ID: 326340
Sample Name:
phunipraaqnstgvldwkomzqrxoefymwylfgzscvkexbiujjdcbht
Cookbook: default.jbs
Time: 10:08:38
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report phunipraaqnstgvldwkomzqrxoefymwyl…

Overview

General Information

Sample Name:	phunipraaqnstgvldwkomzqrxoefymwylfgzscvkexbiujjdcbht
Analysis ID:	326340
MD5:	e242a78a55db0e..
SHA1:	db521a2ce8a341..
SHA256:	31421c4d9dd118..

Errors

- Nothing to analyse, Joe Sandbox has not found any analysis process or sample
- Corrupt sample or wrongly selected analyzer. Details: 80040153

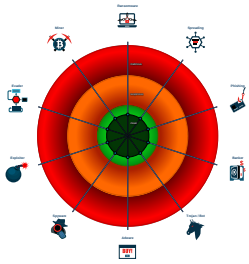
Detection

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

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

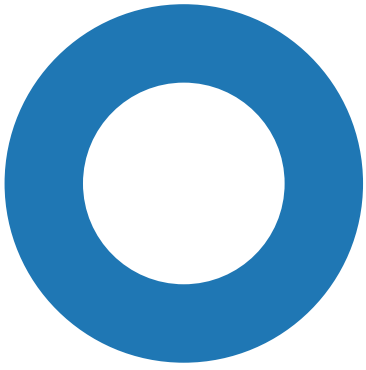
Yara Overview

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
phunipraaqnstgvldwkomzqrxoefymwylfgzscvkexbiujjdcbht	0%	Virustotal		Browse
phunipraaqnstgvldwkomzqrxoefymwylfgzscvkexbiujjdcbht	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:	326340
Start date:	03.12.2020
Start time:	10:08:38
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 1m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	phunipraaqnstgvldwkomzqrxoefymwylfgzscvkexbiujjdcbht
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.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:	data
Entropy (8bit):	7.1967074033599685
TrID:	
File name:	phunipraaqnstgvldwkomzqrxoefymwylfgzscvkexbiujjdcbht
File size:	102400
MD5:	e242a78a55db0eb31b1a99f9a3511a8a
SHA1:	db521a2ce8a34150d04f6c55626f27ac38a7d9c1
SHA256:	31421c4d9dd118ef671bc8a40b0d20cdb4e5c4529da4d53d7e4304b4122566eb
SHA512:	174310d792b1992abb817f7a78696984e14ff8cb842dc48533ef3187d754b7e44dc26c5b322ebc4e48bc3e5ea6f7b2ca069b29603ea98efb13f5e1c944a61234
SSDEEP:	3072:WMMMMMMMMMMMc8KkwVn0KR1hl/1f3e4Z0uPHos5LqMMMMMMMMMMMMMrMMMMMMMK:WMMMMMMMMMMMc87un0KHhlNe4vPHhxf
File Content Preview:	.0.IP3lePXti..5Q.VBvXlBZ.T5AVDh9Zl5TcCRWXm9OTG9eUWdZNUB9O01m.HVREG.Oc.[.t.u#.b8'.....)R.35a.0&.,,N.$D.L,k,,....G5.&.O=KoF15eWUBS..o2.IYW.J..cypCKkB1.ineZI^7a(0Ac.BaI0By.CfxXK9Kf.OeUG.Uef5ReUFkUFIqe1RAbVpHfF5vT.4MPGJWdTdqQ08.OG!XSXxWem$3LClsWV5B@XVBe3Axem0

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly