ID: 532182
Sample Name: QVWb1n5OTH
Cookbook: default.jbs
Time: 20:08:18
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

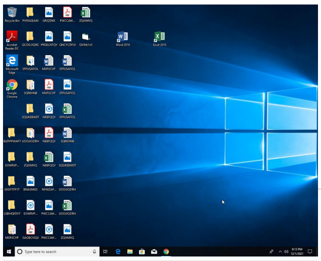
Windows Analysis Report QVWb1n5OTH

Overview

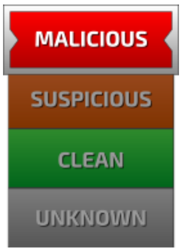
General Information

Sample Name:	QVWb1n5OTH (renamed file extension from none to exe)
Analysis ID:	532182
MD5:	f8236209c7b1928.
SHA1:	7f31471385b3972.
SHA256:	eab40778e702a8..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

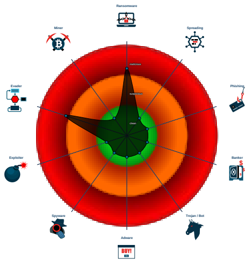


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Found potential dummy code loops (…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function
- PE / OLE file has an invalid certificate
- Program does not show much activi…
- Contains functionality for execution …
- Abnormal high CPU Usage

Classification



Process Tree

- System is w10x64
- QVWb1n5OTH.exe (PID: 6168 cmdline: "C:\Users\user\Desktop\QVWb1n5OTH.exe" MD5: F8236209C7B1928B3F1EB0A7074F6992)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Potential malicious icon found

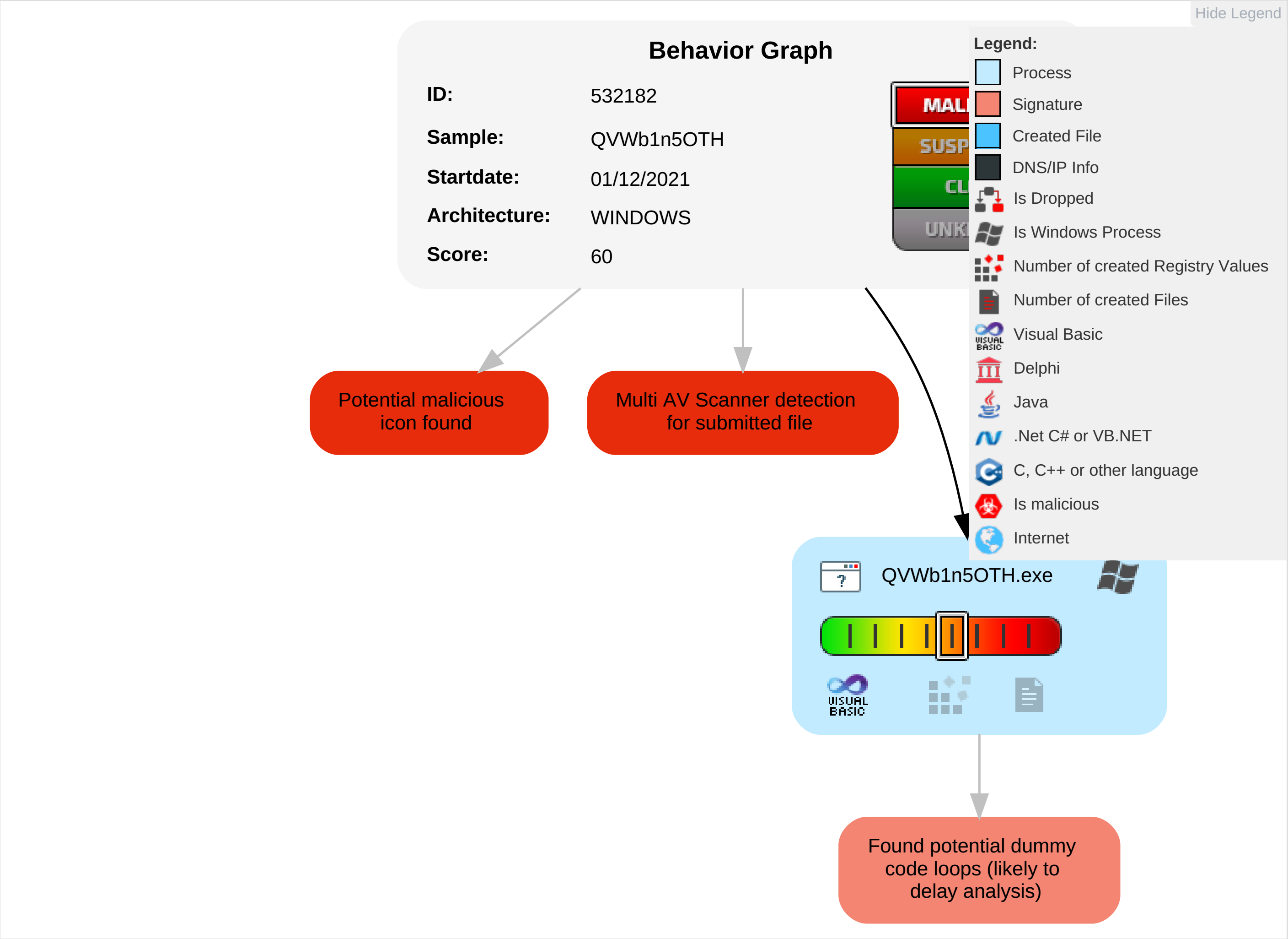
Anti Debugging:

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	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



Hide Legend

Behavior Graph

ID:	532182
Sample:	QVWb1n5OTH
Startdate:	01/12/2021
Architecture:	WINDOWS
Score:	60

Legend:

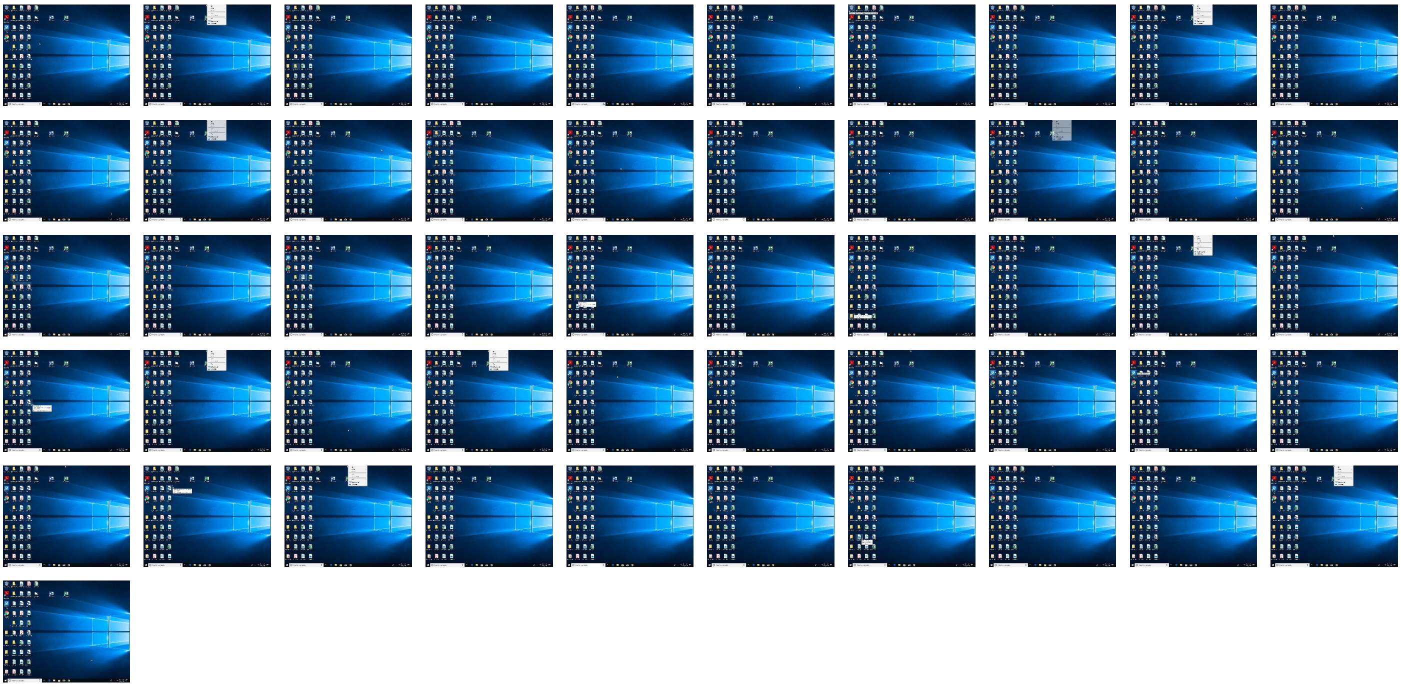
- 🟦 Process
- 🟥 Signature
- 🟦 Created File
- ■ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

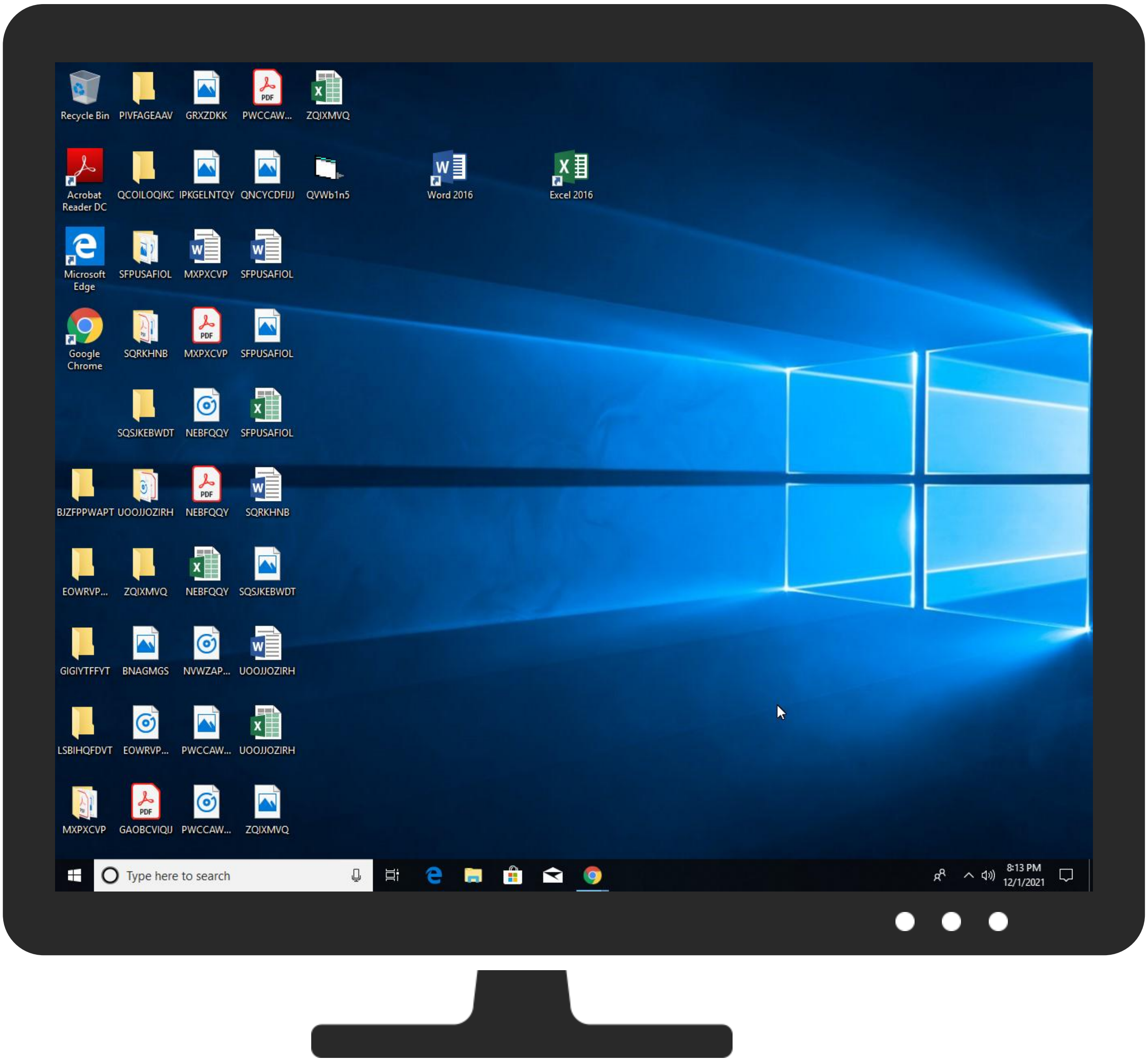
MALI
SUSP
CL
UNK
Potential malicious icon found
Multi AV Scanner detection for submitted file
QVWb1n5OTH.exe
VISUAL BASIC
Found potential dummy code loops (likely to delay analysis)

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
QVWb1n5OTH.exe	60%	Virustotal		Browse
QVWb1n5OTH.exe	29%	Metadefender		Browse
QVWb1n5OTH.exe	49%	ReversingLabs	Win32.Trojan.AgentTesla	

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:	34.0.0 Boulder Opal
Analysis ID:	532182
Start date:	01.12.2021
Start time:	20:08:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QVWb1n5OTH (renamed file extension from none to exe)
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:	16
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:	mal60.rans.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.8% (good quality ratio 15.4%) • Quality average: 29.9% • Quality standard deviation: 26.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

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:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.226986072662153
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	QVWb1n5OTH.exe
File size:	152872
MD5:	f8236209c7b1928b3f1eb0a7074f6992
SHA1:	7f31471385b39722a1c7a6e983ecca372e673796
SHA256:	eab40778e702a859cc33abcd92e796755e95e8fdb0eeb7 c5243b7c1866751bb0
SHA512:	b0619a562d6ed00016ef3c3e3fcbbe917718c770d51db0f ae31f9bd47f05e41bc312197a906b32988a7ad8c50deda4 2c29b150954d3b195d024f2510c7cd2440
SSDEEP:	1536:Lf2yGzzFNaIEP6BWYRVpcjK+zDU1BljlR76UMLV NNdsBkz3hay:yyGzz/aIu6BJRVvBkUMLp62Iy
File Content Preview:	MZ......................@..!..L.!Th is program cannot be run in DOS mode....$........,..SM..S M..SM...Q..RM...o..UM..ek..RM..RichSM..................PE.. L....(!W.....................0......x.............@........

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401578

General

Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x572128D8 [Wed Apr 27 21:02:16 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e6bbebdc7c1418bc1bcdb0dc8a54e696

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Squar5@SPRINDG.Suf, CN=RDDEL, OU=OCTAG, O=PROCOELI, L=GENGAN, S=Ogti8, C=PL
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/24/2021 3:10:46 AM 11/24/2022 3:10:46 AM
Subject Chain	• E=Squar5@SPRINDG.Suf, CN=RDDEL, OU=OCTAG, O=PROCOELI, L=GENGAN, S=Ogti8, C=PL
Version:	3
Thumbprint MD5:	649E58058CF32102CC914157E8C1F36A
Thumbprint SHA-1:	72EE3E0C954978F2C86A7F3128298893C8A634C1
Thumbprint SHA-256:	22458793AFD4DB1F57B56ECFA277B0F70C8C8908C9FD60A56D8D61FD3AB3C819
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1fa84	0x20000	False	0.471748352051	data	6.40978274126	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x21000	0xc24	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x11d2	0x2000	False	0.188354492188	data	2.35778198706	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: QVWb1n5OTH.exe PID: 6168 Parent PID: 2856

General

Start time:	20:09:15
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\QVWb1n5OTH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\QVWb1n5OTH.exe"
Imagebase:	0x400000
File size:	152872 bytes
MD5 hash:	F8236209C7B1928B3F1EB0A7074F6992
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal