ID: 377790
Sample Name:
PHOTOCHLORINATION.exe
Cookbook: default.jbs
Time: 23:35:50
Date: 29/03/2021
Version: 31.0.0 Emerald

Table of Contents

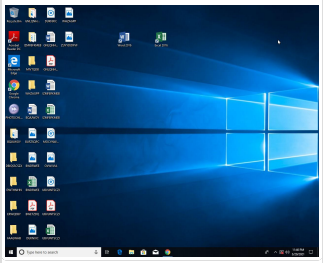
Analysis Report PHOTOCHLORINATION.exe

Overview

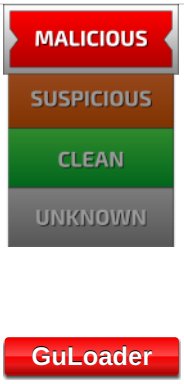
General Information

Sample Name:	PHOTOCHLORINATION.exe
Analysis ID:	377790
MD5:	584c030ac9abd5..
SHA1:	6deb5d5b469ba5..
SHA256:	59662ea91566a6..
Tags:	GuLoader
Infos:	

Most interesting Screenshot:



Detection

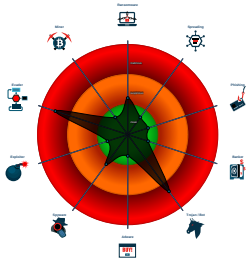


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to query CPU …
- Contains functionality to read the PEB
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- PHOTOCHLORINATION.exe (PID: 3000 cmdline: 'C:\Users\user\Desktop\PHOTOCHLORINATION.exe' MD5: 584C030AC9ABD52C2347214088B1FA14)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

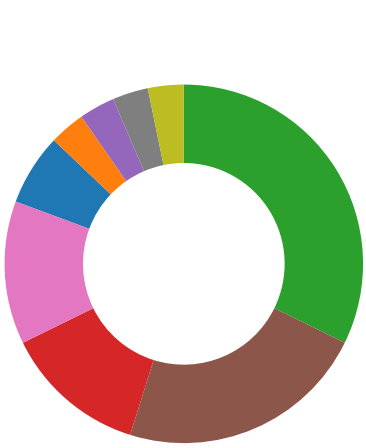
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: PHOTOCHLORINATION.exe PID: 3000	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: PHOTOCHLORINATION.exe PID: 3000	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

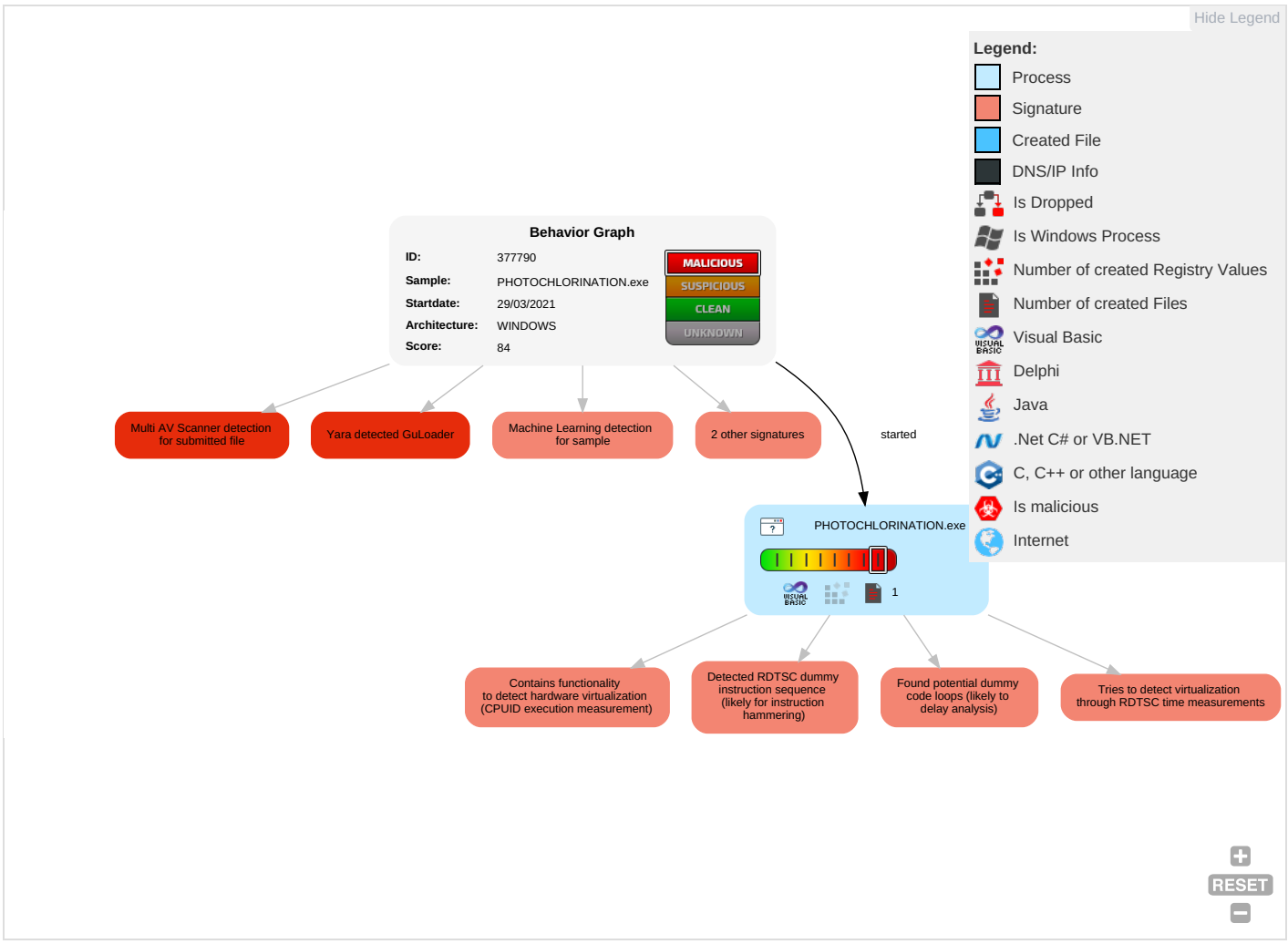
Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 5 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PHOTOCHLORINATION.exe	28%	Virustotal		Browse
PHOTOCHLORINATION.exe	10%	ReversingLabs	Win32.Backdoor.Remcos	
PHOTOCHLORINATION.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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	377790
Start date:	29.03.2021
Start time:	23:35:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PHOTOCHLORINATION.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	1
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.8% (good quality ratio 16.5%) • Quality average: 35.5% • Quality standard deviation: 37.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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):	5.51678687133476
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	PHOTOCHLORINATION.exe
File size:	86016
MD5:	584c030ac9abd52c2347214088b1fa14
SHA1:	6deb5d5b469ba5f63e937bb093281911eab7c054
SHA256:	59662ea91566a6d7578243f8f9ad28d84c2908ba17be418 f0a45cdd218272b0b
SHA512:	3105eacef92279f9a6e666152c5b2ae4f7d5c1fb60ed3ed d3783713fee81b486f06c69580f23c7936e425f26b63c08 0a4df174056ece800ca7f5263fa37061e9
SSDEEP:	768:QaMTZied1gEdEZzH9n8O9MA8f7eyGOjYkrch+rIU k/RjvMgE7D0Bq0XqhyLctUri:JeZZgMYQ9HGOPUekjM AE
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....u...1...1. ..1.....0...~...0.....0...Rich1.....PE..L...[..N..... .....0.....8..... ....@.....

File Icon

Icon Hash:	f1f8f6f0f0e4f831

Static PE Info

General	
Entrypoint:	0x401538
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4EC7825B [Sat Nov 19 10:18:03 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3ecd501451a806efb69c3dc3e8601427

Entrypoint Preview

Instruction
push 0040CBB0h
call 00007FA7A4D97CB3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
dec eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], ch
cmp ch, al
dec esp
or al, B1h
adc eax, dword ptr [edi-7Eh]
sti
dec ebx
xchg byte ptr [ebx-65h], cl
jns 00007FA7A4D97CC2h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, cl
jnle 00007FA7A4D97CC7h
add eax, dword ptr [ecx+72h]
bound esp, dword ptr [ebp+6Ah]
jnc 00007FA7A4D97D30h
popad
jc 00007FA7A4D97D2Dh
jnc 00007FA7A4D97D34h
outsd
insb
imul esi, dword ptr [ecx+ebp*2+6Bh], 00000000h
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or dword ptr [edi-72h], esp
add edi, ecx
enter DBADh, 42h

Instruction
mov dword ptr [edx], esi
pop edx
aas
lodsb
lodsd
cmpsd
and ah, byte ptr [ebx]
mov dh, 57h
pop ebp
push ebx
mov word ptr [ecx], fs
inc ecx
mov ch, al
enter C9ECh, B3h
inc edx
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
outsd
mov ch, 00h
add bl, ah
mov bl, 00h
add byte ptr [eax], al
pop es
add byte ptr [ebx+4Bh], dl
inc ebp
push eax
push ebx
dec ecx
push ebx
add byte ptr [00000D01h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x116e4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x13000	0x1412	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x128	.text
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
.text	0x1000	0x10bdc	0x11000	False	0.442899816176	data	6.14512004052	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0xa50	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x13000	0x1412	0x2000	False	0.291137695312	data	3.29788287231	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x13d4a	0x6c8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x133c2	0x988	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x133a0	0x22	data		
RT_VERSION	0x13120	0x280	data	Guarani	Paraguay

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaLineInputStr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaLateMemSt, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFPFix, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, __vbaObjVar, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaFileOpen, __vbaNew2, __vbaR8Str, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarAdd, __vbaVarDup, __vbaLateMemCallLd, _CIatan, __vbaCastObj, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0474 0x04b0
InternalName	PHOTOCHLORINATION
FileVersion	3.03
CompanyName	Sanyo
Comments	Sanyo
ProductName	Sanyo
ProductVersion	3.03
FileDescription	Sanyo
OriginalFilename	PHOTOCHLORINATION.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Guarani	Paraguay	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: PHOTOCHLORINATION.exe PID: 3000 Parent PID: 5908

General

Start time:	23:36:38
Start date:	29/03/2021
Path:	C:\Users\user\Desktop\PHOTOCHLORINATION.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PHOTOCHLORINATION.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	584C030AC9ABD52C2347214088B1FA14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis