JOE Sandbox Cloud BASIC

ID: 553054
Sample Name: dhl-2020.pdf.shtm
Cookbook: default.jbs
Time: 08:25:40
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report dhl-2020.pdf.shtm

Overview

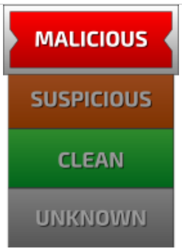
General Information

Sample Name:	dhl-2020.pdf.shtm
Analysis ID:	553054
MD5:	7291ee45c17c3c..
SHA1:	10bdc7316476d8..
SHA256:	320d192a03a6eb..
Infos:	HCA

Errors

- ⚠ No process behavior to analyse as no analysis process or sample was found
- ⚠ Corrupt sample or wrongly selected analyzer. Details: 80040153

Detection



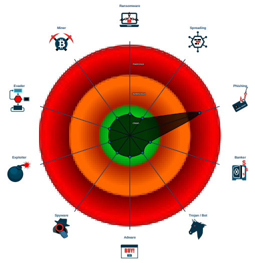
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected obfuscated html page
- Multi AV Scanner detection for subm…
- Yara detected HtmlPhish44

Classification



Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
dhl-2020.pdf.shtm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
dhl-2020.pdf.shtm	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

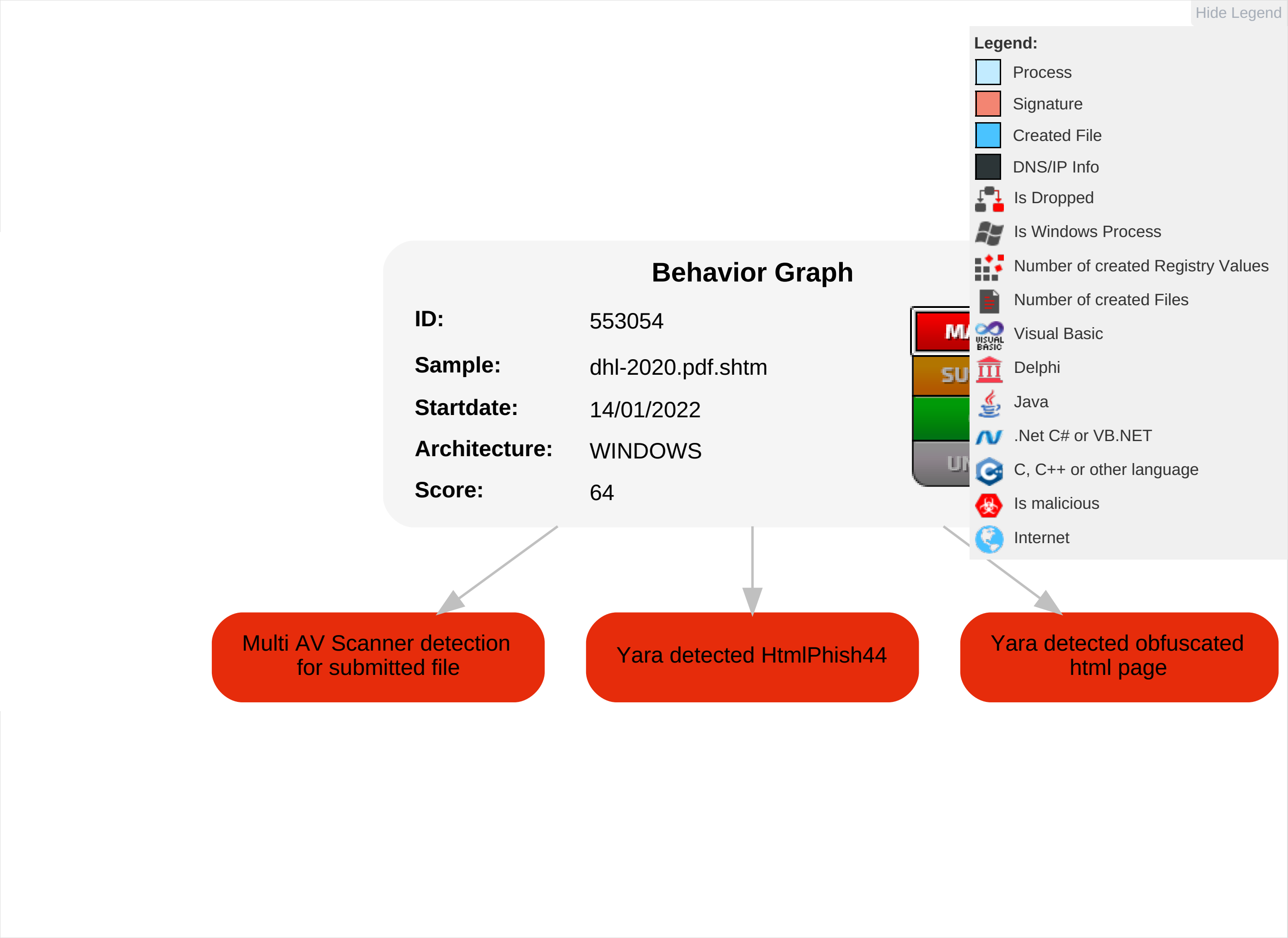
Phishing:

Yara detected obfuscated html page
Yara detected HtmlPhish44

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

Behavior Graph



Hide Legend

Behavior Graph

ID:	553054
Sample:	dhl-2020.pdf.shtm
Startdate:	14/01/2022
Architecture:	WINDOWS
Score:	64

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dhl-2020.pdf.shtm	25%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://snapbuilder.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553054
Start date:	14.01.2022
Start time:	08:25:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dhl-2020.pdf.shtm
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:	9
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:	MAL
Classification:	mal64.phis.winSHTM@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to launch sample, stop analysis
Warnings:	Show All
Errors:	• No process behavior to analyse as no analysis process or sample was found • Corrupt sample or wrongly selected analyzer. Details: 80040153

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):	3.1376659530523456
TrID:	
File name:	dhl-2020.pdf.shtm
File size:	725915
MD5:	7291ee45c17c3c3a982afe4adb84d383
SHA1:	10bdc7316476d8fcfe8950ed667030196fbaa0c2
SHA256:	320d192a03a6eb25ef124898c31f35753679e38b2b51c74 43406d262ae63b6b5
SHA512:	a8693a59e42d6487c016928b728d6d12e69d007f92fde6f b6a9c3f251ee00d5e13d69d682a8b47872e08e9fcb61e3e 877585924968b7bb8a749344e533e1b1f0
SSDEEP:	768:91dB6q4r5263pKdQ3VKt35KU3JKAg+YUTG4MNjNtivVNhHHfwSiBSSKISZSS+oSz:6G8gM
File Content Preview:	<script language="javascript">.. ..// == Begin Free HTML Source Code Obfuscation Protection from https://snapbuilder.com == //..document.write(unescape('%0A%3C%21%64%6F%63%74%79%70%65%20%68%74%6D%6C%3E%0A%3C%68%74%6D%6C%20%6C%61%6E%67%3D%22%65%6E%22%3E

File Icon

🗋	
Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly