ID: 435318
Sample Name: Notepad2.ini
Cookbook: default.jbs
Time: 12:11:06
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

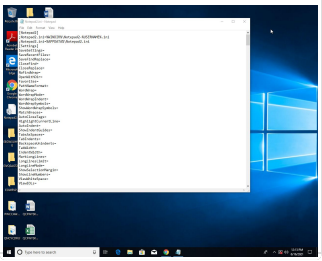
Windows Analysis Report Notepad2.ini

Overview

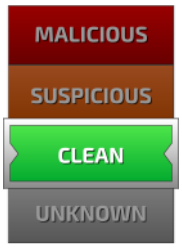
General Information

Sample Name:	Notepad2.ini
Analysis ID:	435318
MD5:	a7b5e91557f8d3d.
SHA1:	3253dfc9aa90131.
SHA256:	61ad82669e0c26..
Infos:	

Most interesting Screenshot:



Detection

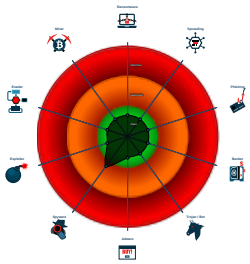


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- notepad.exe (PID: 4556 cmdline: 'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\Desktop\Notepad2.ini MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

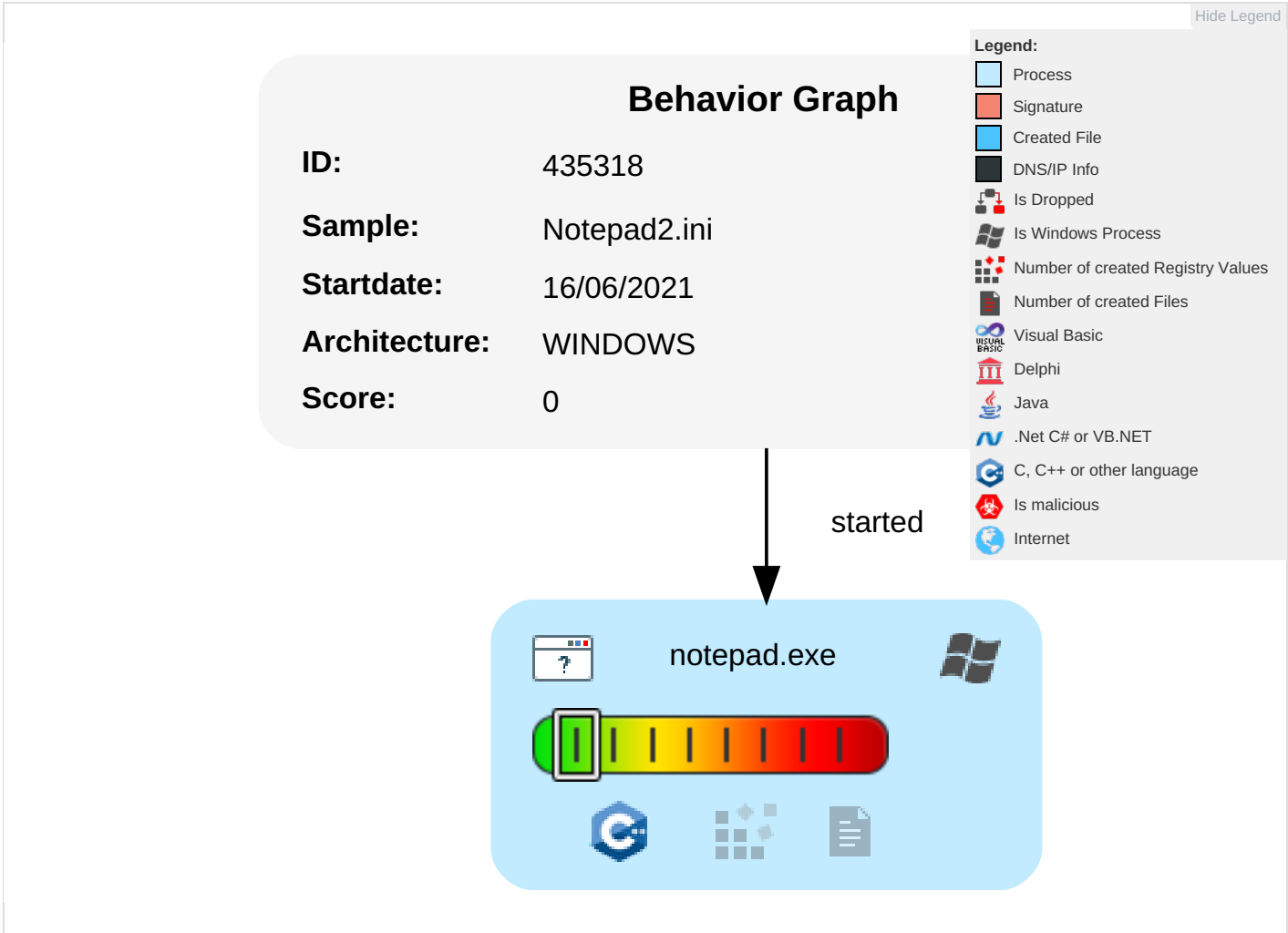
Click to jump to signature section

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	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	Process 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	System Information Discovery 1 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

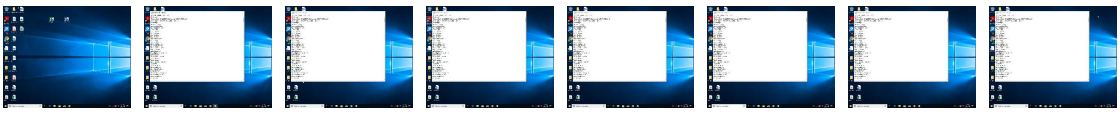
Behavior Graph

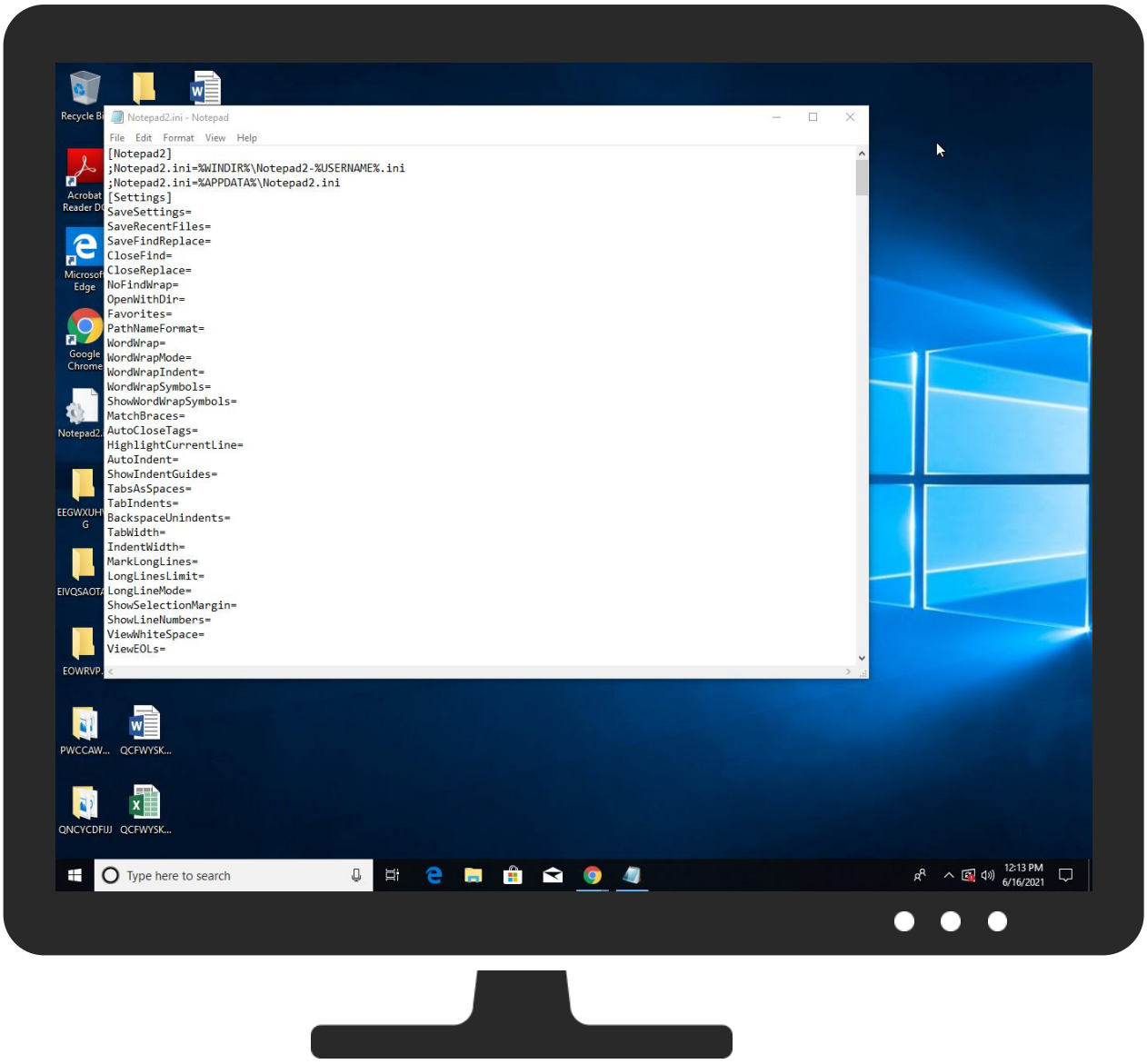


Screenshots

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
Notepad2.ini	0%	Virustotal		Browse
Notepad2.ini	0%	Metadefender		Browse
Notepad2.ini	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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435318
Start date:	16.06.2021
Start time:	12:11:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Notepad2.ini
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:	clean0.winINI@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:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .ini
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:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Entropy (8bit):	3.6978963641969527
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:	Notepad2.ini
File size:	23130
MD5:	a7b5e91557f8d3d23280ac818e9553d6
SHA1:	3253dfc9aa901311ba13e9eddc7b6481c6cf5778
SHA256:	61ad82669e0c260bda5472edca928785b72a0e9ad69d2c821db6bfe1e11df412
SHA512:	c0e8f169d1af09db7ea9cc0834e4438e4e40aac1677610f16f6db5b21ea46d3668a0b1d1e147ee2b981310b3a2116ad2c2d41f2213246278339dce52a28b9f36
SSDEEP:	384:ufooogxiica9TgqSSZ/LLC5FXRCpXOBWo:uAoogBcyeBWo
File Content Preview:	..[.N.o.t.e.p.a.d.2.].....;.N.o.t.e.p.a.d.2...i.n.i.=.%.W.I.N.D.I.R.%.\.N.o.t.e.p.a.d.2.-.%.U.S.E.R.N.A.M.E.%...i.n.i.....;.N.o.t.e.p.a.d.2...i.n.i.=.%.A.P.P.D.A.T.A.%.\.N.o.t.e.p.a.d.2...i.n.i.....[.S.e.t.t.i.n.g.s.].....S.a.v.e.S.e.t.t.i.n.g.s.=.....S.a

File Icon

Icon Hash:	74f0e4e0e2e5e2ec

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: notepad.exe PID: 4556 Parent PID: 5700

General

Start time:	12:11:52
Start date:	16/06/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\Desktop\Notepad2.ini
Imagebase:	0x7ff7977d0000
File size:	245760 bytes
MD5 hash:	BB9A06B8F2DD9D24C77F389D7B2B58D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis