ID: 534004
Sample Name: Everything.ini
Cookbook: default.jbs
Time: 23:37:04
Date: 04/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

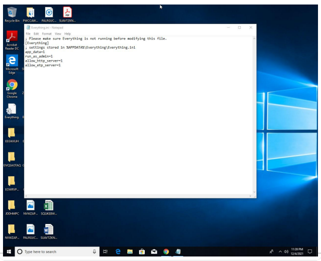
Windows Analysis Report Everything.ini

Overview

General Information

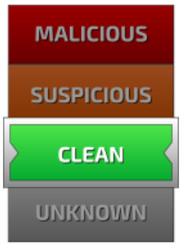
Sample Name:	Everything.ini
Analysis ID:	534004
MD5:	2dd1085be0d738..
SHA1:	9a2a15f7376bc2f..
SHA256:	4da456f41f02783..
Infos:	

Most interesting Screenshot:



```
; Please make sure Everything is not running before modifying this file.
[Everything]
; settings stored in %APPDATA%\Everything\Everything.ini
app_data=1
run_as_admin=1
allow_http_server=1
allow_etp_server=1
```

Detection

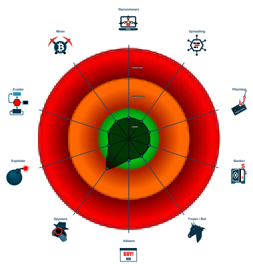


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- notepad.exe (PID: 6964 cmdline: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\Everything.ini MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

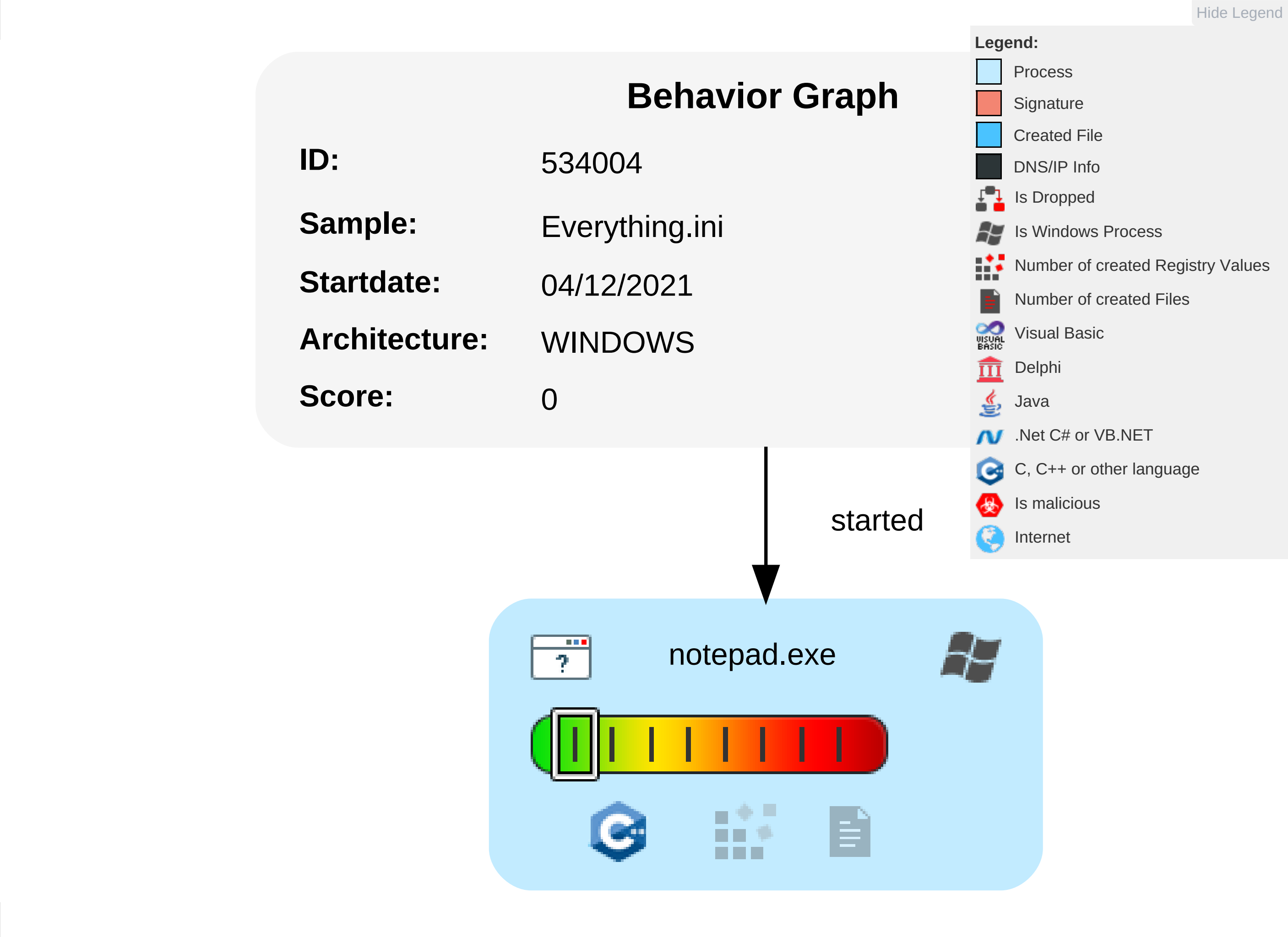
Click to jump to signature section

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



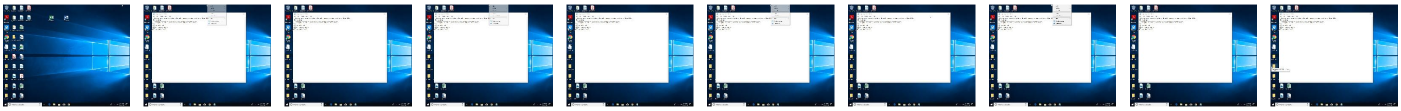
Legend:

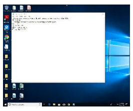
- ■ Process
- ■ Signature
- ■ Created File
- ■ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

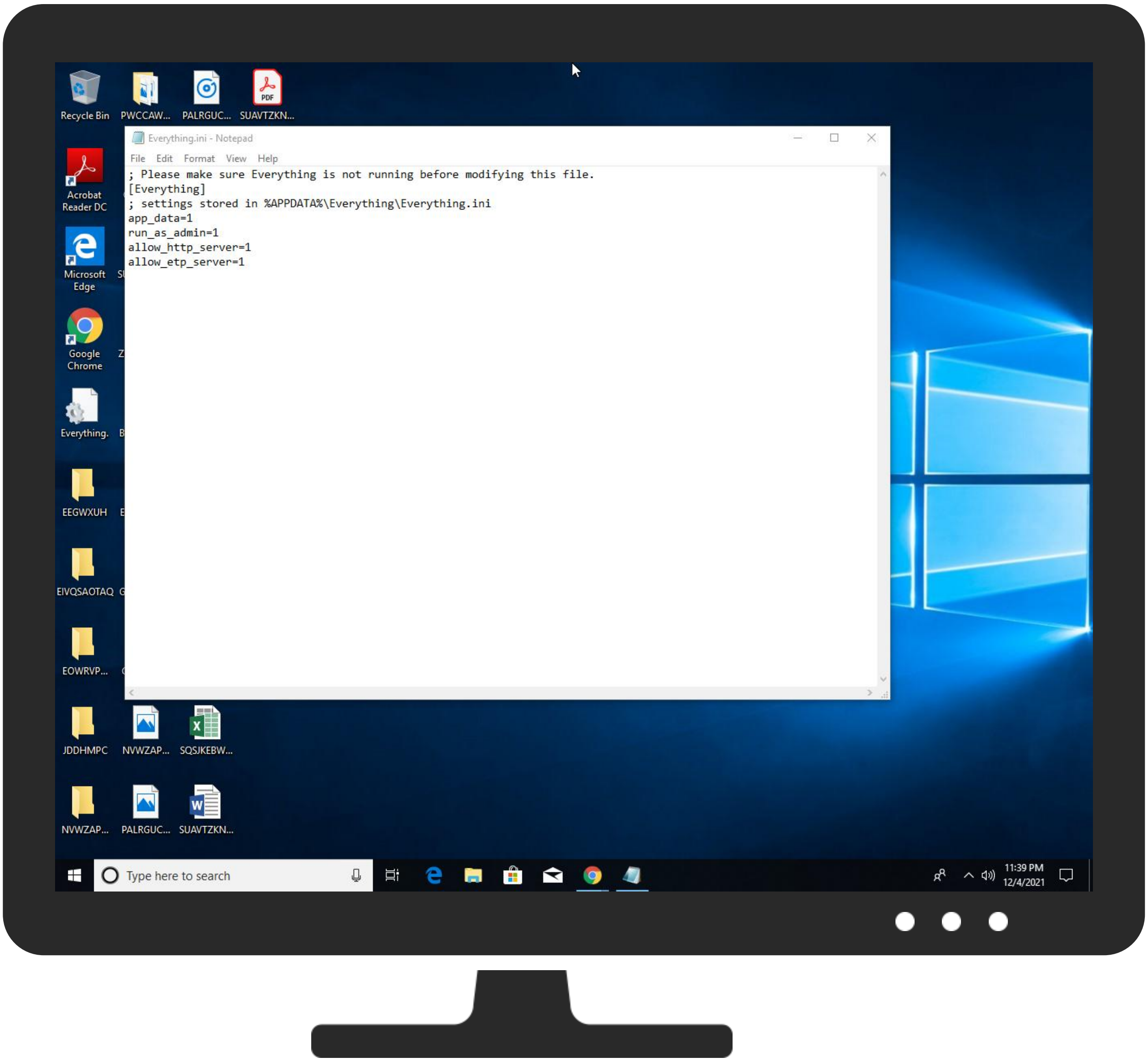
Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.







```
; Please make sure Everything is not running before modifying this file.
[Everything]
; settings stored in %APPDATA%\Everything\Everything.ini
app_data=1
run_as_admin=1
allow_http_server=1
allow_etp_server=1
```

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Everything.ini	0%	Virustotal		Browse
Everything.ini	0%	Metadefender		Browse
Everything.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:	34.0.0 Boulder Opal
Analysis ID:	534004
Start date:	04.12.2021
Start time:	23:37:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Everything.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:	23
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:	ASCII text, with CRLF line terminators
Entropy (8bit):	4.820018471651221
TrID:	
File name:	Everything.ini
File size:	215
MD5:	2dd1085be0d738b72396100119ef4f4f
SHA1:	9a2a15f7376bc2f2d3e781cb02d42c192c691925
SHA256:	4da456f41f0278330f77edadea352c93c812fb526595edbf 6396a97b76acf9bd
SHA512:	21a22c302bbd1d0b0af9aabdcfe4e62d8edc53c54a644c1 1ef40ba926d84a0092e9b4841938f0496065ec04a1ad540 dca31d8fe259d9ca62dabf4197b1fb4c0b
SSDEEP:	6:a1He3YP00iIHlCrev7AU5c2LHd7Mv6BJ3mYxvNDJZ+AmMy:xoflCrDmc2xMv63rxlA
File Content Preview:	; Please make sure Everything is not running before modifying this file...[Everything]..; settings stored in %APPDATA%\Everything\Everything.ini..app_data=1..run_as_admin=1..allow_http_server=1..allow_etp_server=1..

File Icon

Icon Hash:	74f0e4e0e2e5e2ec

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: notepad.exe PID: 6964 Parent PID: 3860

General

Start time:	23:37:55
Start date:	04/12/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\Everything.ini
Imagebase:	0x7ff657970000
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