

JOeSandbox Cloud BASIC



ID: 339444

Sample Name:

#U5e94#U4ed8#U5e10#U5355.JS

Cookbook: default.jbs

Time: 03:52:54

Date: 14/01/2021

Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents	2
Analysis Report #U5e94#U4ed8#U5e10#U5355.JS	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Startup	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Network Behavior	8
Code Manipulations	9
Statistics	9
System Behavior	9
Analysis Process: wscript.exe PID: 6028 Parent PID: 5856	9
General	9
File Activities	9
Disassembly	9
Code Analysis	9
JavaScript Code	9
Call Graph	9
Script:	10
Code	10

Analysis Report #U5e94#U4ed8#U5e10#U5355.JS

Overview

General Information

Sample Name:

#U5e94#U4ed8#U5e10#U5355.JS

Analysis ID:

339444

MD5:

8928fc2990f2c4e...

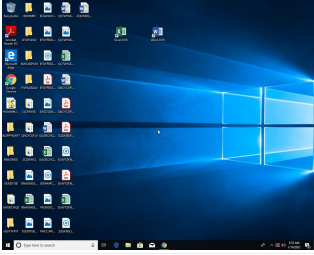
SHA1:

409182c8b6e8f83.

SHA256:

22ad37a20a155fd.

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

1

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

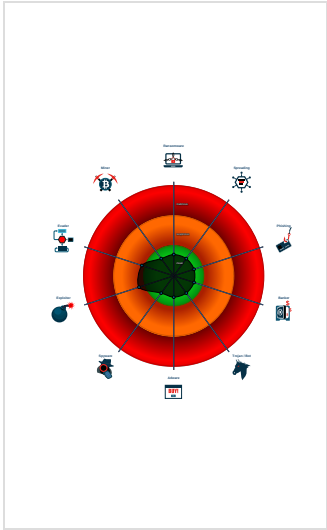
Signatures

Found WSH timer for Javascript or V...

Java / VBScript file with very long s...


Program does not show much activi...

Classification



Startup

System is w10x64

 wscript.exe (PID: 6028 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\Desktop\#U5e94#U4ed8#U5e10#U5355.JS' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)

cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection



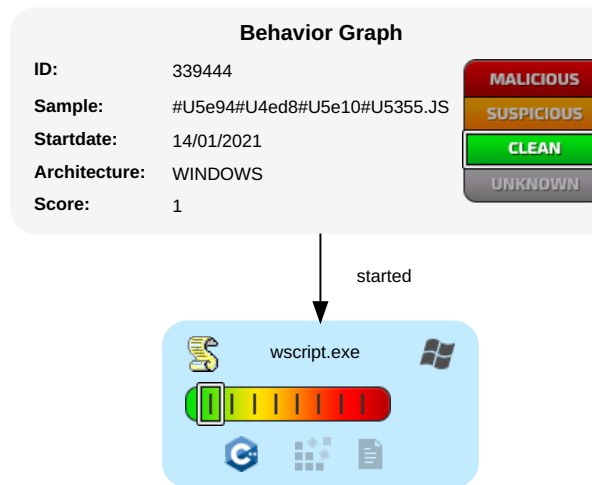
💡 Click to jump to signature section

There are no malicious signatures, [click here to show all signatures](#).

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 2	Path Interception	Path Interception	Scripting 2	OS Credential Dumping	System Information Discovery 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

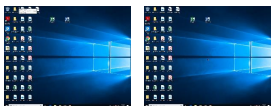
Behavior Graph



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
#U5e94#U4ed8#U5e10#U5355.JS	4%	Virustotal		Browse

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:	339444
Start date:	14.01.2021
Start time:	03:52:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U5e94#U4ed8#U5e10#U5355.JS
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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• GSI enabled (Javascript)• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winJS@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .JS• Stop behavior analysis, all processes terminated

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:	ISO-8859 text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.127302452418976
TrID:	
File name:	#U5e94#U4ed8#U5e10#U5355.JS
File size:	1832
MD5:	8928fc2990f2c4ecb3209c4281c68612
SHA1:	409182c8b6e8f83c4841473d8a31602493129da9
SHA256:	22ad37a20a155fd94df9ac2d68eb8099eb21d24c95689b7b6a2ff28c1b67765e
SHA512:	adfeded01713d7c483de7a33baa0d8f3217c156b8014194fad95ceb3f3a96f3b4fd1961b0b2c910650f49946f998f5df84334af6e661caefba719892f04e8c2e
SSDEEP:	48:iGEH+dEFhQbel30BTyrOk5/BWYgtvGOdCktpOCKCWWco:XEIGU3/gtvNP5
File Content Preview:	function pageInit(){... xRecordSet.New("cdsForm.cds_f p");.....ss="select *,ltrim(str(sjje,10,2)) as sjjea,ltrim(str(sj je/(1+yhsl/1000)*yhsl/1000,10,2)) as yhsea,ltrim(str(sjje/(1+yhsl/1000),10,2)) as wse,"...+" .. (select top 1 lxr fro m wlh where wlh.lib=

File Icon

	
Icon Hash:	e8d69ece968a9ec4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: wscript.exe PID: 6028 Parent PID: 5856

General

Start time:	03:53:41
Start date:	14/01/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\Desktop\#U5e94#U4ed8#U5e10#U5355.JS'
Imagebase:	0x7ff68f930000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

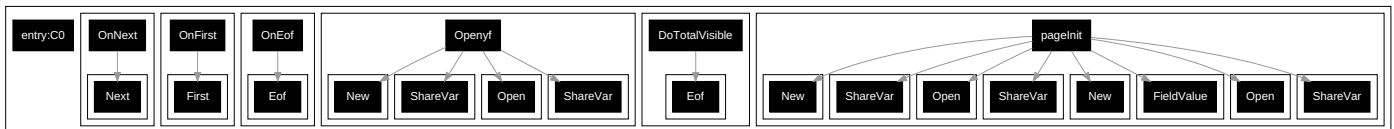
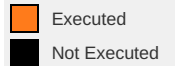
File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Disassembly

Code Analysis

JavaScript Code

Call Graph



Script:

Code

```

0  function pagelnit() {
1      xRecordSet.New ( "cdsForm.cds_fp" );
2      ss = "select *,ltrim(str(sjje,10,2)) as sjjea,ltrim(str(sjje/(1+yhsl/1000)*yhsl/1000,10,2)) as yhsea,ltrim(str(sjje/(1+yhsl/1000),10,2)) as wse," + " (select top 1 lxr from wlh where wlh.lb=cmhctdyffpwlh.lb and wlh.dm=cmhctdyffpwlh.dm) as attn," + " (select top 1 tdh from tddl where tddl.ztddid=cmhctdyffpwlh.tdid) as tdha," + " (case when (mdd is null or mdd='') then (case when (jhdd is null or jhdd = '' ) then xhg else jhdd end) else mdd end) as xhga " + " from cmhctdyffpwlh" + " where fpid=" + xScript.ShareVar ( "fpid" );
3      xRecordSet.Open ( "cdsForm.cds_fp", xScript.ShareVar ( "dbname" ), "", ss );
4      xRecordSet.New ( "cdsForm.cds_td" );
5      ss = "gettdxcxs " + xRecordSet.FieldValue ( "cdsForm.cds_fp.tdid" );
6      xRecordSet.Open ( "cdsForm.cds_td", xScript.ShareVar ( "dbname" ), "", ss );
7  }
8  function DoTotalVisible() {
9      if ( xRecordSet.Eof ( "cdsForm.cds_fp" ) == 1 )
10         return "true";
11     else
12         return "false";
13 }
14 function Openyf() {
15     xRecordSet.New ( "cdsForm.cds_yf" );
16     ss = "select yf.*, (case when ((fymc in (select fymc from fydm)) and ((select top 1 fjmc from fydm where fydm.fymc=yf.fymc) != '')) then (select top 1 fjmc from fydm where fydm.fymc=yf.fymc) else fymc end) as fjmc,ltrim(str((yf.jg*(case when yf.ysyf='x04e6lxffdxfffd' then 1 else -1 end)),12,2)) as jga,ltrim(str((yf.sjje*(case when yf.ysyf='x04e6lxffdxfffd' then 1 else -1 end)),12,2)) as sjjea from yf where (fpid=" + xScript.ShareVar ( "fpid" ) + " );";
17     xRecordSet.Open ( "cdsForm.cds_yf", xScript.ShareVar ( "dbname" ), "", ss );
18 }
19 function OnEof(tablename) {
20     return xRecordSet.Eof ( "cdsForm.cds_" + tablename );
21 }
22 function OnFirst(tablename) {
23     xRecordSet.First ( "cdsForm.cds_" + tablename );
24 }
25 function OnNext(tablename) {
26     xRecordSet.Next ( "cdsForm.cds_" + tablename );
27 }

```