ID: 490252
Sample Name: ryxu0LoCH3.exe
Cookbook: default.jbs
Time: 10:12:14
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Windows Analysis Report ryxu0LoCH3.exe

Overview

General Information

Sample Name:	ryxu0LoCH3.exe
Analysis ID:	490252
MD5:	0ad6beff5dc6704..
SHA1:	b4536a89dbaa58..
SHA256:	6b364b7c12a4e4..
Tags:	exe
Infos:	

Errors

- Nothing to analyse, Joe Sandbox has not found any analysis process or sample
- Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.

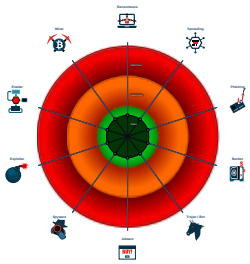
Detection

Score:	22
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Machine Learning detection for samp…
- PE file overlay found
- Uses 32bit PE files
- PE file contains sections with non-s…
- PE file contains an invalid checksum

Classification



Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

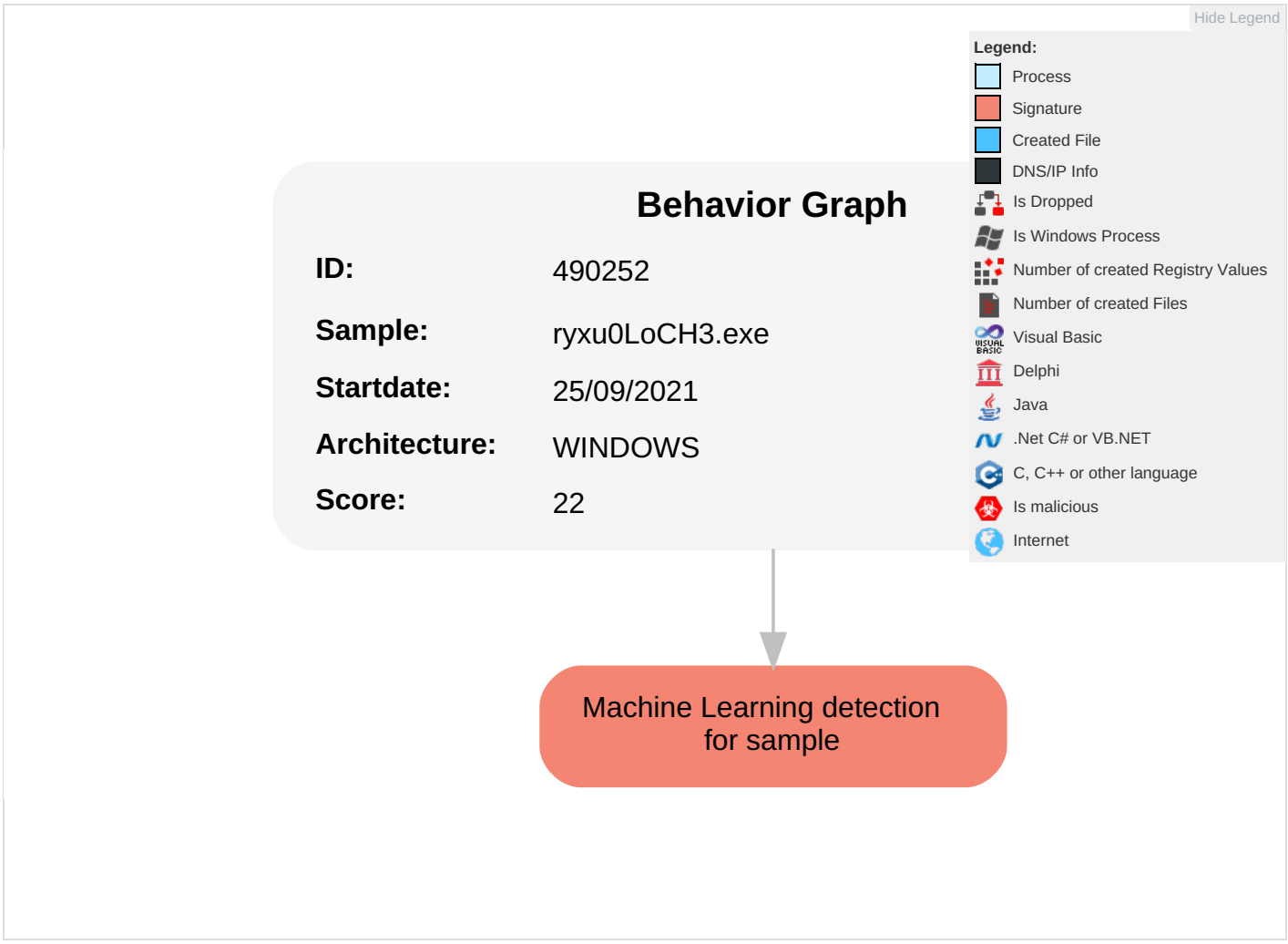
Machine Learning detection for sample

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

Copyright Joe Security LLC 2021

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ryxu0LoCH3.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490252
Start date:	25.09.2021
Start time:	10:12:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ryxu0LoCH3.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:	4
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:	SUS
Classification:	sus22.winEXE@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Unable to launch sample, stop analysis
Warnings:	Show All
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample • Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Copyright Joe Security LLC 2021

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):	2.0948410959489343
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:	ryxu0LoCH3.exe
File size:	1040347
MD5:	0ad6beff5dc6704a93dc36ea43dc739c
SHA1:	b4536a89dbaa58deb5c5ef299d71982259521d91
SHA256:	6b364b7c12a4e4d7f7275006be3adc70984086843f1cd01 3b2745ecbbb8fca00
SHA512:	893b7c98a41dbdc97418702462bc539ecdc2b6fdbecc64 8adad213880ca19155ce24cd15115e681c0f3afc4f7c086 45420a1467a7bc4c4ebf469d9a40dd72141
SSDEEP:	3072:CORDINSkUIWnxw8CmtqvylJ10nkcvryr5dqT0NM dIp2uogBpUDZyL+UoPxwAnjac:Ti+qg0vryiT0NMd+2u/ NLGb
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L..... ;a.....................p...D...F............@.................................... ....

File Icon

Icon Hash:	aca9a8acaca6a888

Static PE Info

General

Entrypoint:	0x404612
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x613B8C85 [Fri Sep 10 16:49:09 2021 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:	15cdf6e35545e491e70d9cafb0fc7871

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d054	0x2d200	False	0.412883050554	data	6.07840510931	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2f000	0x1000	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x30000	0x400201c	0x4400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4033000	0x13c54	0x13e00	False	0.147270538522	data	4.78681021699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lwox	0x4047000	0x45000	0x45000	False	0.00105086616848	data	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.vvny	0x408c000	0x48000	0x48000	False	0.00104437934028	data	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.vtbg	0x40d4000	0x45000	0x45000	False	0.00109533354036	data	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.qtxm	0x4119000	0x45000	0x45000	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021