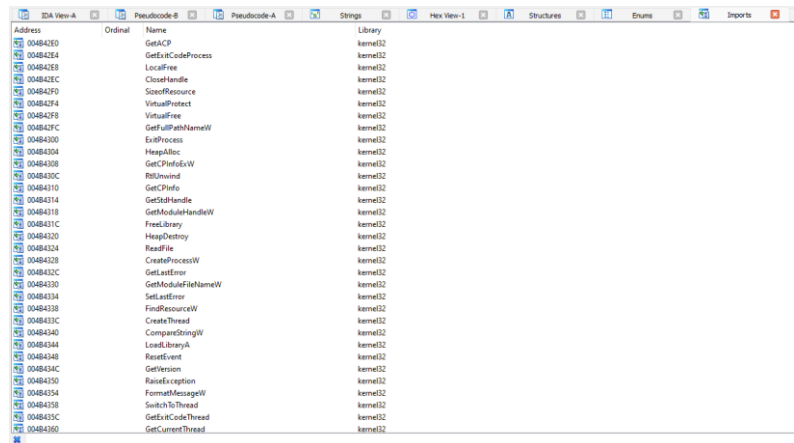


## Статический анализ

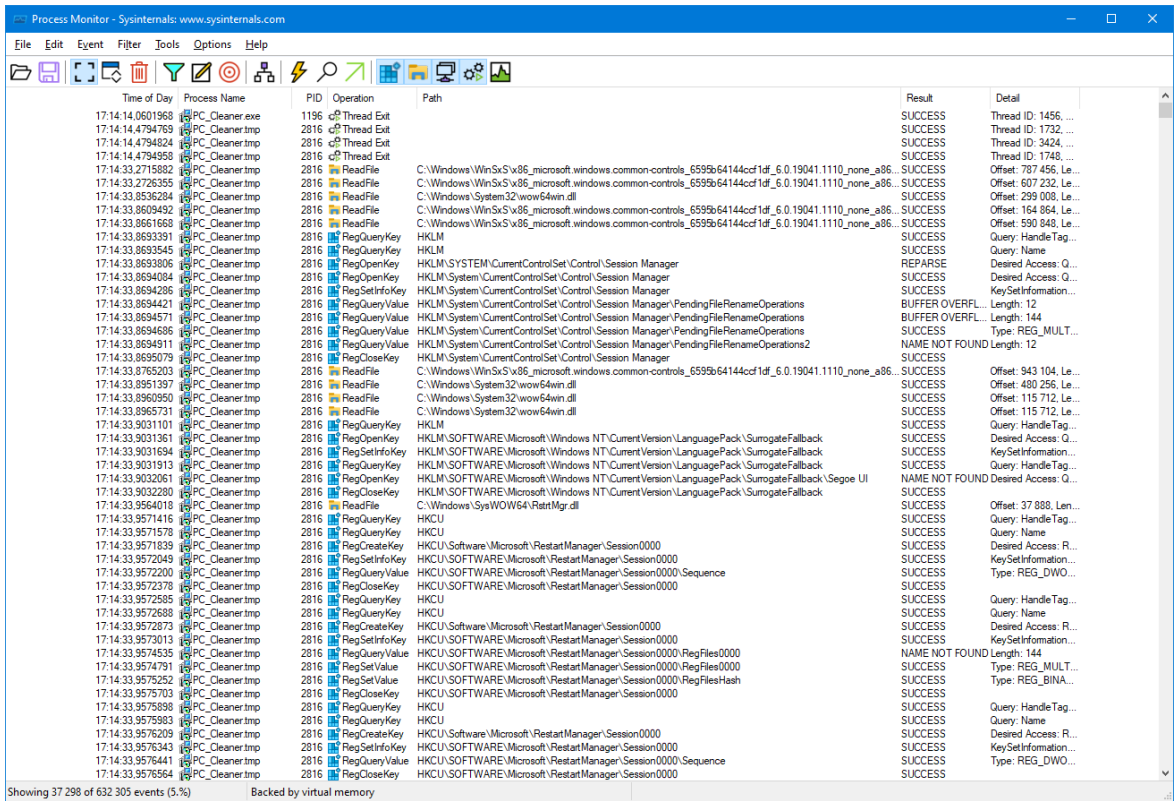
Задание представлено в виде файла «PC\_Cleaner.exe». Изначально, был проведен статический анализ файла в IDA Pro. Большой интерес представляла вкладка с импортами, чтоб определить ход динамического анализа. После осмотра дизассемблированный кода становится понятно, что файл является инсталлятором и использует библиотеку Inno Setup, в таблице импортов не было замечено функций для работы с сокетами, а также подозрительных структур.



Address	Ordinal	Name	Library
004B42E9		GetCP	kernel32
004B42E4		GetExitCodeProcess	kernel32
004B42E9		LocalFree	kernel32
004B42EC		CloseHandle	kernel32
004B42F0		SizeofResource	kernel32
004B42F4		VirtualProtect	kernel32
004B42F9		VirtualFree	kernel32
004B42FC		GetFullPathNameW	kernel32
004B4300		ExitProcess	kernel32
004B4304		HeapAlloc	kernel32
004B4308		GetPrivateW	kernel32
004B430C		PtrUnwind	kernel32
004B4310		GetPrivate	kernel32
004B4314		GetStdHandle	kernel32
004B4318		GetModuleHandleW	kernel32
004B431C		FreeLibrary	kernel32
004B4320		HeapDestroy	kernel32
004B4324		ReadFile	kernel32
004B4328		CreateProcessW	kernel32
004B432C		GetLastError	kernel32
004B4330		GetModuleFileNameW	kernel32
004B4334		SetLastError	kernel32
004B4338		FindResourceW	kernel32
004B433C		CreateThread	kernel32
004B4340		CompareStringW	kernel32
004B4344		LoadLibraryA	kernel32
004B4348		ResetEvent	kernel32
004B434C		GetVersion	kernel32
004B4350		RaiseException	kernel32
004B4354		FormatMessageW	kernel32
004B4358		SwitchToThread	kernel32
004B435C		GetExitCodeThread	kernel32
004B4360		GetCurrentThread	kernel32

## Динамический анализ

После первичного ознакомлением с инсталлятором можно попробовать проследить за его действиями. Для этой задачи использовалась виртуальная машина с Windows 10 и утилиты: regshot (для получения снимков реестра и сравнения ключей и значений после установки), autoruns (для получения отфильтрованной информации об автозапуске, службах, заданиях и т.д), procmon (для отслеживания действий программы), process hacker (проследить за деревом процессов, получить информацию о потоках и дескрипторах), wireshark (детектирование сетевого взаимодействия). Перед запуском процесса установки были сделаны снимки реестра и автозапуска, также запущен procmon, который выводил информацию только по процессам «PC\_Cleaner.exe», «PC\_Cleaner.tmp», «PCCleaner.exe» .



Time of Day	Process Name	PID	Operation	Path	Result	Detail
17:14:14.0601968	PC_Cleaner.exe	1196	Thread Exit		SUCCESS	Thread ID: 1456, ...
17:14:14.4794769	PC_Cleaner.tmp	2816	Thread Exit		SUCCESS	Thread ID: 1732, ...
17:14:14.4794824	PC_Cleaner.tmp	2816	Thread Exit		SUCCESS	Thread ID: 3424, ...
17:14:14.4794958	PC_Cleaner.tmp	2816	Thread Exit		SUCCESS	Thread ID: 1748, ...
17:14:33.2715882	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccd1df_6.0.19041.1110_none_a86...	SUCCESS	Offset: 787 455, Le...
17:14:33.2726355	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccd1df_6.0.19041.1110_none_a86...	SUCCESS	Offset: 607 232, Le...
17:14:33.8536284	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 299 008, Le...
17:14:33.8609492	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccd1df_6.0.19041.1110_none_a86...	SUCCESS	Offset: 164 864, Le...
17:14:33.8661668	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccd1df_6.0.19041.1110_none_a86...	SUCCESS	Offset: 590 848, Le...
17:14:33.8693391	PC_Cleaner.tmp	2816	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
17:14:33.8693445	PC_Cleaner.tmp	2816	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Query: Name
17:14:33.8693806	PC_Cleaner.tmp	2816	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
17:14:33.8694084	PC_Cleaner.tmp	2816	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
17:14:33.8694286	PC_Cleaner.tmp	2816	RegSetInfoKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
17:14:33.8694421	PC_Cleaner.tmp	2816	RegQueryValue	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations	BUFFER OVERFL...	Length: 12
17:14:33.8694571	PC_Cleaner.tmp	2816	RegQueryValue	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations	BUFFER OVERFL...	Length: 144
17:14:33.8694686	PC_Cleaner.tmp	2816	RegQueryValue	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations	SUCCESS	Type: REG_MULT...
17:14:33.8694911	PC_Cleaner.tmp	2816	RegQueryValue	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations2	NAME NOT FOUND	Length: 12
17:14:33.8695079	PC_Cleaner.tmp	2816	RegCloseKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	
17:14:33.8765203	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccd1df_6.0.19041.1110_none_a86...	SUCCESS	Offset: 943 104, Le...
17:14:33.8951397	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 480 256, Le...
17:14:33.8960950	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 115 712, Le...
17:14:33.8965731	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 115 712, Le...
17:14:33.9031101	PC_Cleaner.tmp	2816	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
17:14:33.9031361	PC_Cleaner.tmp	2816	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback	SUCCESS	Desired Access: Q...
17:14:33.9031694	PC_Cleaner.tmp	2816	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback	SUCCESS	KeySetInformation...
17:14:33.9031913	PC_Cleaner.tmp	2816	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback	SUCCESS	Query: HandleTag...
17:14:33.9032061	PC_Cleaner.tmp	2816	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\Segoe UI	NAME NOT FOUND	Desired Access: Q...
17:14:33.9032280	PC_Cleaner.tmp	2816	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback	SUCCESS	
17:14:33.9564018	PC_Cleaner.tmp	2816	ReadFile	C:\Windows\SysWow64\RateMgr.dll	SUCCESS	Offset: 37 888, Len...
17:14:33.9571416	PC_Cleaner.tmp	2816	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
17:14:33.9571578	PC_Cleaner.tmp	2816	RegOpenKey	HKCU	SUCCESS	Query: Name
17:14:33.9571839	PC_Cleaner.tmp	2816	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS	Desired Access: R...
17:14:33.9572049	PC_Cleaner.tmp	2816	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS	KeySetInformation...
17:14:33.9572200	PC_Cleaner.tmp	2816	RegQueryValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\Sequence	SUCCESS	NAME NOT FOUND Length: 144
17:14:33.9572378	PC_Cleaner.tmp	2816	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS	Type: REG_MULT...
17:14:33.9572585	PC_Cleaner.tmp	2816	RegOpenKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS	Type: REG_BINA...
17:14:33.9572688	PC_Cleaner.tmp	2816	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
17:14:33.9572773	PC_Cleaner.tmp	2816	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS	Query: Name
17:14:33.9573013	PC_Cleaner.tmp	2816	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS	Desired Access: R...
17:14:33.9574335	PC_Cleaner.tmp	2816	RegQueryValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0000	NAME NOT FOUND	Length: 144
17:14:33.9574791	PC_Cleaner.tmp	2816	RegSetValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0000	SUCCESS	Type: REG_MULT...
17:14:33.9575252	PC_Cleaner.tmp	2816	RegSetValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\RegFilesHash	SUCCESS	Type: REG_BINA...
17:14:33.9575703	PC_Cleaner.tmp	2816	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS	
17:14:33.9575988	PC_Cleaner.tmp	2816	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
17:14:33.9575983	PC_Cleaner.tmp	2816	RegOpenKey	HKCU	SUCCESS	Query: Name
17:14:33.9576209	PC_Cleaner.tmp	2816	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS	Desired Access: R...
17:14:33.9576343	PC_Cleaner.tmp	2816	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS	KeySetInformation...
17:14:33.9576441	PC_Cleaner.tmp	2816	RegQueryValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\Sequence	SUCCESS	Type: REG_DWOW...
17:14:33.9576564	PC_Cleaner.tmp	2816	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS	



pestudio 9.46 - Malware Initial Assessment - www.winitor.com - [c:\program files (x86)\pc cleaner\pccleaner.exe]

file settings about

c:\program files (x86)\pc cleaner\pccleaner.exe

library (46)	duplicate (0)	flag (6)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (2)	imports (797)	description
oleaut32.dll	-	-	-	0x00516258	0x00516D04	implicit	3	oleaut32 library
advapi32.dll	-	-	-	0x00516268	0x00516E04	implicit	3	Advanced Windows
user32.dll	-	-	-	0x00516278	0x00516E14	implicit	2	Multi-User Windows
kernel32.dll	-	-	-	0x00516284	0x00516E20	implicit	52	Windows NT BASE A
kernel32.dll	-	-	-	0x00516358	0x00516EF4	implicit	10	Windows NT BASE A
user32.dll	-	-	-	0x00516384	0x00516F20	implicit	203	Multi-User Windows
gdi32.dll	-	-	-	0x00516684	0x00517250	implicit	99	GDI Client Library
version.dll	-	-	-	0x00516844	0x005173E0	implicit	3	Version Checking an
kernel32.dll	-	-	-	0x00516854	0x005173F0	implicit	149	Windows NT BASE A
advapi32.dll	-	-	-	0x00516A4C	0x00517648	implicit	18	Advanced Windows
SHFolder.dll	-	x	-	0x00516AF8	0x00517694	implicit	1	Shell Folder Library
kernel32.dll	-	-	-	0x00516B00	0x0051769C	implicit	1	Windows NT BASE A
netapi32.dll	-	x	-	0x00516B08	0x005176A4	implicit	1	Network Win32 Libr
oleaut32.dll	-	-	-	0x00516B10	0x005176AC	implicit	13	oleaut32 library
oleaut32.dll	-	-	-	0x00516B48	0x005176E4	implicit	4	oleaut32 library
ole32.dll	-	-	-	0x00516B5C	0x005176F8	implicit	29	Microsoft OLE for Wi
comctl32.dll	-	-	-	0x00516BD4	0x00517770	implicit	32	Common Controls L
user32.dll	-	-	-	0x00516C58	0x005177F4	implicit	4	Multi-User Windows
msvcrt.dll	-	-	-	0x00516C6C	0x00517808	implicit	20	Windows NT CRT Lib
shell32.dll	-	-	-	0x00516CC0	0x0051785C	implicit	8	Windows Shell Libr
wininet.dll	-	x	-	0x00516CE4	0x00517880	implicit	1	Internet Extensions f
shell32.dll	-	-	-	0x00516CEC	0x00517888	implicit	8	Windows Shell Libr
comdlg32.dll	-	-	-	0x00516D10	0x005178AC	implicit	2	Common Dialogs Lit
crtdll.dll	-	-	-	0x00516D1C	0x005178B8	implicit	3	n/a
oleacc.dll	-	-	-	0x00516D2C	0x005178C8	implicit	2	Active Accessibility C
sqlite3.dll	-	-	-	0x00516D38	0x005178D4	implicit	27	n/a

sha256: D259BAC5CEE241CFA481078BEAFAC6636CA673F0F0005B0668479B7F56F732 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x004EC494 signature: n/a

pestudio 9.46 - Malware Initial Assessment - www.winitor.com - [c:\program files (x86)\pc cleaner\pccnotifications.exe]

file settings about

c:\program files (x86)\pc cleaner\pccnotifications.exe

library (39)	duplicate (0)	flag (5)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (2)	imports (616)	description
netapi32.dll	-	x	-	0x003259B4	0x0032631C	implicit	1	Network Win32 Libr
oleaut32.dll	-	-	-	0x003259BC	0x00326324	implicit	13	oleaut32 library
oleaut32.dll	-	-	-	0x003259F4	0x0032635C	implicit	3	oleaut32 library
ole32.dll	-	-	-	0x00325A04	0x0032636C	implicit	11	Microsoft OLE for Wi
comctl32.dll	-	-	-	0x00325A34	0x0032639C	implicit	29	Common Controls L
user32.dll	-	-	-	0x00325AAC	0x00326414	implicit	4	Multi-User Windows
msvcrt.dll	-	-	-	0x00325AC0	0x00326428	implicit	20	Windows NT CRT Lib
shell32.dll	-	-	-	0x00325B14	0x0032647C	implicit	3	Windows Shell Libr
wininet.dll	-	x	-	0x00325B24	0x0032648C	implicit	1	Internet Extensions f
shell32.dll	-	-	-	0x00325B2C	0x00326494	implicit	1	Windows Shell Libr
crtdll.dll	-	-	-	0x00325B34	0x0032649C	implicit	3	n/a
sqlite3.dll	-	-	-	0x00325B44	0x003264AC	implicit	2	n/a
winmm.dll	-	-	-	0x00325B58	0x003264C0	implicit	1	Windows Managem
kernel32.dll	-	-	-	0x00325B60	0x003264C8	implicit	3	Windows NT BASE A
kernel32.dll	-	-	-	0x00325928	0x0032921C	delay-load	1	Windows NT BASE A
user32.dll	-	-	-	0x00329330	0x00329220	delay-load	1	Multi-User Windows
wtapi32.dll	-	x	-	0x00329338	0x00329224	delay-load	2	Windows Remote De
user32.dll	-	-	-	0x00329344	0x0032922C	delay-load	4	Multi-User Windows
msimg32.dll	-	-	-	0x00329358	0x0032923C	delay-load	2	GDIEXT Client Library
kernel32.dll	-	-	-	0x00329364	0x00329244	delay-load	5	Windows NT BASE A
advapi32.dll	-	-	-	0x0032937C	0x00329258	delay-load	1	Advanced Windows
rpcrt4.dll	-	x	-	0x00329384	0x0032925C	delay-load	1	Remote Procedure C
windowscodecs.dll	-	-	-	0x0032938C	0x00329260	delay-load	1	Microsoft Windows C
uxtheme.dll	-	-	-	0x00329394	0x00329264	delay-load	10	Microsoft UxTheme I
imm32.dll	-	-	-	0x003293C0	0x0032928C	delay-load	7	Multi-User Windows
dwmapi.dll	-	x	-	0x003293E0	0x003292A8	delay-load	2	Microsoft Desktop W

sha256: 37B2F84AD0328C4C5838981E01E233F4E0499D4E67E8CB05CD50FF05AC94E4C9 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x002FE8E0 signature: n/a

Необходимо сделать новые снимки реестра и автозапуска для сравнения с исходным состоянием перед установкой. В автозагрузке лишь одно изменение – создана задача для запуска «PCCNotifications.exe» при входе любого зарегистрированного пользователя.

Autonom - SystemInfo www.systeminfo.com (Administrator) [D:\C:\TOP-N7K\9\04\rescue]

File Search Entry User Options Category Help

Everything Print Monitors LSA Providers Services Network Providers WMI Known DLLs WinLogon Winsock Providers

Autonom Entry Description Publisher Image Path Timestamp Virus Total

Services	Scheduled Tasks
PC Cleaner automatic scan and notifications	PC Cleaner automatic scan and notifi...

PC Cleaner automatic scan and notifi... 4 629 K

PC Cleaner automatic scan and notifi... Time: Mon Apr 20 14:48:06 2020

(Verified) PC HelpSoft Labs Inc. Version: 7.1.8.6

C:\Program Files (x86)\PC Cleaner\PCNotifications.exe

Ready

В результате сравнения снимков реестра ничего подозрительного, кроме создания задачи замечено не было.

```
kompass.regedit - Runasnet
@id: Дашаа Фопггв Ваа Стрвва
Regshot 1.9.0 x64 Unicode
Comments:
Dateline: 2022/11/9 10:41:28 , 2022/11/9 10:46:18
Computer: DESKTOP-HTKJV0H , DESKTOP-HTKJV0H
Username: rescue , rescue

-----
Keys deleted: 5
-----
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\8e9d21d7-32e5-47fc-8189-e964892b3c85
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\8e9d21d7-32e5-47fc-8189-e964892b3c85
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000000EA

-----
Keys added: 17
-----
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\logon\{78180740-DF12-4309-826D-078CAEF790DE}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{78180740-DF12-4309-826D-078CAEF790DE}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\PC Cleaner automatic scan and notifications
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PC Cleaner_is1
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000000578
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Microsoft\RestartManager
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Classes\PCHS
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Classes\PCHS\shell
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Classes\PCHS\shell\open
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Classes\PCHS\shell\open\command
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Licenses
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Licenses\d245d16c219a0913f2cb2177b11da31a
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\PC Cleaner
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\Classes\PCHS
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\Classes\PCHS\shell
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\Classes\PCHS\shell\open
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\Classes\PCHS\shell\open\command

-----
Values deleted: 2
-----
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\Perf\PMF\Name: "Global\PMF_BITS58bf19db-67db-4152-b584-bca4ead7a7bf"
HKU\S-1-5-21-1098110791-1873385835-1420079644-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000000EA\VirtualDesktop: 10 00 00 00 30 30 44 56 F4 08 52 08 98 AB 85 44 A7 C2 4D 28 60 66 D7 48

-----
Values added: 161
-----
```

Включив проверку обновлений и Wireshark, в работе двух программ «PCCleaner.exe» сетевой активности, подобной той, что была во время установки не было замечено.

**Вывод**

С помощью статического и динамического анализа подозрительное поведение не выявлено, кроме того, что программа сама по себе является твикером-сканером системы и собирает телеметрию. Следовательно, ПО является легитимным, но нежелательным к установке, потому что непосредственно влияет на работу других программ и/или системы.