JoeSandbox Cloud BASIC

ID: 412882
Sample Name: HTM
Cookbook: default.jbs
Time: 02:26:26
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

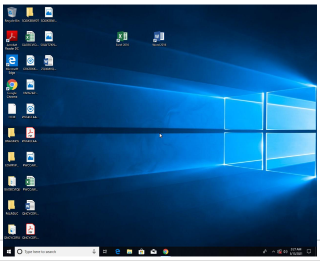
Analysis Report HTM

Overview

General Information

Sample Name:	HTM
Analysis ID:	412882
MD5:	35962556551e11..
SHA1:	413f182eed91659.
SHA256:	357915a1fd342de.
Infos:	HCA

Most interesting Screenshot:



Errors

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

⚠ Corrupt sample or wrongly selected analyzer. Details: 80040153

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

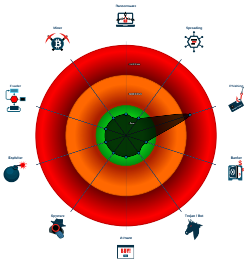
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected HtmlPhish44

Classification



Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
HTM	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- ● Phishing
- ● System Summary

Click to jump to signature section

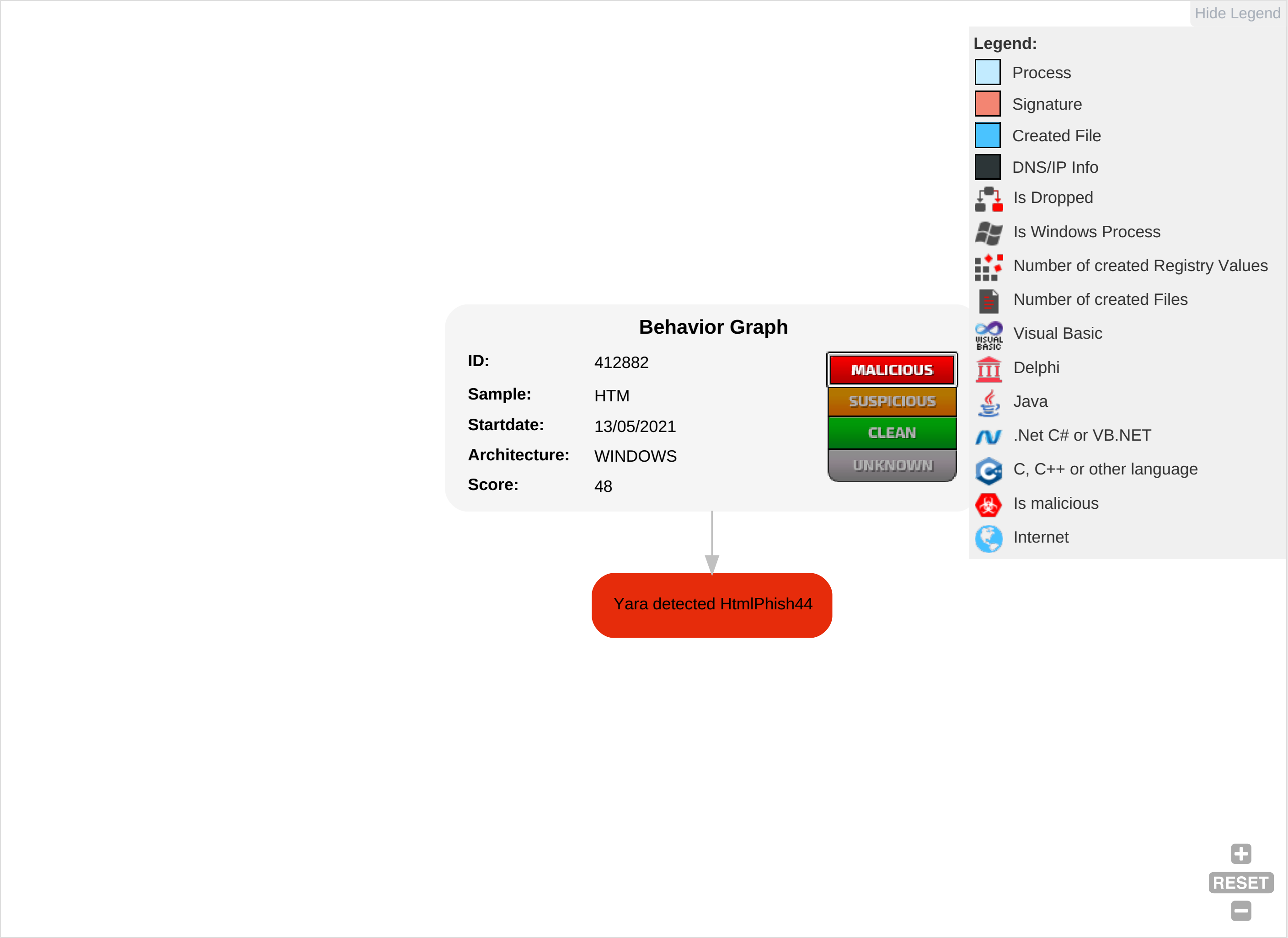
Phishing:

Yara detected HtmlPhish44

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

Behavior Graph



Behavior Graph

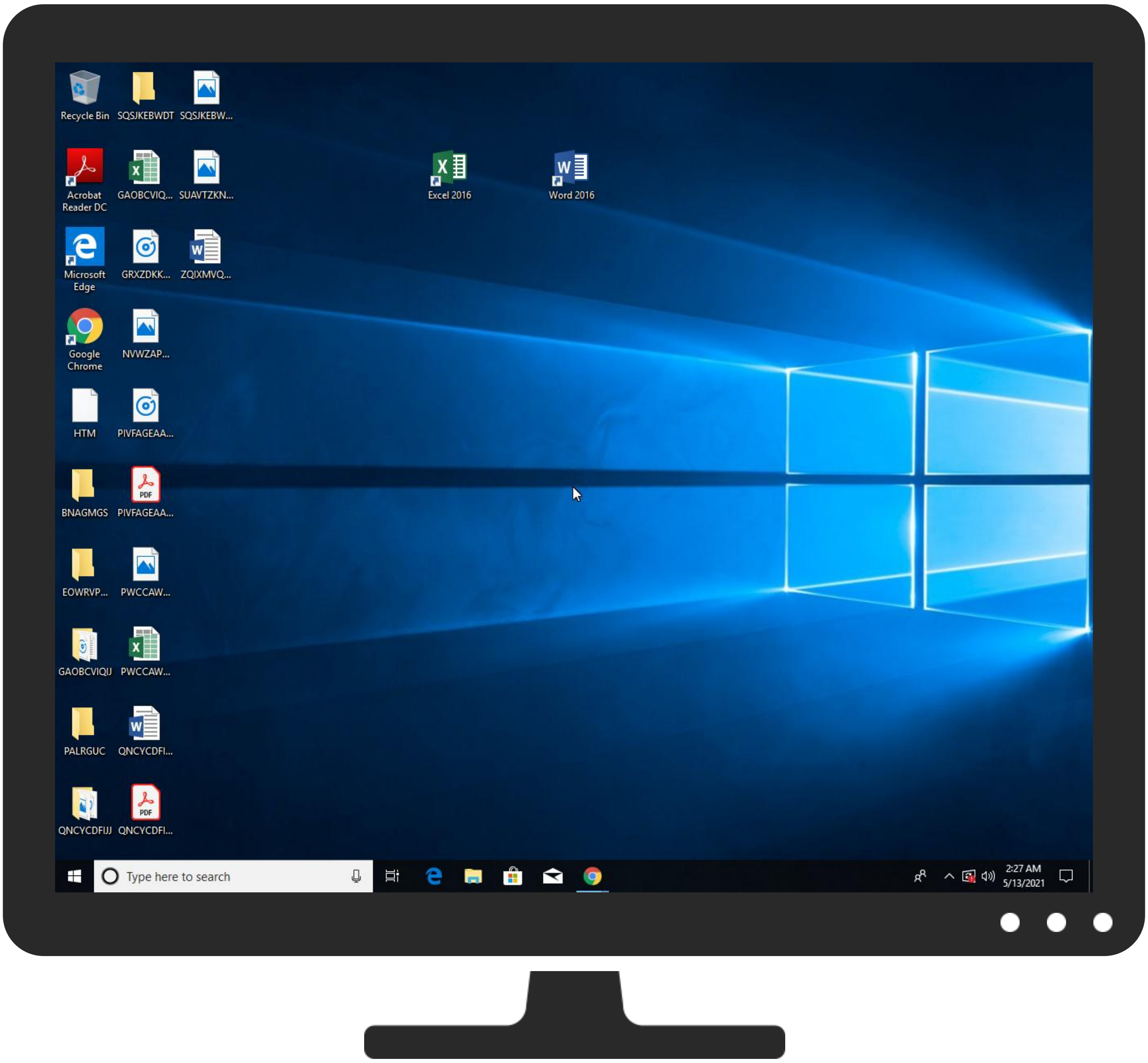
ID:	412882
Sample:	HTM
Startdate:	13/05/2021
Architecture:	WINDOWS
Score:	48

Yara detected HtmlPhish44

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

No Antivirus matches

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:	32.0.0 Black Diamond
Analysis ID:	412882
Start date:	13.05.2021
Start time:	02:26:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	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:	1
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:	mal48.phis.win@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to launch sample, stop analysis
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample • 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 no line terminators
Entropy (8bit):	3.6257304574553664
TrID:	
File name:	HTM
File size:	1551
MD5:	35962556551e113cc8fca2249f25ee29
SHA1:	413f182eed91659012d8f362454411850c4ceb6e
SHA256:	357915a1fd342de4b6350753eee9901eca9710b290bae6c129d0d188aea0c81f
SHA512:	6288301f76c6f858fc7047de4c5d9cf3b1c4af655a0362e72b458941fc9a4137c9bdb3776fbcc46fdb87210246f20effa52a3c5622c8f9af6ab77f82301d7797
SSDEEP:	24:SaX6N12tNQbH+yyA3/R8WkQ1sYSiYVdJDRcRA9C8ibMUk/zQs7Rb:SabtiTrh2NfpF9C1bEzQG9
File Content Preview:	<script language="javascript">document.write(unescape('%3C%21%44%4F%43%54%59%50%45%20%48%54%4D%4C%3E%0D%0A%3C%68%74%6D%6C%20%6C%61%6E%67%3D%22%65%6E%2D%55%53%22%3E%0D%0A%20%20%20%20%3C%68%65%61%64%3E%0D%0A%20%20%20%20%20%20%20%20%3C%73%63%72%69%70%74%20

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly