ID: 451510
Sample Name: 8rbuJ8Ycv1
Cookbook: default.jbs
Time: 18:23:55
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

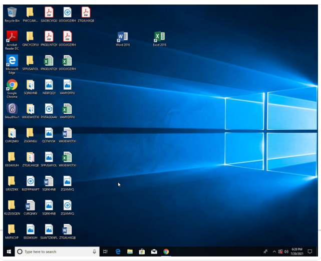
Windows Analysis Report 8rbuJ8Ycv1

Overview

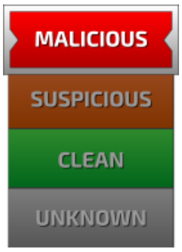
General Information

Sample Name:	8rbuJ8Ycv1 (renamed file extension from none to exe)
Analysis ID:	451510
MD5:	546f9c26cb739f1..
SHA1:	452ee936bbade0..
SHA256:	6bd6a8e685288c..
Infos:	🔍 ⚙

Most interesting Screenshot:



Detection

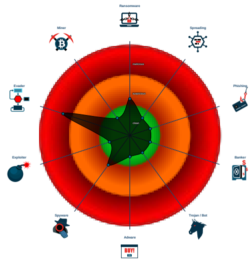


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to query CPU …
- Contains functionality to read the PEB
- Detected potential crypto function
- Found large amount of non-executed…
- PE file contains strange resources
- Program does not show much activi

Classification



Process Tree

- **System is w10x64**
- 8rbuJ8Ycv1.exe (PID: 6936 cmdline: 'C:\Users\user\Desktop\8rbuJ8Ycv1.exe' MD5: 546F9C26CB739F1E3EA5BA1605AA7328)
- **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

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Tries to detect virtualization through RDTSC time measurements

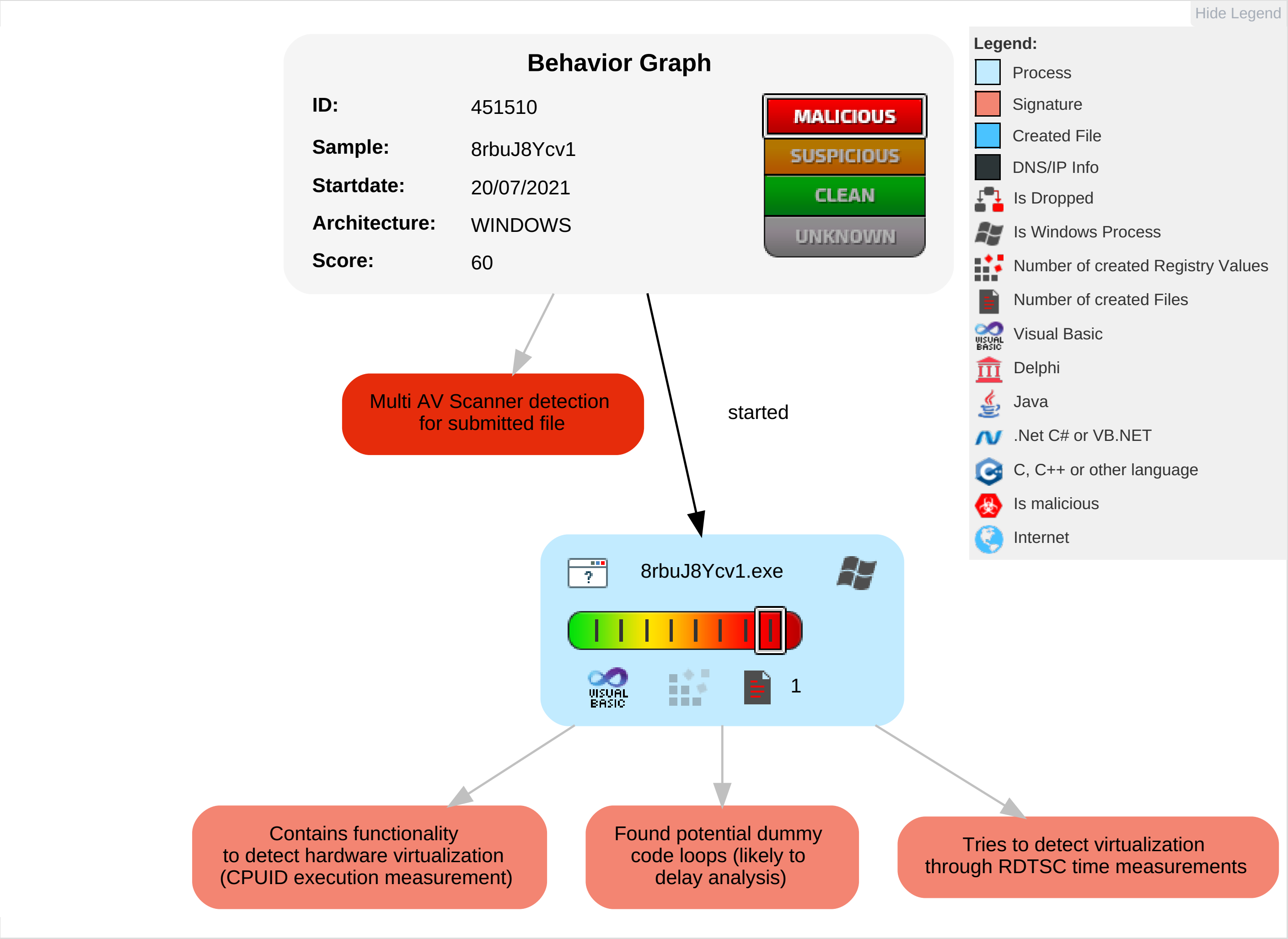
Anti Debugging:

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 3 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 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



Hide Legend

Behavior Graph

ID: 451510

Sample: 8rbuJ8Ycv1

Startdate: 20/07/2021

Architecture: WINDOWS

Score: 60

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Multi AV Scanner detection for submitted file
started
8rbuJ8Ycv1.exe
1
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements

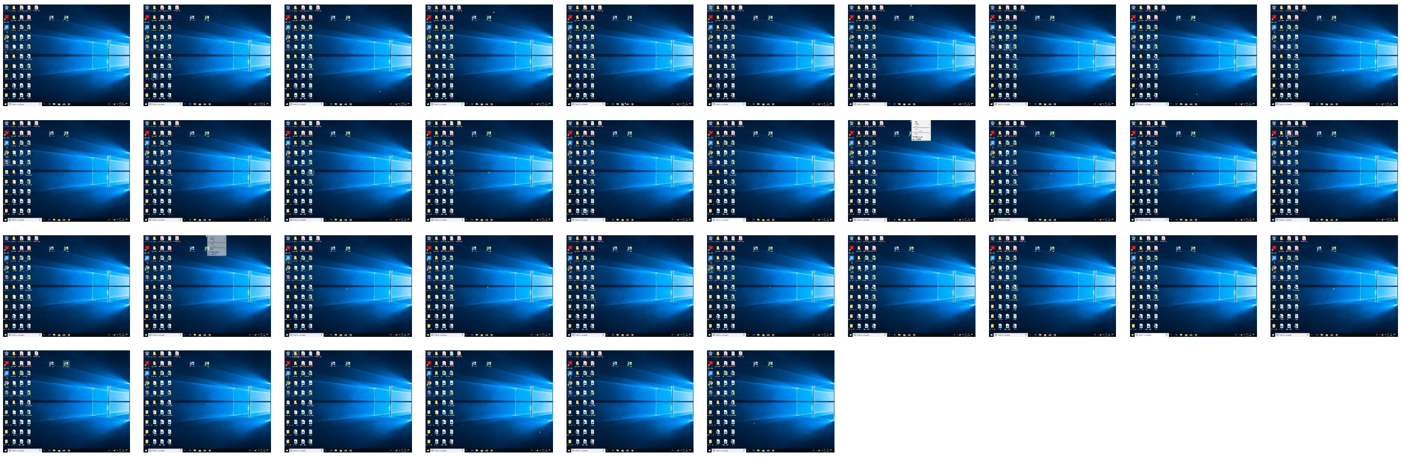
Legend:

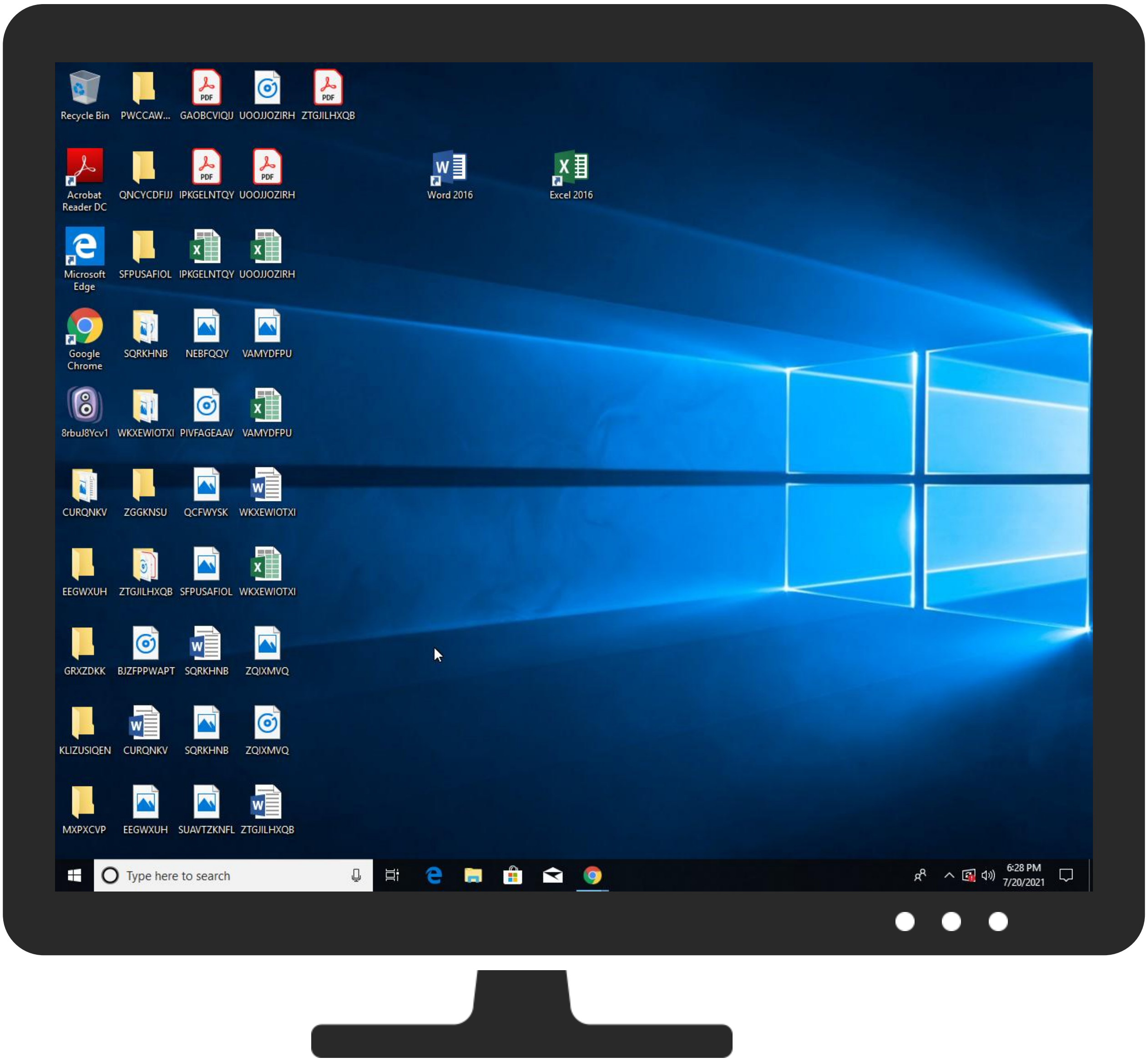
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

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
8rbuJ8Ycv1.exe	20%	Virustotal		Browse
8rbuJ8Ycv1.exe	41%	ReversingLabs	Win32.Trojan.GuLoader	

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:	33.0.0 White Diamond
Analysis ID:	451510
Start date:	20.07.2021
Start time:	18:23:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8rbuJ8Ycv1 (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:	13
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.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.4% (good quality ratio 13.4%) • Quality average: 23.9% • Quality standard deviation: 32.5%
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):	6.2334205108883545
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:	8rbuJ8Ycv1.exe
File size:	241664
MD5:	546f9c26cb739f1e3ea5ba1605aa7328
SHA1:	452ee936bbade0510c6c56d6e2b25f6ce7b835ff
SHA256:	6bd6a8e685288ca0af1d41d4d88fabd465f211c7cef32c00c994b89ea0a94f51
SHA512:	c454f30df142f374f8423d025b4b989b7667b0c7c91558e88f0e31723bfd01f22ac539c31ab5d0ef4a0dc05e66577316bea935403b340b188e79dd0f84a01ac9
SSDEEP:	3072:53BepJlZa/UNKcz3YU3OVEVGrBI4lsHJlZapGBR:PiUUQcz3zYEMiZHP
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........#...B...B...B..L^...B...`...B...d...B..Rich.B..........PE..L......U................. ....0....@................

File Icon

Icon Hash:	f8fcd4ccf4e4e8d0

Static PE Info

General

Entrypoint:	0x4019b0

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x55C60000 [Sat Aug 8 13:11:28 2015 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:	e9f7dd0da1a2a1266893e1ae4ef42b67

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x31b84	0x32000	False	0.39130859375	data	6.38659297214	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x33000	0x1290	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x35000	0x6d1e	0x7000	False	0.481828962054	data	5.45374661294	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	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: 8rbuJ8Ycv1.exe PID: 6936 Parent PID: 5824

General

Start time:	18:24:44
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\8rbuJ8Ycv1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\8rbuJ8Ycv1.exe'
Imagebase:	0x400000
File size:	241664 bytes
MD5 hash:	546F9C26CB739F1E3EA5BA1605AA7328
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis