ID: 296302
Sample Name: transferir.exe
Cookbook: default.jbs
Time: 16:10:08
Date: 11/10/2020
Version: 30.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report transferir.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
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 5
Domains and IPs 6
Contacted Domains 6
Contacted IPs 6
General Information 6
Simulations 6
Behavior and APIs 6
Joe Sandbox View / Context 7
IPs 7
Domains 7
ASN 7
JA3 Fingerprints 7
Dropped Files 7
Created / dropped Files 7
Static File Info 7
General 7
File Icon 7
Network Behavior 7
Code Manipulations 8
Statistics 8
System Behavior 8
Disassembly 8

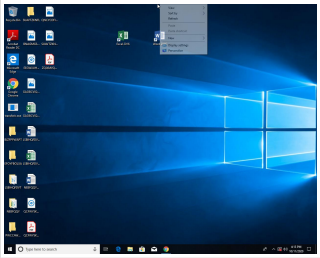
Analysis Report transferir.exe

Overview

General Information

Sample Name:	transferir.exe
Analysis ID:	296302
MD5:	4842e206e4cfff2…
SHA1:	80c9820ff2efe8a…
SHA256:	2acab1228e8935..

Most interesting Screenshot:



Errors

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

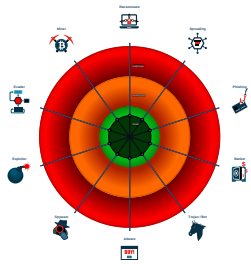
Detection

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

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

Yara Overview

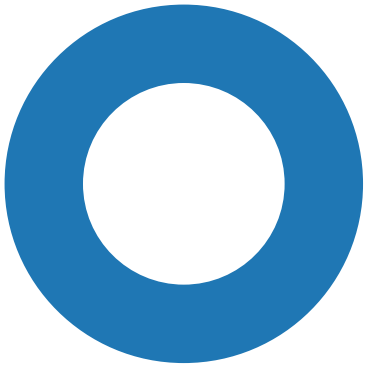
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- System Summary



Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

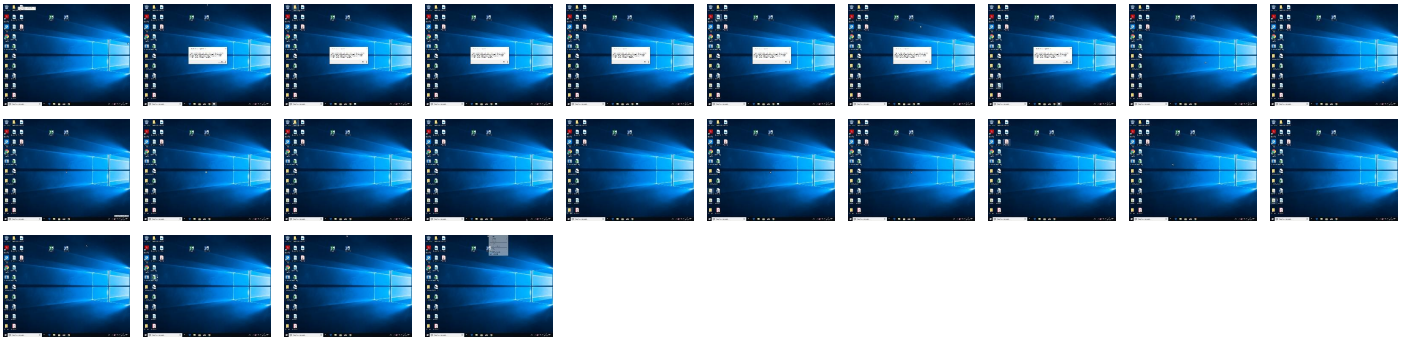
Mitre Att&ck Matrix

No Mitre Att&ck techniques found

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
transferir.exe	0%	Virustotal		Browse
transferir.exe	0%	Metadefender		Browse
transferir.exe	0%	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

Joe Sandbox Version:	30.0.0 Red Diamond
Analysis ID:	296302
Start date:	11.10.2020
Start time:	16:10:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	transferir.exe
Cookbook file name:	default.jbs
Analysis system description:	w10x64 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:	17
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:	UNKNOWN
Classification:	unknown0.winEXE@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample

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:	data
Entropy (8bit):	1.9219280948873623
TrID:	
File name:	transferir.exe
File size:	5
MD5:	4842e206e4cfff2954901467ad54169e
SHA1:	80c9820ff2efe8aa3d361df7011ae6eee35ec4f0
SHA256:	2acab1228e8935d5dfdd1756b8a19698b6c8b786c90f879 93ce9799a67a96e4e
SHA512:	ff537b1808fcb03cfb52f768fbd7e7bd66baf6a8558ee5b8f 2a02f629e021aa88a1df7a8750bae1f04f3b9d86da56f0bd cba2fdbc81d366da6c97eb76ecb6cba
SSDEEP:	3:w:w
File Content Preview:	0....

File Icon

Icon Hash:	00828e8e8686b000

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly