ID: 679318
Sample Name: qwgrp.js
Cookbook: default.jbs
Time: 15:21:10
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

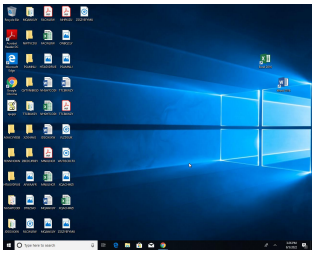
Windows Analysis Report

qwgrp.js

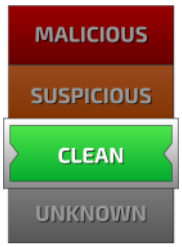
Overview

General Information

Sample Name:	qwgrp.js
Analysis ID:	679318
MD5:	5eeaaf798aff432..
SHA1:	a161f51b686662..
SHA256:	8fae44f0db835c7..
Tags:	apt DangerousPassword js Lazarus



Detection

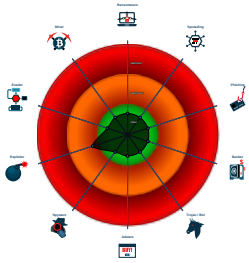


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Program does not show much activi…
- Java / VBScript file with very long s…
- Found WSH timer for Javascript or V…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5440 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\qwgrp.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

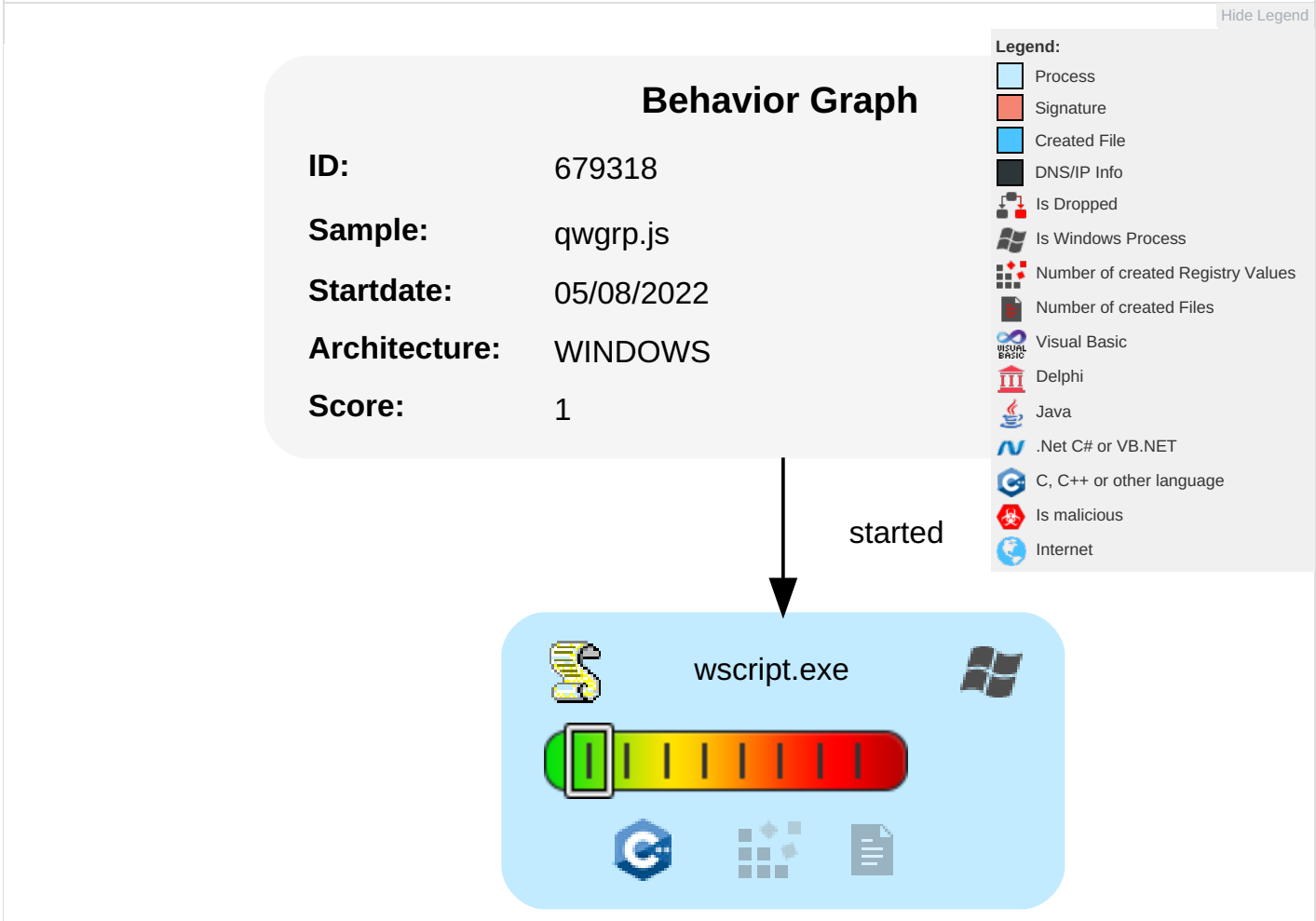
Joe Sandbox Signatures

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	2 Scripting	Path Interception	Path Interception	2 Scripting	OS Credential Dumping	2 System Information 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 Obfuscated Files or Information	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

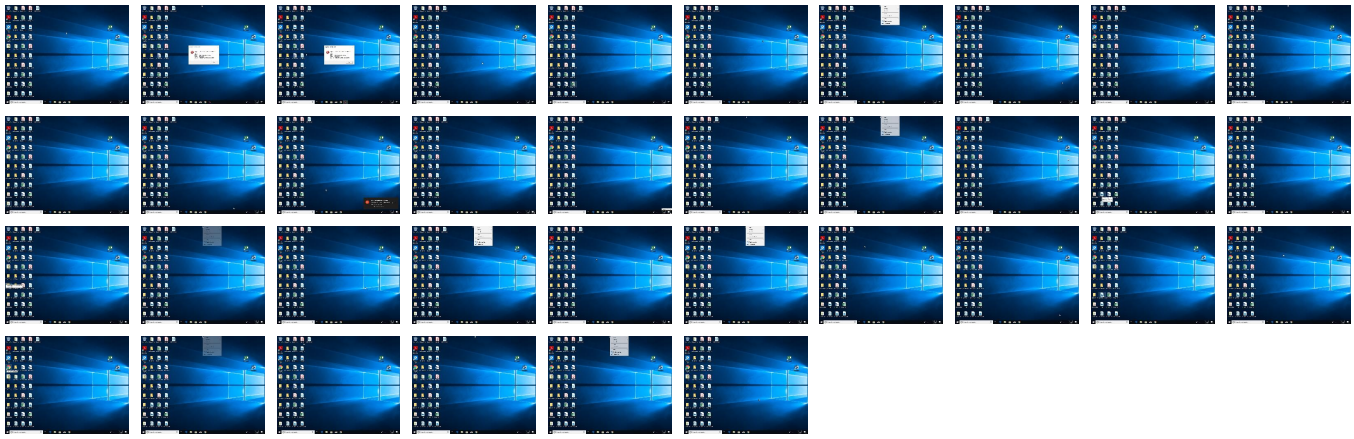
Behavior Graph



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
qwgrp.js	5%	Virustotal		Browse
qwgrp.js	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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679318
Start date and time: 05/08/202215:21:10	2022-08-05 15:21:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qwgrp.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:	22
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:	CLEAN
Classification:	clean1.winJS@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: .js • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, licensing.mp.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.

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:	Little-endian UTF-16 Unicode text, with very long lines, with CR line terminators

Entropy (8bit):	3.4267066166756632
TrID:	• Text - UTF-16 (LE) encoded (2002/1) 64.44% • MP3 audio (1001/1) 32.22% • Lumena CEL bitmap (63/63) 2.03% • Corel Photo Paint (41/41) 1.32%
File name:	qwgrp.js
File size:	3194
MD5:	5eeaaf798aff4328ae6afdffc28546bd
SHA1:	a161f51b686662e887b83cf8b2b0ea31e102d76f
SHA256:	8fae44f0db835c7ced4cddafcf64b8221822ae0384a8575911f84b98f9bf7dc3
SHA512:	af53659dcd8d6ce2d7e742d14a2902c341ebc0e56b07a160556fdf0064c16ef891bad11f27b565ddbe41aec2111ad97c83337962fbb318f4c9dc5fc88a4a27da
SSDEEP:	48:X3RlBbtu6apcfxNJ0lrd+1YKSWMjaBdIf7cUo50r0FZhoN1H+:XBkRpcpNerU1YXWwoIf7to//KH+
TLSH:	4A61AC383AD3331A7FBA9A00C9F20613B1373643BA11960CC4AE2B0D4A2373558E6E1D
File Content Preview:	..v.a.r. .h.\.u.0.0.7.3.=.W.S.c.\.u.0.0.7.2.\.u.0.0.6.9.\.u.0.0.7.0.\.u.0.0.7.4...a.r.g.\.u.0.0.7.5.\.u.0.0.6.d.\.u.0.0.6.5.n.t.\.u.0.0.7.3.(.0.).;.v.a.r. .m.\.u.0.0.6.d.=.".M.S.X.M.L.";.v.a.r. .s.=.".a.";.v.a.r. .m.t.=.".2.\.u.0.0.2.e.S.e.r.v.e.\.x.7.2

File Icon

Icon Hash:	e8d69ece968a9ec4

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: wscript.exe PID: **5440**, Parent PID: **684**

General

Target ID:	0
Start time:	15:22:21
Start date:	05/08/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\qwgrp.js"
Imagebase:	0x7ff7eccb0000
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly