ID: 632579
Sample Name: Scan 4405.vbs
Cookbook: default.jbs
Time: 20:29:09
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

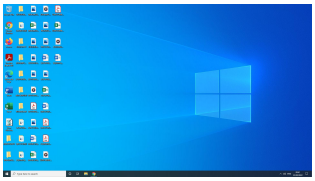
Windows Analysis Report

Scan 4405.vbs

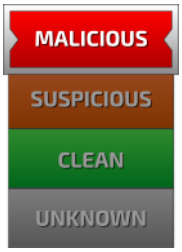
Overview

General Information

Sample Name:	Scan 4405.vbs
Analysis ID:	632579
MD5:	5e8adfeca0bdc8…
SHA1:	bd6dad1a8d3335.
SHA256:	ab87133662dddf..
Infos:	YARA



Detection

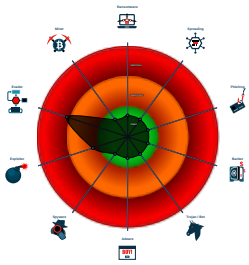


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found potential dummy code loops …
- Potential malicious VBS script foun…
- Yara signature match
- Java / VBScript file with very long s…
- Tries to load missing DLLs
- Program does not show much activi…
- Found WSH timer for Javascript or V…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 8880 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Scan 4405.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Scan 4405.vbs	WScript_Shell_PowerShell_Combo	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth	• 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)

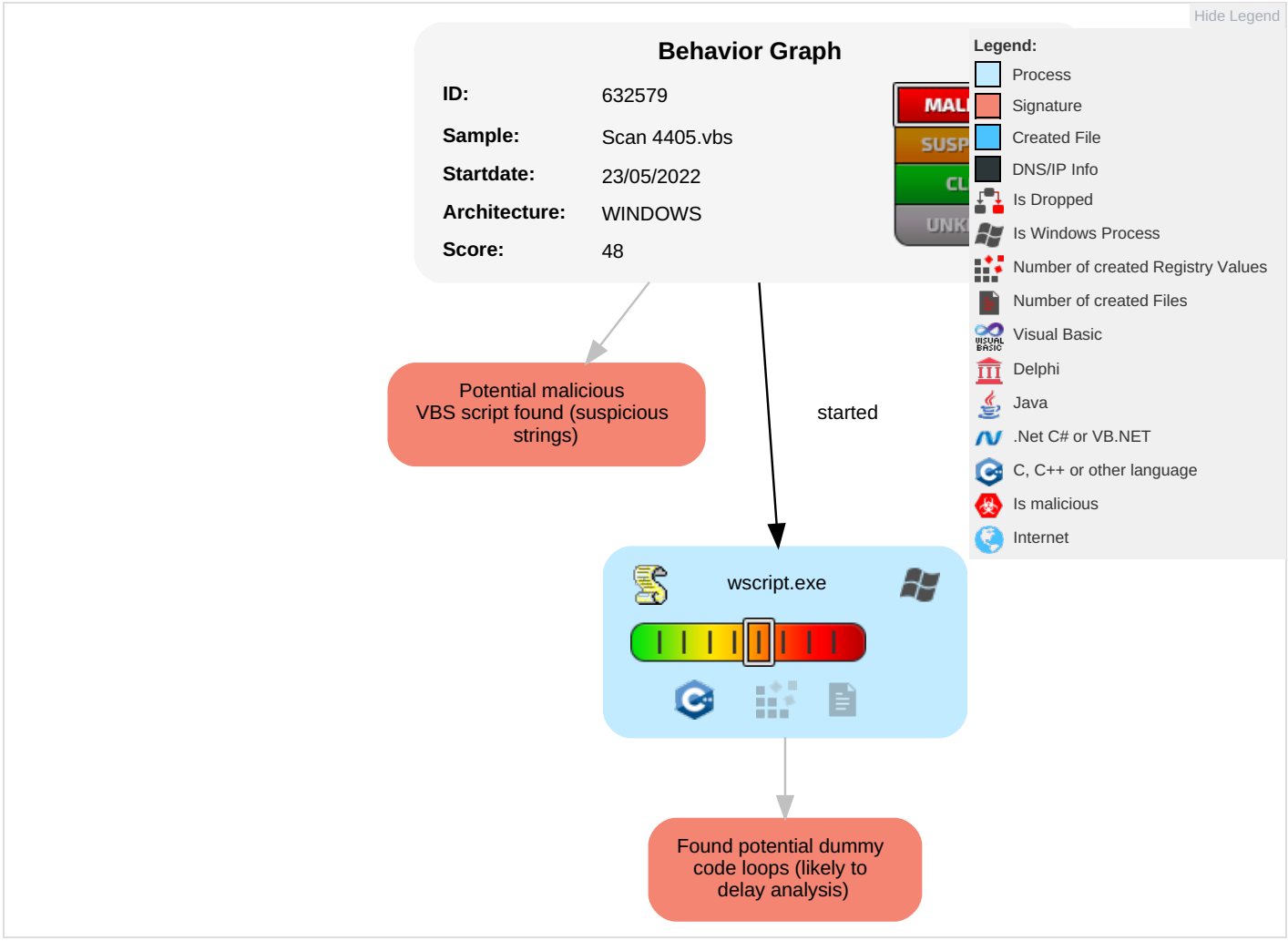
Anti Debugging

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	1 2 1 Scripting	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 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	1 2 1 Scripting	LSASS Memory	1 1 Virtualization/Sandbox Evasion	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)	1 DLL Side-Loading	Security Account Manager	2 System Information Discovery	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)	1 Obfuscated Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

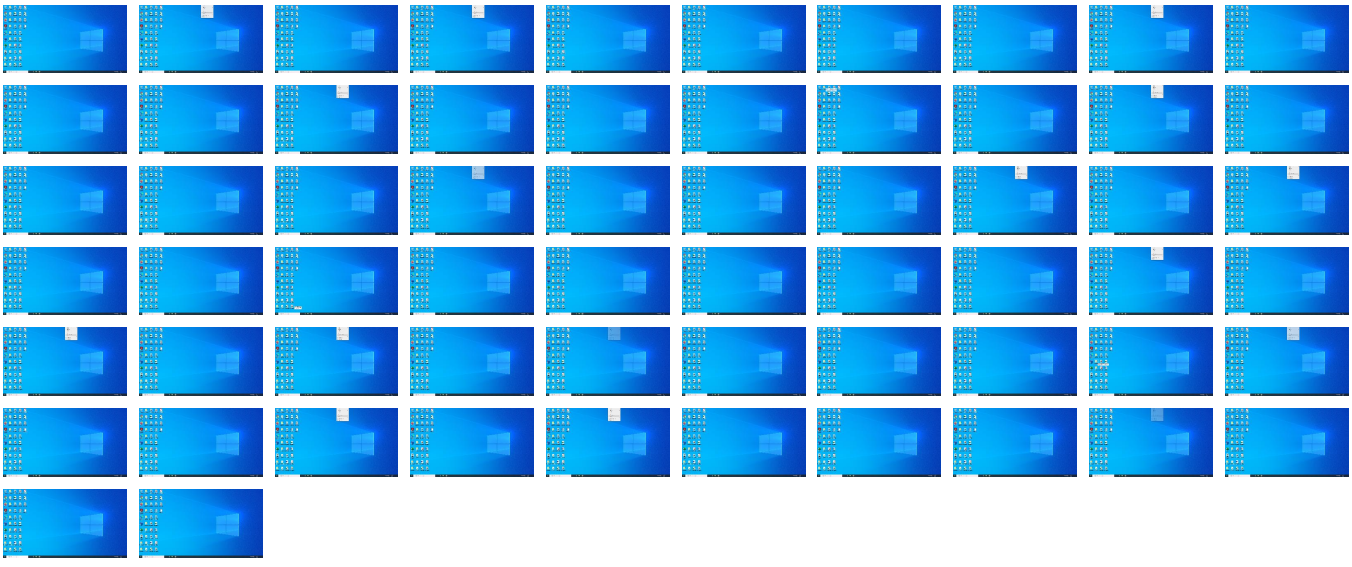
Behavior Graph



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

Source	Detection	Scanner	Label	Link
dual-a-0001.dc-msedge.net	0%	Virustotal		Browse
e-0009.e-msedge.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dual-a-0001.dc-msedge.net	13.107.22.200	true	false	• 0%, Virustotal, Browse	unknown
e-0009.e-msedge.net	13.107.5.88	true	false	• 0%, Virustotal, Browse	unknown

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: 23/05/202220:29:09	2022-05-23 20:29:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 7s
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 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	29
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.evad.winVBS@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MusNotification.exe, dllhost.exe, RuntimeBroker.exe, SIHClient.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, MusNotificationUx.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.117.96.136, 20.54.122.82, 20.82.207.122
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, slscr.update.microsoft.com, wd-prod-cp-eu-north-2-fe.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, ris.api.iris.microsoft.com, wd-prod-cp-eu-north-1-fe.northeurope.cloudapp.azure.com, wdcpalt.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, login.live.com, apimgmttmr17ij3jt5dneg64srod9jevcuajxaoube4brtu9cq.trafficmanager.net, evoke-windowsservices-tas.msedge.net, apimgmthszbjimgeglorvthkncixvpso9vnynvh3ehmsdll33a.cloudapp.net, img-prod-cms-rt-microsoft-com.akamaized.net, nexusrules.officeapps.live.com, manage.devcenter.microsoft.com

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:	• Visual Basic Script (13500/0) 100.00%
File name:	Scan 4405.vbs
File size:	98906
MD5:	5e8adfeca0bdc8322938f25e46efa629
SHA1:	bd6dad1a8d3335216e53217773b798c553cdfae1
SHA256:	ab87133662dddfbede53d3bbb558cb5f0720ffdd42136358c1a30f1d9919aba7
SHA512:	f0b733424fd4e3ceb971c46280ac54a32f0e4180f84c61c8c07e623eeae83ad86971384ac97fd95e8172c2e2aba87cc0c7a20f937f5079d5371a72666e9acd72
SSDEEP:	1536:hxs1Mwn50M7Sp5riTA4455Ib0BDKAhhIO7M5j3CCj41Rf58IKiAQIBq9:IpCXp4C5IQN5hOO7M5DK1Rf5JKLQIk9
TLSH:	A5A3709CA7D2DDBB66C4CB647DAF4B035D4694E198FE01F7244A28D6A41C7F08E2E803
File Content Preview:	'Skyldfr Medal Finan Westerl FURUNCLESK MICRON DISPOSSE noncan LIZARYOCTA Mjavdefens Monitering Misalp eksklu Pelsvrker ..'UNENTHUSED lyophobic Ozonl Tortonian3 datas Bugtnin Tabskont coronet Trowelerha Retina5 NODDYEK maksi 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: 8880, Parent PID: 4772

General

Target ID:	0
Start time:	20:33:28
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:	0x7ff7387f0000
File size:	170496 bytes
MD5 hash:	0639B0A6F69B3265C1E42227D650B7D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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