

JoeSandbox Cloud BASIC



ID: 632579

Sample Name: Scan 4405.vbs

Cookbook: default.jbs

Time: 19:40:23

Date: 23/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

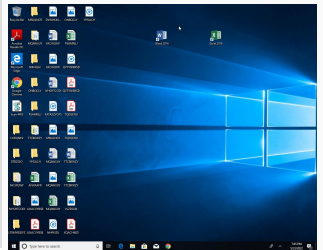
Table of Contents	2
Windows Analysis Report Scan 4405.vbs	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Initial Sample	3
Sigma Signatures	3
Snort Signatures	4
Joe Sandbox Signatures	4
System Summary	4
Anti Debugging	4
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
World Map of Contacted IPs	7
General Information	7
Warnings	7
Simulations	7
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Network Behavior	9
Statistics	9
System Behavior	9
Analysis Process: wscript.exePID: 6384, Parent PID: 3688	9
General	9
File Activities	9
Disassembly	9

Windows Analysis Report

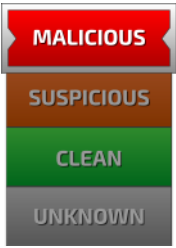
Scan 4405.vbs

Overview

General Information

Sample Name:	Scan 4405.vbs
Analysis ID:	632579
MD5:	5e8adfec0bdc8...
SHA1:	bd6dad1a8d3335.
SHA256:	ab87133662dddf..
Tags:	vbs
Infos:	Yara
	

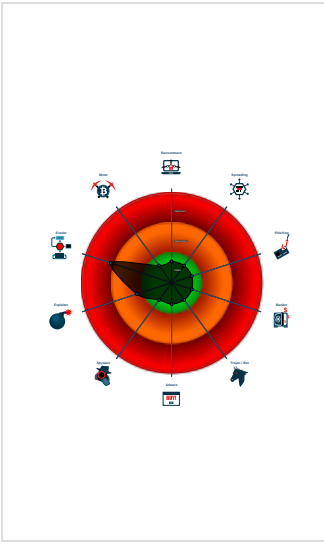
Detection

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


Signatures

Found potential dummy code loops ...
Potential malicious VBS script foun...
Yara signature match
Java / VBScript file with very long s...
Monitors certain registry keys / valu...
Program does not show much activi...
Found WSH timer for Javascript or V...
Abnormal high CPU Usage

Classification



Process Tree

- System is w10x64
-  wscript.exe (PID: 6384 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Scan 4405.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Scan 4405.vbs	WScript_Shell_PowerShell_Comb	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth	<ul style="list-style-type: none">0x17e0b:\$s1: .CreateObject("WScript.Shell")0x17fa7:\$p1: powershell.exe

Sigma Signatures

No Sigma rule has matched

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

System Summary











Potential malicious VBS script found (suspicious strings)

Anti Debugging

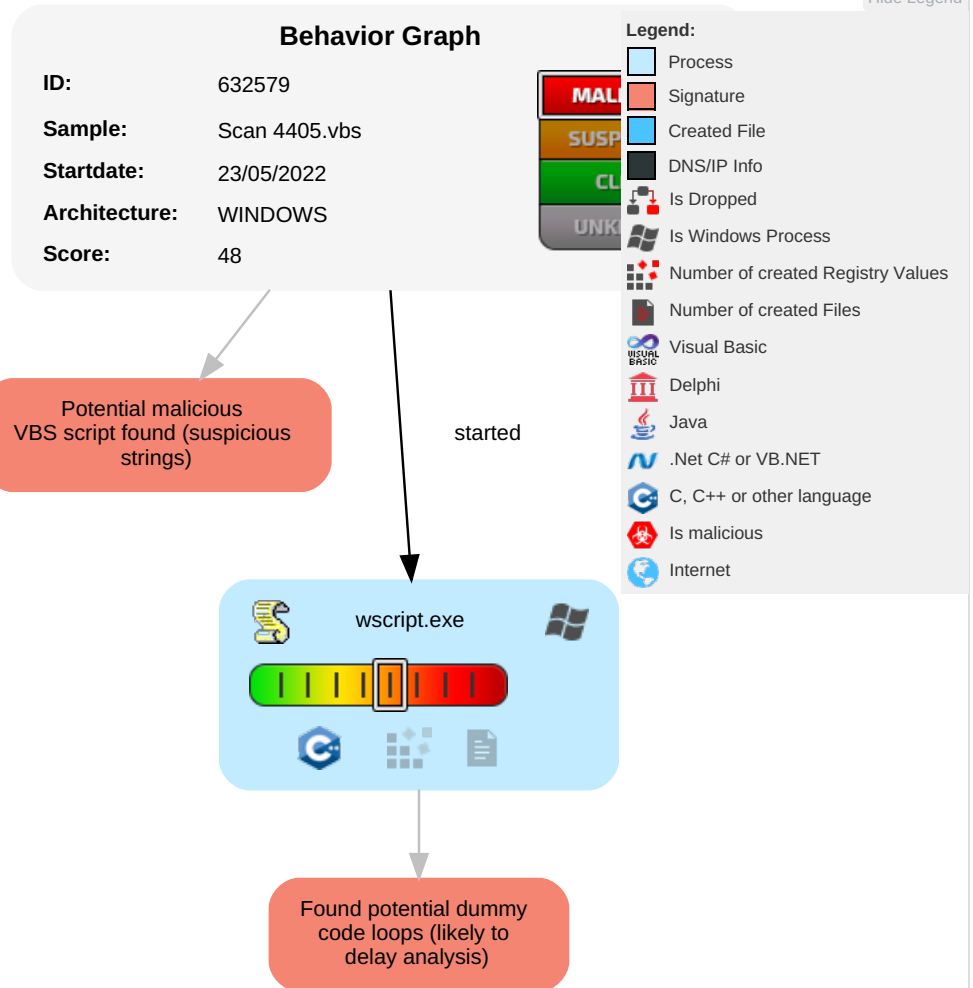


Found potential dummy code loops (likely to delay analysis)

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	Path Interception	Path Interception	 Virtualization/Sandbox Evasion	OS Credential Dumping	 Security Software Discovery	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	 Scripting	LSASS Memory	 Query Registry	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	 Obfuscated Files or Information	Security Account Manager	 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

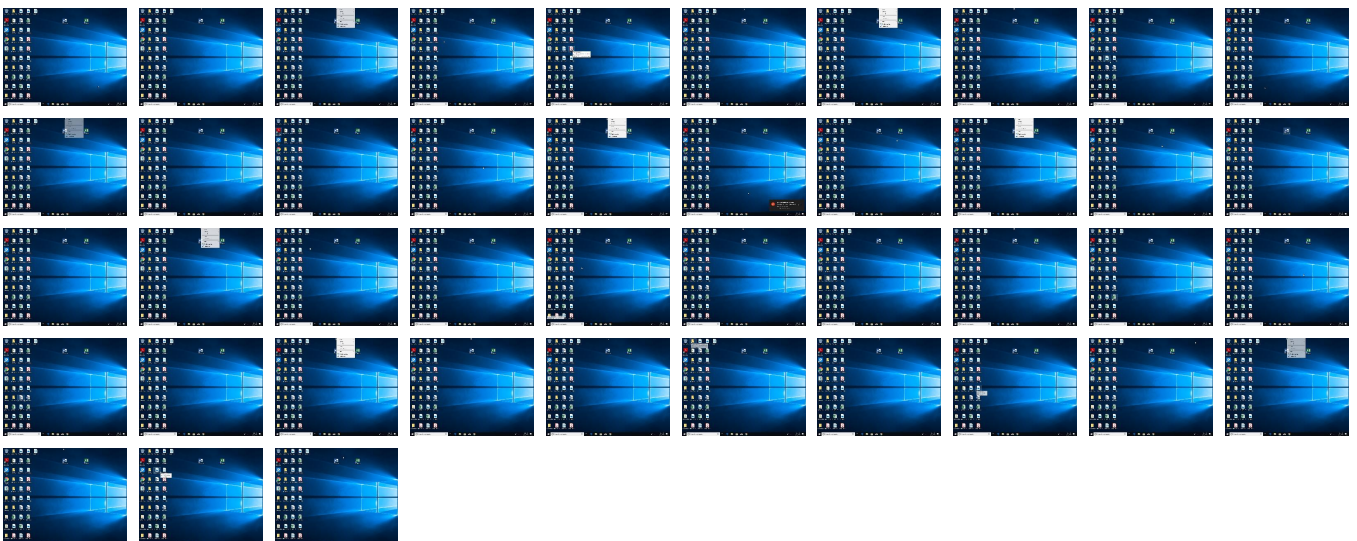
Behavior Graph



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
Scan 4405.vbs	5%	Virustotal		Browse
Scan 4405.vbs	2%	ReversingLabs	Win32.Trojan.Generic	

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

World Map of Contacted IPs

 No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632579
Start date and time: 23/05/202219:40:23	2022-05-23 19:40:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scan 4405.vbs
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:	21
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• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.evad.winVBS@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">• Found application associated with file extension: .vbs• Adjust boot time• Enable AMSI• Override analysis time to 240s for JS files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.213.168.66, 51.104.136.2, 51.11.168.232
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, settings-prod-neu-2.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, settings-prod-uks-1.uksouth.cloudapp.azure.com, prod.fs.microsoft.com.akadns.net, atm-settingsfe-prod-geo.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files


No created / dropped files found

Static File Info

General


File type:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.680075831434168
TrID:	<ul style="list-style-type: none">Visual Basic Script (13500/0) 100.00%
File name:	Scan 4405.vbs
File size:	98906
MD5:	5e8adfecabdc8322938f25e46efa629
SHA1:	bd6dad1a8d3335216e53217773b798c553cdfae1
SHA256:	ab87133662dddfbede53d3bbb558cb5f0720ffdd42136358c1a30f1d9919aba7
SHA512:	f0b733424fd4e3ceb971c46280ac54a32f0e4180f84c61c8c07e623eeae83ad86971384ac97fd95e8172c2e2aba87cc0c7a20f937f5079d5371a72666e9acd72
SSDEEP:	1536:hxs1Mwn50M7Sp5riTA4455Ib0BDKAhhIO7M5j3CCj41Rf58IKiAQIBq9:lpCXp4C5IQN5hOO7M5DK1Rf5JKLQIk9
TLSH:	A5A3709CA7D2DDBB66C4CB647DAF4B035D4694E198FE01F7244A28D6A41C7F08E2E803
File Content Preview:	'Skyldfr Medal Finan Westerl FURUNCLESK MICRON DISPOSSE noncan LIZARYOCTA Mjvdefens Monitering Misalp eksku Pelsvrker ..'UNENTHUSED lyophobic Ozonl Tortonian3 datas Bugtnin Tabskont coronet Trowelerha Retina5 NODDYEK maks CRINALWI tachylyti Piet Undef4

File Icon



Icon Hash: e8d69ece869a9ec4

Network Behavior

 No network behavior found

Statistics

 No statistics

System Behavior

Analysis Process: wscript.exe PID: 6384, Parent PID: 3688

General

Target ID:	0
Start time:	19:41:38
Start date:	23/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Scan 4405.vbs"
Imagebase:	0x7ff7db660000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Disassembly

 No disassembly