C:\Users\user\AppData\Roaming\84EA9F6-7868-49F8-8972-4A3A5D1326D2\Logs
12:39:37 Create Folder C:\Users\user\AppData\Roaming\84EA9F6-7868-49F8-8972-4A3A5D1326D2\Logs\User

```

Install and Trace | Stop

**Autoruns [WINDOWS-F3PGAL2\user] - Sysinternals: www.sysinternals.com**

Auton Entry	Description	Publisher	Image Path	Timestamp
<input checked="" type="checkbox"/> CurrentControlSet\Control\SafeBoot\AllowUnsafeShell				7/13/2009 9:49 PM
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor (Verified) Microsoft Windows	c:\windows\system32\cmd.exe		3/25/2016 10:49 AM
<input checked="" type="checkbox"/> HKEY SOFTWARE\Microsoft\Windows\CurrentVersion\Run				5/24/2021 9:46 AM
<input checked="" type="checkbox"/> VMware User Pro - VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe		4/16/2021 10:34 AM
<input checked="" type="checkbox"/> HKCU\Software\Microsoft\Windows\CurrentVersion\Run				5/24/2021 12:39 PM
<input checked="" type="checkbox"/> Java	Tonalo GmbH	c:\users\user\appdata\local\java\jdk\dmpr.exe		12/5/2009 3:10 PM
<input checked="" type="checkbox"/> SandboxControl	Sandbox Control (Verified) Tonalo GmbH	c:\program files\sandbox\abieict.exe		4/11/2021 6:30 AM
<input checked="" type="checkbox"/> HKEY SOFTWARE\Microsoft\Active Setup\Installed Components				5/23/2021 12:11 PM
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer (Verified) Google LLC	c:\program files\google\chrome\application\90.0.4430.212\install_		5/7/2021 5:07 PM
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY (Verified) Microsoft Corporation	c:\windows\system32\msncons.dll		2/27/2014 12:41 AM
<input checked="" type="checkbox"/> Themes Setup	Microsoft(C) Register Server (Verified) Microsoft Windows	c:\windows\system32\ye\gsvr32.exe		7/13/2009 5:14 PM
<input checked="" type="checkbox"/> Windows Desktop	Microsoft(C) Register Server (Verified) Microsoft Windows	c:\windows\system32\ye\gsvr32.exe		7/13/2009 5:14 PM
<input checked="" type="checkbox"/> HKEY SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				5/24/2021 9:43 AM
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY (Verified) Microsoft Corporation	c:\windows\syswow64\msncons.dll		2/27/2014 1:50 AM
<input checked="" type="checkbox"/> Themes Setup	Microsoft(C) Register Server (Verified) Microsoft Windows	c:\windows\syswow64\regsvr32.exe		7/13/2009 4:58 PM
<input checked="" type="checkbox"/> Windows Desktop	Microsoft(C) Register Server (Verified) Microsoft Windows	c:\windows\syswow64\regsvr32.exe		7/13/2009 4:58 PM

dmpr.exe Size: 660 K Time: 12/5/2009 3:50 PM

C:\Users\user\AppData\Roaming\auto\dmpr.exe

Ready. Signed Windows Entries Hidden.

**Process Explorer - Sysinternals: www.sysinternals.com [WINDOWS-F3PGAL2\user] (Administrator)**

Process	VirusTotal	CPU	Private Bytes	Working Set	PID	Description	Company Name	User No.
taskhost.exe	< 0.01	15.63 K	15-651 K	708	Host Process for Windows T...	Microsoft Corporation	WINDOV	
svchost.exe	2.37 K	6.190 K	3252	Host Process for Windows S...	Microsoft Corporation	NT AUTO		
taskhost.exe	4.312 K	6.856 K	2494	Host Process for Windows T...	Microsoft Corporation	WINDOV		
maxexec.exe	2.836 K	7.124 K	2424	WindInstall	Microsoft Corporation	NT AUTO		
lsass.exe	1.568 K	3.924 K	2116	Host Process for Windows S...	Microsoft Corporation	NT AUTO		
lsass.exe	5.800 K	13.620 K	512	Local Security Authority Proc...	Microsoft Corporation	NT AUTO		
lsm.exe	2.996 K	5.040 K	520	Local Session Manager Serv...	Microsoft Corporation	NT AUTO		
GoogleCrashHandler.exe	1.620 K	1.204 K	1652	Google Crash Handler	Google LLC	NT AUTO		
GoogleCrashHandler64.exe	1.832 K	1.290 K	3052	Google Crash Handler	Google LLC	NT AUTO		
crss.exe	0.01	10.360 K	14.294 K	2520	Client Server Runtime Process	Microsoft Corporation	NT AUTO	
wlonlogon.exe	0.01	3.832 K	8.560 K	3976	Windows Logon Application	Microsoft Corporation	NT AUTO	
explorer.exe	0.01	70.172 K	119.960 K	996	Windows Explorer	Microsoft Corporation	WINDOV	
win32kfull.exe	0.03	20.812 K	31.354 K	2140	Windows Driver Core Service	VMware, Inc.	WINDOV	
process.exe	0.01	4.284 K	16.334 K	3772	Sandbox Control	sandbox-plus.com	WINDOV	
process64.exe	0.25	4.708 K	3.644 K	1804	Systematics Process Explorer	Syntimelabs - www.syntimel...	WINDOV	
chrome.exe	0.01	68.505 K	140.500 K	744	Google Chrome	Google LLC	WINDOV	
chrome.exe	3.384 K	6.560 K	5094	Google Chrome	Google LLC	WINDOV		
chrome.exe	199.776 K	224.020 K	4412	Google Chrome	Google LLC	WINDOV		
chrome.exe	15.032 K	33.750 K	2416	Google Chrome	Google LLC	WINDOV		
chrome.exe	8.568 K	15.840 K	460	Google Chrome	Google LLC	WINDOV		
chrome.exe	90.432 K	180.380 K	4436	Google Chrome	Google LLC	WINDOV		
chrome.exe	11.808 K	16.320 K	4508	Google Chrome	Google LLC	WINDOV		
chrome.exe	30.100 K	55.264 K	4120	Google Chrome	Google LLC	WINDOV		
chrome.exe	24.668 K	41.380 K	3556	Google Chrome	Google LLC	WINDOV		
chrome.exe	39.740 K	77.576 K	1952	Google Chrome	Google LLC	WINDOV		
chrome.exe	20.532 K	22.620 K	4388	Google Chrome	Google LLC	WINDOV		
chrome.exe	31.536 K	30.320 K	3095	Google Chrome	Google LLC	WINDOV		

CPU Usage: 0.99% Commit Charge: 24.23% Processes: 61