

JOeSandbox Cloud BASIC



**ID:** 452329

**Sample Name:** Checks-  
Lists.htm\_

**Cookbook:** default.jbs

**Time:** 06:35:47

**Date:** 22/07/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report Checks-Lists.htm_	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Malware Configuration	3
Yara Overview	3
Initial Sample	3
Sigma Overview	3
Jbx Signature Overview	3
Phishing:	3
Mitre Att&ck Matrix	4
Behavior Graph	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	6
IPs	6
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	7
Statistics	8
System Behavior	8
Disassembly	8

# Windows Analysis Report Checks-Lists.htm\_

## Overview

### General Information

Sample Name:

Checks-Lists.htm\_

Analysis ID:

452329

MD5:

e425a0a3fbc7d10.


SHA1:

2a2c33635681b0..

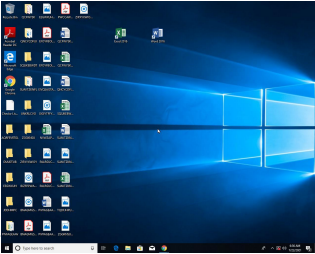
SHA256:

6d5fde6ca1bc806..


Infos:




Most interesting Screenshot:



Errors

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

 Corrupt sample or wrongly selected configuration file R000163

Malware Configuration

No configuration details found

### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

HTMLPhisher

Score:

56

Range:

0 - 100

Whitelisted:

false

Confidence:

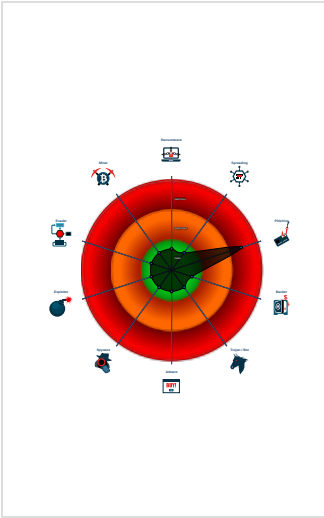
100%

### Signatures

Yara detected HtmlPhish44

Yara detected HtmlPhish6

### Classification



## Yara Overview


### Initial Sample

Source	Rule	Description	Author	Strings
Checks-Lists.htm_	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	
Checks-Lists.htm_	JoeSecurity_HtmlPhish_6	Yara detected HtmlPhish_6	Joe Security	

## Sigma Overview

No Sigma rule has matched

## Jbx Signature Overview

 Click to jump to signature section

### Phishing:



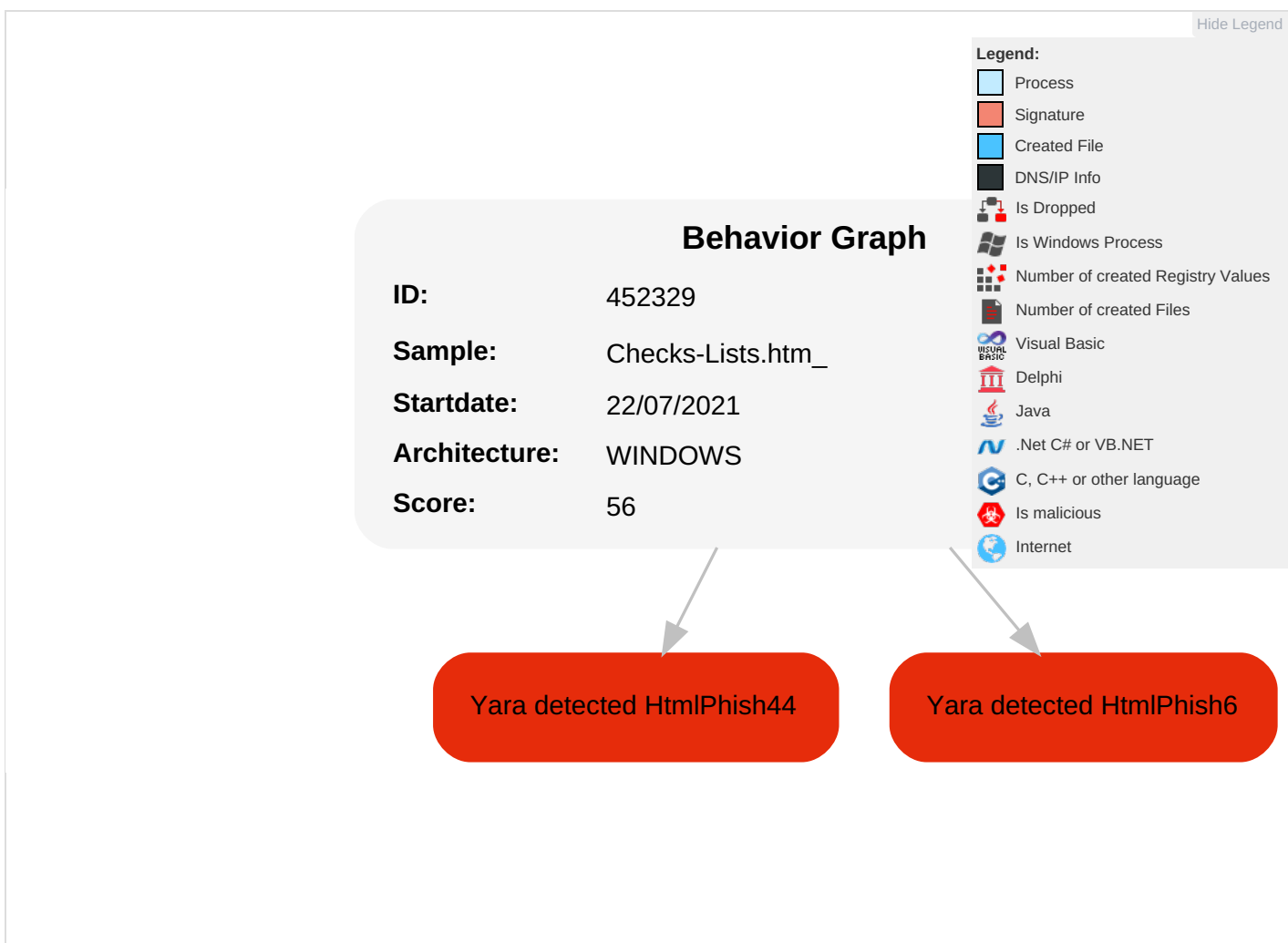
Yara detected HtmlPhish44

Yara detected HtmlPhish6

## Mitre Att&ck Matrix

No Mitre Att&ck techniques found

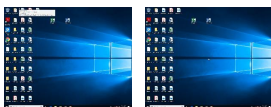
## Behavior Graph



## 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
Checks-Lists.htm_	3%	Virustotal		<a href="#">Browse</a>

### 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:	33.0.0 White Diamond
Analysis ID:	452329
Start date:	22.07.2021
Start time:	06:35:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Checks-Lists.htm_
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:	MAL
Classification:	mal56.phis.winHTM_@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</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: 80040153</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:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.8911559931066915
TrID:	
File name:	Checks-Lists.htm_
File size:	33879
MD5:	e425a0a3fbc7d10cbc4356bef4b9c6f8
SHA1:	2a2c33635681b0834508d33f8e02cfa2fd680e6
SHA256:	6d5fde6ca1bc80611ee7708a71aa9577b8efad6faad9b85e44d7aeb4d57af7a5
SHA512:	f6b013d72eb230fd4c9c8e87011c82bc70589dff47fa8ce1cb3c8aae813b3fb59ac8d9f1dacfd6cf0c9a5a23b10713358024300c2d0272eac3b0e1d13b6959d0
SSDEEP:	384:ZDKouXieT2FRdddT4q/qxhhCmwaJcw6LihTLV5qTLCxHwv3xivT1:ZDPFCx9NbjxM3xs
File Content Preview:	<script language="javascript">document.write( unescape( "%3C%21doctype%20html%3E%0A%3Chtml%20lang%3D%22en%22%3E%0A%0A%3Chead%3E%0A%20%20%3Cscript%20src%3D%22https%3A//code.jquery.com/jquery-3.1.1.min.js%22%20crossorigin%3D%22anonymous%22%3E%3C/script%3E%0

## File Icon

	
Icon Hash:	74f0e4e4e4e4e0e4

## Network Behavior

No network behavior found

## Code Manipulations

## Statistics

## System Behavior

## Disassembly