ID: 882714
Sample Name: Order.gz.exe
Cookbook: default.jbs
Time: 17:27:42
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

Windows Analysis Report

Order.gz.exe

Overview

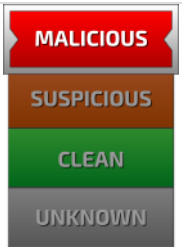
General Information

Sample Name:	Order.gz.exe
Analysis ID:	882714
MD5:	856dbd09409d…
SHA1:	04ac238a5349…
SHA256:	8873e65ad529…
Tags:	exe STRRAT
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



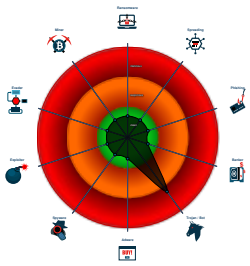
RATDispenser

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected RATDispenser

Classification



Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Order.gz.exe	JoeSecurity_RATDispenser	Yara detected RATDispenser	Joe Security	

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

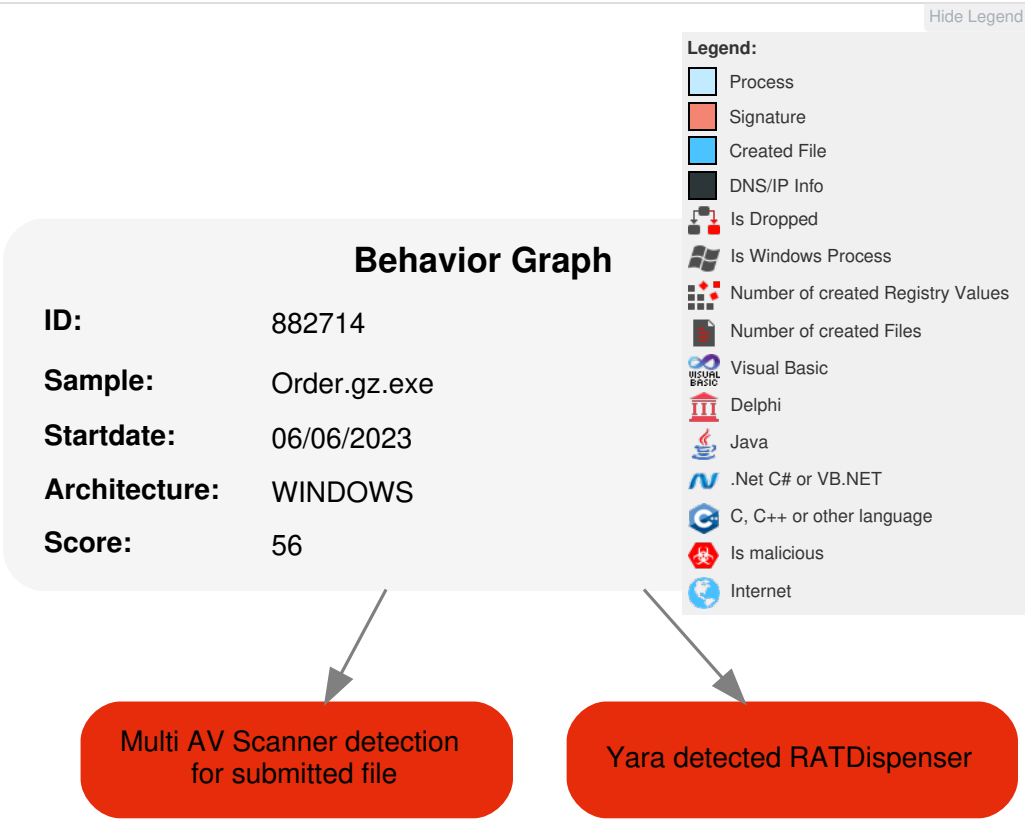
Data Obfuscation

Yara detected RATDispenser

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
Order.gz.exe	46%	ReversingLabs	Script-JS.Trojan.Cryxos	
Order.gz.exe	44%	Virustotal		Browse

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:	37.1.0 Beryl
Analysis ID:	882714
Start date and time:	2023-06-06 17:27:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 28s
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
Run name:	Without Instrumentation
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:	Order.gz.exe
Detection:	MAL
Classification:	mal56.troj.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:	ASCII text, with very long lines (64177), with CRLF line terminators
Entropy (8bit):	5.591378716994313
TrID:	• 669 Tracker Module (2002/1) 100.00%
File name:	Order.gz.exe
File size:	368827
MD5:	856dbd09409da8b58b98d75bb8b6c7c0
SHA1:	04ac238a5349afe2f3f0a2dffad9cf615130b674
SHA256:	8873e65ad529e832113ee75d5bc8e3a18d150ed475c09e0c6f5ce1458f0bf9a3
SHA512:	bfe9543baef25017dd61339c75c9c38d05bd903256cc592a5b964055bb62fd932422714461557c8fc8a2ea280d56627dd52e0cd9a990a3ad787dff27fbf195bc
SSDEEP:	6144:1piSQi4W9Bmmdk2DT0uYdIHIBIbmSmSBJB6fmpXAhtagxMI2b+ORpNqE3KqT:1fHX/mKaSvoGX4tagutDo8T
TLSH:	90747D6A49AC1225DF74620DD89717BFE0B4962EF1B7C04F7BE91BDEAE2150D180B20D
File Content Preview:	if (typeof {} != "array") {.. String.prototype.xX7rOlQ = function () {.. var kd3$_ = "";...var hDrF04m = "5=jLUS.XNv4TY789JnGqkAogFbECP";...hDrF04m = hDrF04m + 'QBlwD2KOWV6suaRpdfrzHcM1ty0hiZxemI3"';.....var inDu4Sl = str2arr(this, " ");...var tmmp =

File Icon

Icon Hash:	90cecececе8e8eb0

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

No system behavior

Disassembly

No disassembly