ID: 778224
Sample Name: Yoh6xJ4fc5.exe
Cookbook: default.jbs
Time: 08:20:10
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

Yoh6xJ4fc5.exe

Overview

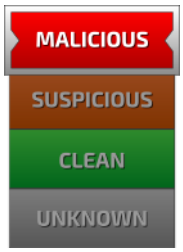
General Information

Sample Name:	Yoh6xJ4fc5.exe
Analysis ID:	778224
MD5:	d14ceedb53cf53…
SHA1:	ba84d27b6ce687..
SHA256:	118c81907f82df9..
Tags:	exe
Infos:	YARA

Errors

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

Detection

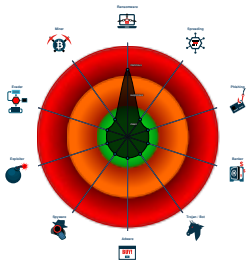


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Yara signature match
- Sample file is different than original …
- PE file contains an invalid checksum
- PE file overlay found
- PE file contains executable resourc…

Classification



Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Yoh6xJ4fc5.exe	Linux_Trojan_Pornoasset_927f314f	unknown	unknown	• 0x146304:$a: C3 D3 CB D3 C3 48 31 C3 48 0F AF F0 48 0F AF F0 48 0F AF F0 48

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

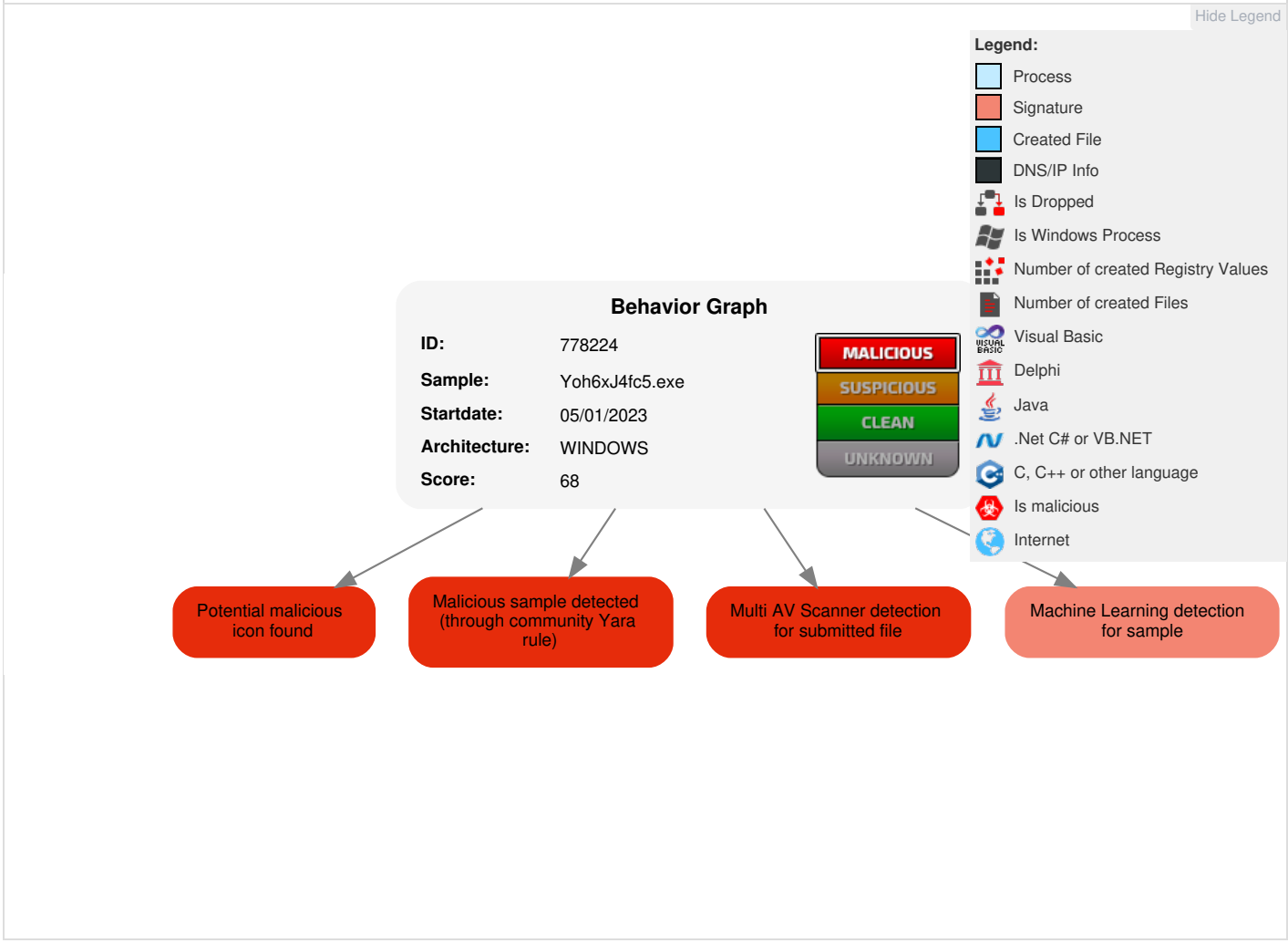
Malicious sample detected (through community Yara rule)

Potential malicious icon found

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
Yoh6xJ4fc5.exe	44%	Virustotal		Browse
Yoh6xJ4fc5.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:	36.0.0 Rainbow Opal
Analysis ID:	778224
Start date and time:	2023-01-05 08:20:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Yoh6xJ4fc5.exe
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
Detection:	MAL
Classification:	mal68.rans.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

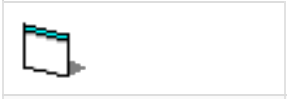
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.225533763154112
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:	Yoh6xJ4fc5.exe
File size:	2164910
MD5:	d14ceedb53cf5316ecc6a09eace27be4
SHA1:	ba84d27b6ce687fe6360fa1f55efd78fca01f94f
SHA256:	118c81907f82df9e435fc2dae7ab84cf61d07f628ac1238f615fdc16c81e6a88
SHA512:	e644633ca5a6a1ff368b8ff5fee3cafeec43475e68a715dfa72f0fa4051d117872da1bfaeef6ca163a6c309e0a7e7a4ac45315502feba8e770e57345f6302e36
SSDEEP:	49152:0/2N9SdDAe7HNEZ6ia/ulEVuaMYEuFShvXAaiW5DjocFtZLj2XMhpF25FxjZVqiQ:0/eSdMeEZvlEVuaMYPShvXAaiW5Djocb
TLSH:	4FA52917E19350FCC67BC134875BA573B972F86912307EBF2664DB342E62E60262DB24
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K...*...*...*...6...*...5...*..t5...*..Rich.*.....PE..L....fvb.....0...@.....@....@.....

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401318
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x62766604 [Sat May 7 12:28:52 2022 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:	1a903a65eaa735683683eef11a03cfb0

Entrypoint Preview

Instruction
push 004014A4h
call 00007F3B60F99AB5h
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
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, al
mov bl, A9h
in eax, 63h
or dh, byte ptr [ebx+0F7D8943h]
and esi, ebx
inc edi
jecxz 00007F3B60F99AC2h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], dh
xor dh, byte ptr [eax]
xor al, 33h
xor byte ptr [eax+72h], dl
outsd
push 00000065h
arpl word ptr [ecx+esi+00h], si
xor byte ptr [30303043h], ch
sub eax, 00000000h

Instruction
dec esp
xor dword ptr [eax], eax
add byte ptr [esp+edx], bh
mov seg?, word ptr [ecx]
add cl, 0000002Ah
inc esp
xchg eax, ebx
mov ecx, 975E124Ch
imul ebx, dword ptr [edi+582A52BDh], 4B86047Eh
xchg byte ptr [esi-56h], bh
retn 58EAh
sqrtps xmm7, dqword ptr [edx]
dec edi
lodsd
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
inc ebp
add byte ptr [eax], al
add byte ptr [eax+00h], al
add byte ptr [eax], al
add byte ptr [726F4600h], al
insd
xor dword ptr [eax], eax
or eax, 46000501h
outsd
jc 00007F3B60F99B2Fh
xor dword ptr [eax], eax
sbb dword ptr [ecx], eax
add byte ptr [edx+00h], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2be4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5000	0x7f2f3c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x230	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xf4	.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	0x2080	0x3000	False	0.2984212239583333	data	4.071789033390128	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x4000	0xa5c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x5000	0x7f2f3c	0x7f3000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
CUSTOM	0x7f7e7c	0xc0	empty	English	United States
CUSTOM	0x7f45ac	0x38d0	empty	English	United States
CUSTOM	0x59ac	0x7eec00	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows	English	United States
RT_ICON	0x587c	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 256		
RT_ICON	0x5594	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640		
RT_ICON	0x546c	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192		
RT_GROUP_ICON	0x543c	0x30	data		
RT_VERSION	0x5250	0x1ec	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaPutOwner3, __vbaI2I4, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaVarCat, _CIlog, __vbaFileOpen, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarSetVar, __vbaStrToAnsi, __vbaVarLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

No system behavior

Disassembly

No disassembly