JoeSandbox Cloud BASIC

ID: 435307
Sample Name: Notepad2.exe
Cookbook: default.jbs
Time: 11:54:17
Date: 16/06/2021
Version: 32.0.0 Black Diamond

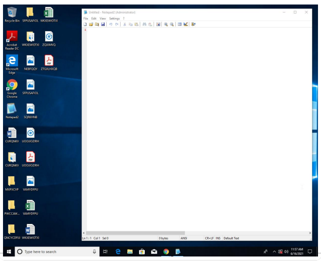
Table of Contents

Windows Analysis Report Notepad2.exe

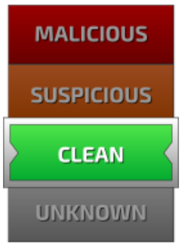
Overview

General Information

Sample Name:	Notepad2.exe
Analysis ID:	435307
MD5:	f6d48867d815d63.
SHA1:	f8f9c191d37b643..
SHA256:	c6086336a827a9..
Infos:	
Most interesting Screenshot:	



Detection

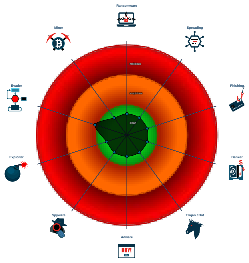


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- PE file contains strange resources
- Sample file is different than original …

Classification



Process Tree

- **System is w10x64**
- Notepad2.exe (PID: 6948 cmdline: 'C:\Users\user\Desktop\Notepad2.exe' MD5: F6D48867D815D6322199E90AA71A8C69)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

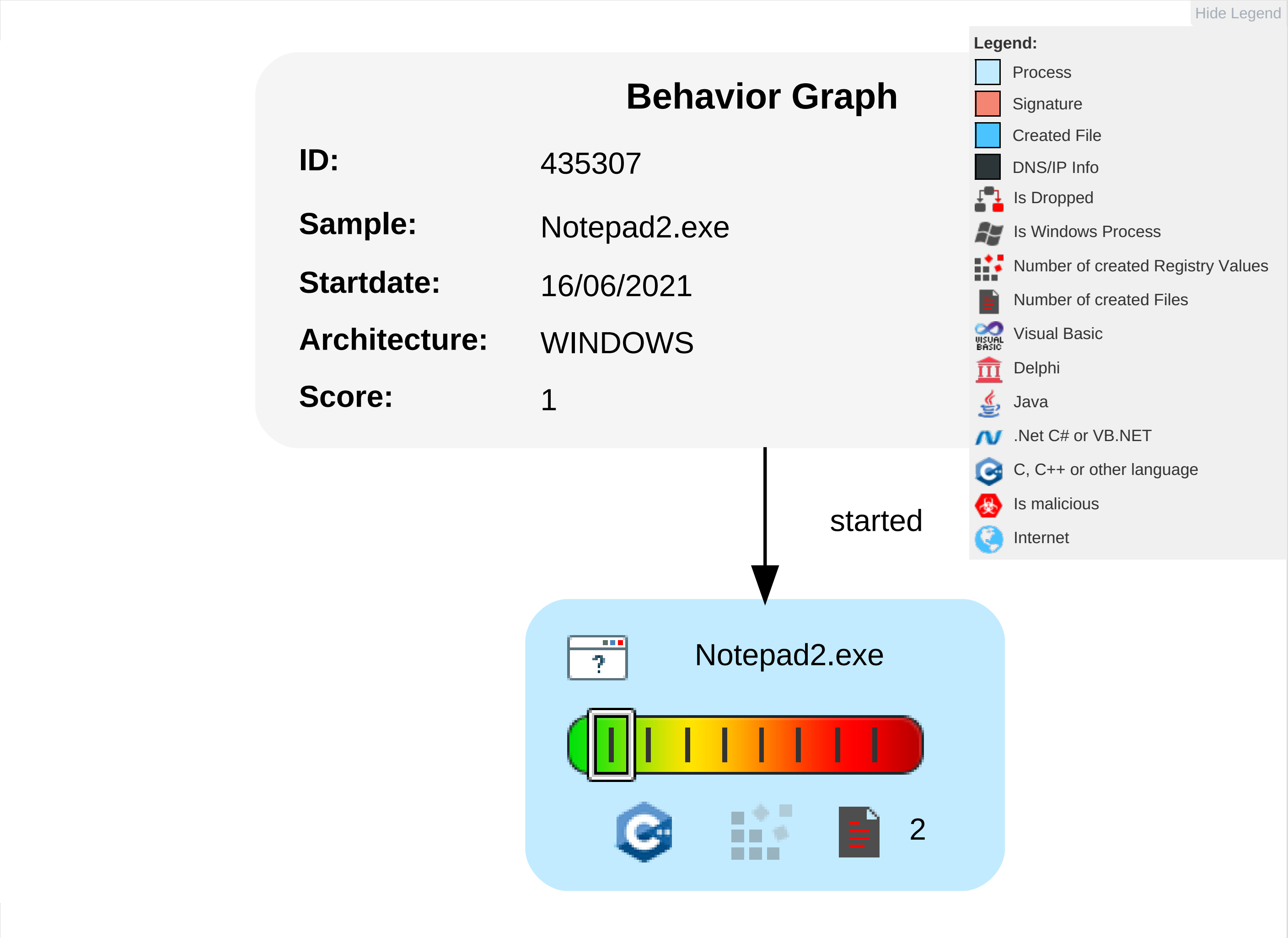
Click to jump to signature section

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	Command and Scripting Interpreter 2	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	System Time Discovery 1	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	Rootkit	LSASS Memory	Process Discovery 1	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	System Information Discovery 2	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

Behavior Graph



Behavior Graph

ID: 435307

Sample: Notepad2.exe

Startdate: 16/06/2021

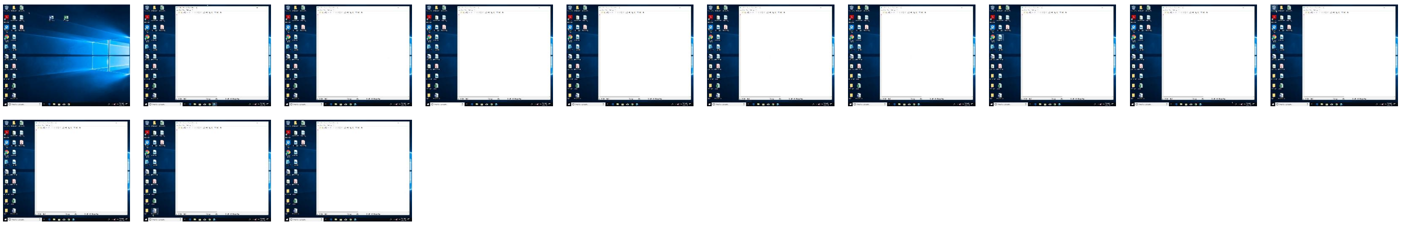
Architecture: WINDOWS

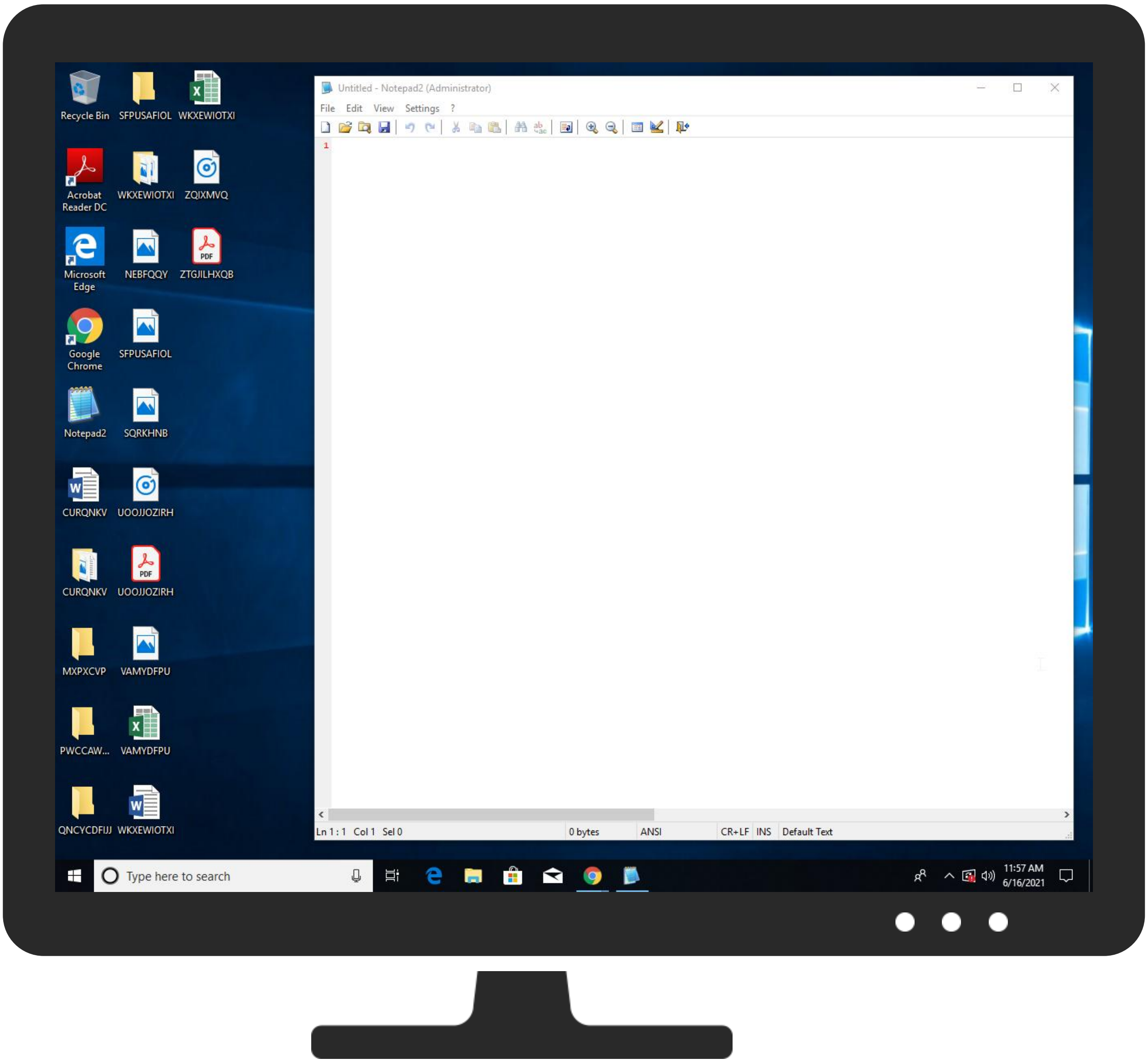
Score: 1

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
Notepad2.exe	0%	Virustotal		Browse
Notepad2.exe	0%	Metadefender		Browse
Notepad2.exe	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.flos-freeware.ch.JNo	0%	Avira URL Cloud	safe	
http://www.flos-freeware.chFlorian	0%	Avira URL Cloud	safe	
http://www.flos-freeware.chflorian.balmer	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435307
Start date:	16.06.2021
Start time:	11:54:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Notepad2.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:	19
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.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.3% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
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) x86-64, for MS Windows
Entropy (8bit):	5.889404378786351
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Notepad2.exe
File size:	919552
MD5:	f6d48867d815d6322199e90aa71a8c69
SHA1:	f8f9c191d37b643a20870ab8d0af39780c4677ff
SHA256:	c6086336a827a9852ee5cf6f46ffb7b1fccf82f194132a0c8a217d1240654f9f
SHA512:	05b1bc5b750955bda17d8baf29aecf019fe07cb9723acab8bd4b6384f4426b837b5bf9c07ac80ff4812081e3bee6ae15e05387810c060adeb05531219082bcfe
SSDEEP:	24576:ptdaP4lgqVU2stGJPATW2cmGxxO9s4tjp:ptdM4Wg5stGJ4kkt9

General

File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$........@...!s..! s..!s..Y...!s..Y...!s..Y...!s..!r..#s..Y...!s..Y...!s......!s..Y...!s.. Y...!s.Rich.!s.........................PE..d..

File Icon

Icon Hash:	62747ededed6761e

Static PE Info

General

Entrypoint:	0x14009a770
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x4DC3C2FE [Fri May 6 09:44:30 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	37dbcc3aa03d6ea9633e60bf6bdf58bb

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa633a	0xa6400	False	0.479179393797	data	6.44097042111	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xa8000	0x21aa8	0x19600	False	0.0519839131773	data	0.837018933287	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xca000	0x4d28	0x4e00	False	0.472005208333	data	5.84155138667	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xcf000	0x1a2d8	0x1a400	False	0.332282366071	data	4.69733076355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0x1602	0x1800	False	0.2900390625	data	3.8290677788	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

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: Notepad2.exe PID: 6948 Parent PID: 5816

General

Start time:	11:55:21
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\Notepad2.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Notepad2.exe'
Imagebase:	0x7ff7ec980000
File size:	919552 bytes
MD5 hash:	F6D48867D815D6322199E90AA71A8C69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis