

JoeSandbox Cloud BASIC



**ID:** 321438

**Sample Name:** ZHR2970.EXE

**Cookbook:** default.jbs

**Time:** 05:54:35

**Date:** 22/11/2020

**Version:** 31.0.0 Red Diamond

# Table of Contents

Table of Contents	2
Analysis Report ZHR2970.EXE	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
Mitre Att&ck Matrix	4
Antivirus, Machine Learning and Genetic Malware Detection	4
Initial Sample	4
Dropped Files	4
Unpacked PE Files	4
Domains	4
URLs	4
Domains and IPs	4
Contacted Domains	4
Contacted IPs	4
General Information	4
Simulations	5
Behavior and APIs	5
Joe Sandbox View / Context	5
IPs	5
Domains	5
ASN	5
JA3 Fingerprints	5
Dropped Files	5
Created / dropped Files	6
Static File Info	6
General	6
File Icon	6
Network Behavior	6
Code Manipulations	6
Statistics	6
System Behavior	6
Disassembly	7


# Analysis Report ZHR2970.EXE


## Overview

General Information

Sample Name:	ZHR2970.EXE
Analysis ID:	321438
MD5:	796956fcf58ff688..
SHA1:	6f2efcc9970286f...
SHA256:	4762bcdde5768b..

Errors

 Nothing to analyse, Joe Sandbox has not found any analysis process or sample

 Corrupt sample or wrongly selected analyzer. Details: The image file %1 is valid, but is for a machine type other than the current machine.

Detection

MALICIOUS

SUSPICIOUS

CLEAN

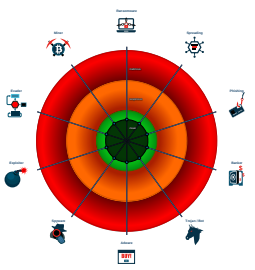
UNKNOWN

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

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

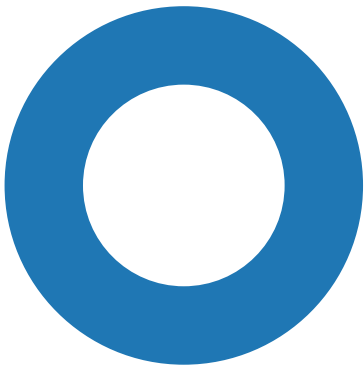
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



● [System Summary](#)

There are no malicious signatures, [click here to show all signatures](#).

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	System Information Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
ZHR2970.EXE	0%	Virustotal		<a href="#">Browse</a>
ZHR2970.EXE	2%	Metadefender		<a href="#">Browse</a>
ZHR2970.EXE	3%	ReversingLabs		

### 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

Analysis ID:	321438
Start date:	22.11.2020
Start time:	05:54:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZHR2970.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:	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:	<ul style="list-style-type: none"> <li>• EGA enabled</li> <li>• HDC enabled</li> <li>• AMSI enabled</li> </ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.winEXE@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none"> <li>• Adjust boot time</li> <li>• Enable AMSI</li> <li>• Found application associated with file extension: .EXE</li> <li>• Unable to launch sample, stop analysis</li> </ul>
Errors:	<ul style="list-style-type: none"> <li>• Nothing to analyse, Joe Sandbox has not found any analysis process or sample</li> <li>• Corrupt sample or wrongly selected analyzer. Details: The image file %1 is valid, but is for a machine type other than the current machine.</li> </ul>

## 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:	MS-DOS executable, LZEXE v0.90 compressed
Entropy (8bit):	7.437933132842257
TrID:	<ul style="list-style-type: none"><li>• LZEXE compressed DOS executable (2015/5) 9.14%</li><li>• Generic Win/DOS Executable (2004/3) 9.09%</li><li>• Win64 Device Driver (generic) (2002/3) 9.08%</li><li>• Win32 Device Driver (generic) (2002/3) 9.08%</li><li>• DOS Executable Generic (2002/1) 9.08%</li></ul>
File name:	ZHR2970.EXE
File size:	2320
MD5:	796956fcf58ff688a2e8df96317ca2fb
SHA1:	6f2efcc9970286fe8931f038897cae0cd9e802f0
SHA256:	4762bcdde5768b0d75bdbbd6c129f7301b87e902f54992f21898d799596d92a5
SHA512:	b69215341248db99481b60f2a99700c476d149c9bf2af6b5013e4d891f6640d8ba9f1db5538fe2b175537cd018bedaa79bb943ba4c2feb8c7931d799e0361677
SSDEEP:	48:p58jE5riSZzdmWCJ01azopMlyfCMlreCEzFMgNRkBwDKK9:p5hrzzAWHaskmyg2OKs
File Content Preview:	MZ.....r.....LZ09..Copyright (C) 1..986 by John Soch..a.....u.....#.....*.....0.....0!.....&.....=.....Y.r..N..=.....L..?.....PSQ.....+.....J..Y[X..P.....C.z#%.....~..R..S.....D.!..Z.Z..V...m.;..

File Icon

	
Icon Hash:	00828e8e8686b000

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

