ID: 321435
Sample Name: CW-0282.COM
Cookbook: default.jbs
Time: 05:38:16
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

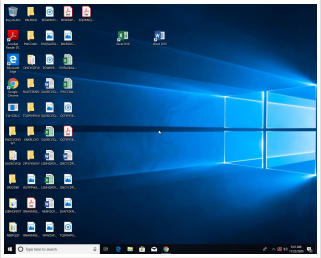
Analysis Report CW-0282.COM

Overview

General Information

Sample Name:	CW-0282.COM
Analysis ID:	321435
MD5:	2af23d7b372063c.
SHA1:	eabe88ad07af121.
SHA256:	781620cc0695cb...

Most interesting Screenshot:



Errors

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

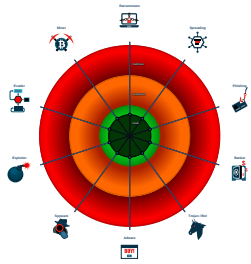
Detection

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

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

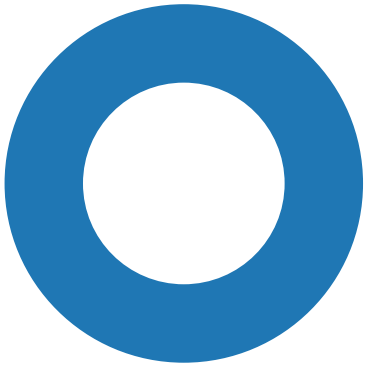
Yara Overview

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.

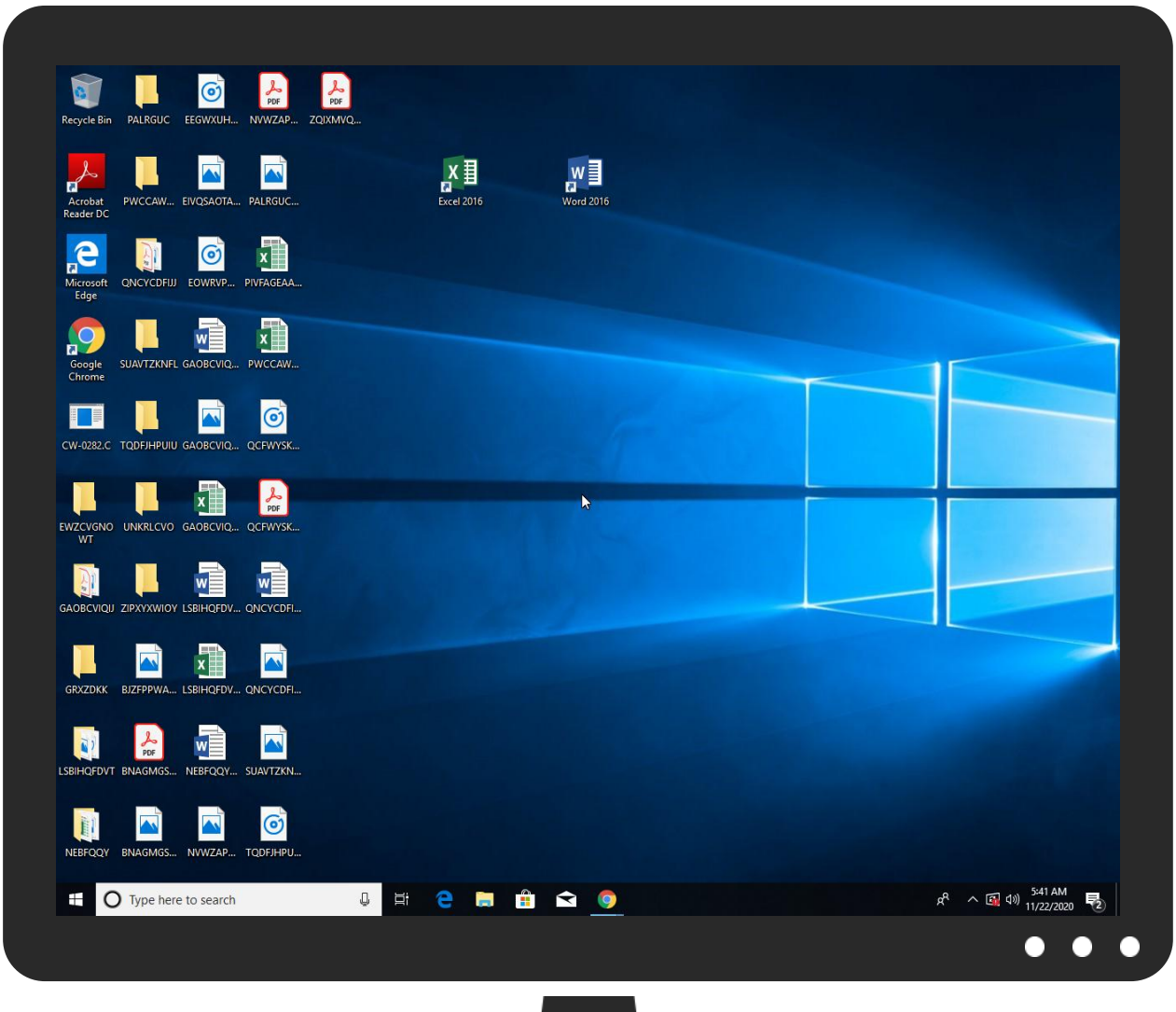
Mitre Att&ck Matrix

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
CW-0282.COM	0%	Virustotal		Browse
CW-0282.COM	0%	Metadefender		Browse
CW-0282.COM	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:	31.0.0 Red Diamond
Analysis ID:	321435
Start date:	22.11.2020
Start time:	05:38:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CW-0282.COM
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:	23
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.winCOM@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .COM
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, 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:	Non-ISO extended-ASCII text, with no line terminators
Entropy (8bit):	2.584962500721156
TrID:	
File name:	CW-0282.COM
File size:	6
MD5:	2af23d7b372063c74749151a76c29263
SHA1:	eabe88ad07af121c5c08df21f71b3812a5014bb0
SHA256:	781620cc0695cb5cc2bf360fb64d9a850edf15fc5e202119406dbe7e0a4db953
SHA512:	85c1eed2193e43bb3b9de85dd1beeb4c4ec329ae0a7eb98ed88fce54e0e00a0ab2dca53405f4108a8a9578cfe0adf3065e836c28168b68e12bbacbf8177f5722
SSDEEP:	3:mhtl:m7l
File Content Preview:	.. DH.

File Icon	
	
Icon Hash:	00828e8e8686b000

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly