ID: 831158
Sample Name: PC-SOFT_Set-Up.exe
Cookbook: default.jbs
Time: 07:06:12
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report PC-SOFT_Set-Up.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 3
AV Detection 3
System Summary 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Antivirus, Machine Learning and Genetic Malware Detection 4
Initial Sample 4
Dropped Files 4
Unpacked PE Files 5
Domains 5
URLs 5
Domains and IPs 5
Contacted Domains 5
World Map of Contacted IPs 5
General Information 5
Errors 5
Simulations 6
Behavior and APIs 6
Joe Sandbox View / Context 6
IPs 6
Domains 6
ASNs 6
JA3 Fingerprints 6
Dropped Files 6
Created / dropped Files 6
Static File Info 6
General 6
File Icon 6
Static PE Info 7
General 7
Entrypoint Preview 7
Data Directories 8
Sections 8
Resources 9
Imports 9
Possible Origin 10
Network Behavior 10
Statistics 10
System Behavior 10
Disassembly 10

Windows Analysis Report

PC-SOFT_Set-Up.exe

Overview

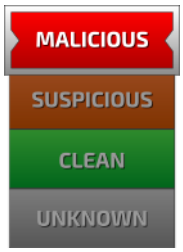
General Information

Sample Name:	PC-SOFT_Set-Up.exe
Analysis ID:	831158
MD5:	f448d2bbece9f…
SHA1:	acab3e78eb72…
SHA256:	bf83c57f5b1ae…
Tags:	exe, expert-topcom, malware, pass-1212, stealer

Errors

- No process behavior to analyse as no analysis process or sample was found
- Corrupt sample or wrongly selected analyzer. Details: C000007B

Detection

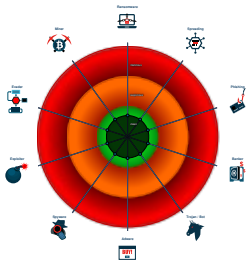


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Machine Learning detection for sam…
- PE file contains section with specia…
- PE file overlay found
- Uses 32bit PE files
- Entry point lies outside standard sec…
- PE file contains sections with non-s…

Classification



Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Machine Learning detection for sample

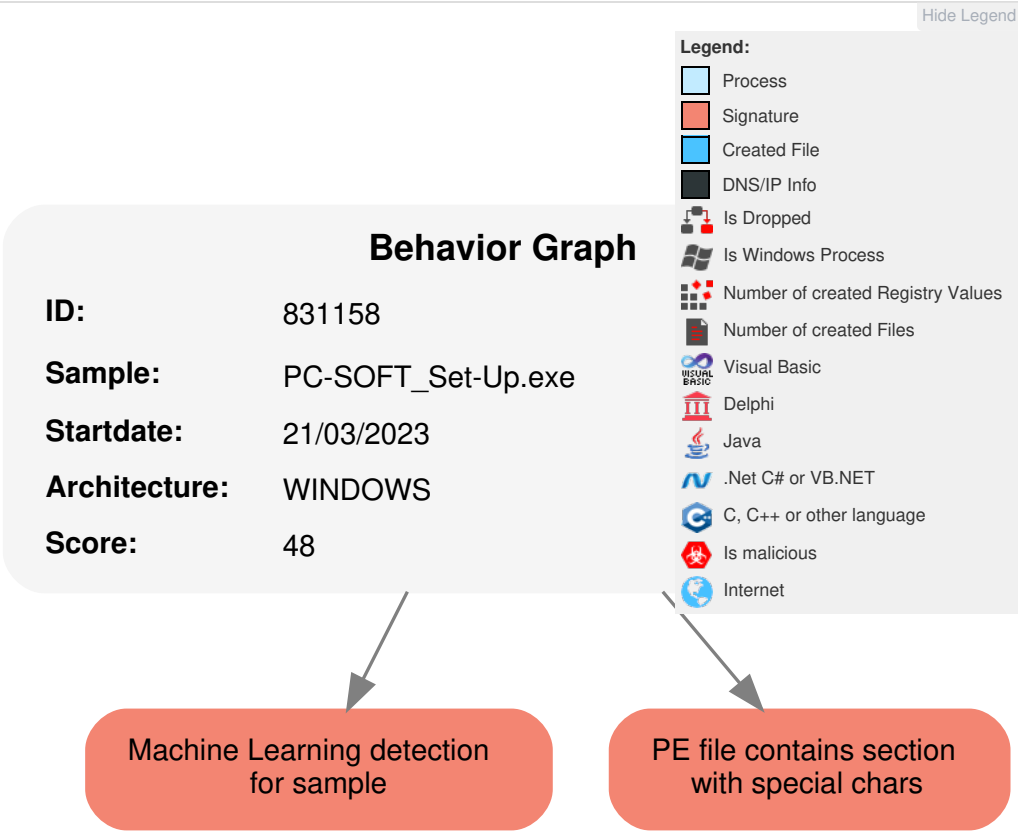
System Summary

PE file contains section with special chars

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PC-SOFT_Set-Up.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831158
Start date and time:	2023-03-21 07:06:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	0
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	PC-SOFT_Set-Up.exe
Detection:	MAL
Classification:	mal48.winEXE@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .exe • Unable to launch sample, stop analysis

Errors

- No process behavior to analyse as no analysis process or sam ple was found
- Corrupt sample or wrongly sele cted analyzer. Details: C000007B

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.962363679493409
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PC-SOFT_Set-Up.exe
File size:	10371193
MD5:	f448d2bbece9ffca6d35b72ad699c545
SHA1:	acab3e78eb72b8cde7f686a7adce243e819fa5ed
SHA256:	bf83c57f5b1ae62b3a671d93d263d9704c4e5dc82a4b381b216afd7b1d4764aa
SHA512:	08a5c4adc2ec0112547f1f7705e1bcf29d40700e8f16bfaa752ad542ce0fa956e761e8bacc31343d92d26dea0d244acf2d5f7811faee3d181c9984ccd316689e
SSDEEP:	196608:BhzWfNRbFvKkdDlGBpcb5jlxprm3dbeNYieb6ifmhDEZmnr/KVx2B9to:BkhqBpcNcPr6beSOr/mxoHo
TLSH:	15A63333A39D00C0C5D48D3A8937BEE9B8F61F775B06B97AF9A67AC10132594B311987
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....t.....t.....t.....|j.....|j.....|j.....Rich.....PE..L.....d.....

File Icon

Icon Hash:	fe7be6c293b3d2e6

Static PE Info

General

Entrypoint:	0x14101a0
Entrypoint Section:	.tve
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x640C95D2 [Sat Mar 11 14:53:06 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e9fa0dc321486a0834a2759b64589900

Entrypoint Preview

Instruction
push ebx
pushfd
mov ebx, 072D1758h
not bl
neg bx
test bl, 00000002h
push ebx
setle bl
and dword ptr [esp+ebx*2-0E5BD002h], 00361B9Eh
mov ebx, dword ptr [esp+ebx*2-0E5BCFFAh]
mov dword ptr [esp+08h], 5BC79C22h
push dword ptr [esp+04h]
popfd
lea esp, dword ptr [esp+08h]
call 00007FD560239FAEh
jmp 00007FD560A994F9h
jmp edi
mov bh, 08h
neg dword ptr [esi+1DA0DFBCh]
iretd
mov esp, 30D65AB3h
fidivr word ptr [eax-66CCCC7Bh]
das
add al, E9h
xor byte ptr [ebx+18h], dh
movsd
dec ebx
retf
pop ebx
jnp 00007FD560ACA85Ch
xor byte ptr [ebp+34B5FBE1h], dh
xor al, 29h

Instruction
push edx
fmul st(0), st(7)
push ss
pop es
adc edi, ecx
or eax, dword ptr [ebp+47CF6779h]
xlatb
sbb eax, C0CBCC30h
xor eax, 5345C865h
or eax, 98ED306Bh
insd
movsd
cmp ecx, dword ptr [esi+ebx*2]
push es
test al, FFh
add eax, 7ACFC8B5h
mov al, byte ptr [14054FDAh]
loope 00007FD560ACA8ABh
mov al, A6h
mov cl, 2Bh
and bl, ch
add cl, byte ptr [esp+edx]
add ebp, edi
push di
xor ecx, eax
xor cl, byte ptr [edx-74h]
push es
test dword ptr [ecx+2D1ECDBDh], edx
mov eax, 591202C8h
fistp qword ptr [edi+4Dh]
shl ebp, cl
inc eax
popad
xchg eax, ecx
cmp dword ptr [eax+0000002Fh], eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1034ea8	0x8c	.tve
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10b8000	0x4c279	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10b7360	0x38	.tve
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x71f000	0x1f0	.(Y,
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x187f8	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1a000	0x298a	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1d000	0x5dc	0x200	False	0.02734375	data	0.020393135236084953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.Y :	0x1e000	0x7002d1	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.(Y,	0x71f000	0x374	0x400	False	0.466796875	data	3.4850465125342907	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tve	0x720000	0x9973a0	0x997400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x10b8000	0x4c279	0x4c400	False	0.448377675689019	data	5.232399128159855	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10b8250	0x368	Device independent bitmap graphic, 16 x 32 x 24, image size 832		
RT_ICON	0x10b85b8	0x748	Device independent bitmap graphic, 24 x 48 x 24, image size 1824		
RT_ICON	0x10b8d00	0xca8	Device independent bitmap graphic, 32 x 64 x 24, image size 3200		
RT_ICON	0x10b99a8	0x1ca8	Device independent bitmap graphic, 48 x 96 x 24, image size 7296		
RT_ICON	0x10bb650	0x3228	Device independent bitmap graphic, 64 x 128 x 24, image size 12800		
RT_ICON	0x10be878	0x70a8	Device independent bitmap graphic, 96 x 192 x 24, image size 28800		
RT_ICON	0x10c5920	0xc828	Device independent bitmap graphic, 128 x 256 x 24, image size 51200		
RT_ICON	0x10d2148	0x32028	Device independent bitmap graphic, 256 x 512 x 24, image size 204800		
RT_GROUP_ICON	0x1104170	0x76	data		
RT_MANIFEST	0x11041e8	0x91	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	LocalSize, lstrlenA, LocalAlloc, IsBadCodePtr, GetProcAddress, LoadLibraryA
GDI32.dll	GetDeviceCaps
ole32.dll	CoInitialize
KERNEL32.dll	GetSystemTimeAsFileTime, GetModuleHandleA, CreateEventA, GetModuleFileNameW, TerminateProcess, GetCurrentProcess, CreateToolhelp32Snapshot, Thread32First, GetCurrentProcessId, GetCurrentThreadId, OpenThread, Thread32Next, CloseHandle, SuspendThread, ResumeThread, WriteProcessMemory, GetSystemInfo, VirtualAlloc, VirtualProtect, VirtualFree, GetProcessAffinityMask, SetProcessAffinityMask, GetCurrentThread, SetThreadAffinityMask, Sleep, LoadLibraryA, FreeLibrary, GetTickCount, SystemTimeToFileTime, FileTimeToSystemTime, GlobalFree, LocalAlloc, LocalFree, GetProcAddress, ExitProcess, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSection, DeleteCriticalSection, GetModuleHandleW, LoadResource, MultiByteToWideChar, FindResourceExW, FindResourceExA, WideCharToMultiByte, GetThreadLocale, GetUserDefaultLCID, GetSystemDefaultLCID, EnumResourceNamesA, EnumResourceNamesW, EnumResourceLanguagesA, EnumResourceLanguagesW, EnumResourceTypesA, EnumResourceTypesW, CreateFileW, LoadLibraryW, GetLastError, FlushFileBuffers, WriteConsoleW, SetStdHandle, IsProcessorFeaturePresent, DecodePointer, GetCommandLineA, RaiseException, HeapFree, GetCPInfo, InterlockedIncrement, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, SetLastError, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, LCMapStringW, GetStringTypeW, SetHandleCount, GetStdHandle, InitializeCriticalSectionAndSpinCount, GetFileType, GetStartupInfoW, GetModuleFileNameA, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapCreate, HeapDestroy, QueryPerformanceCounter, HeapSize, WriteFile, RtlUnwind, SetFilePointer, GetConsoleCP, GetConsoleMode, HeapReAlloc, VirtualQuery
USER32.dll	CharUpperBuffW
KERNEL32.dll	LocalAlloc, LocalFree, GetModuleFileNameW, ExitProcess, LoadLibraryA, GetModuleHandleA, GetProcAddress

Possible Origin		
Language of compilation system	**Country where language is spoken**	**Map**
English	United States	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

No system behavior

Disassembly

No disassembly