ID: 612089
Sample Name: autorun.inf
Cookbook: default.jbs
Time: 15:07:11
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

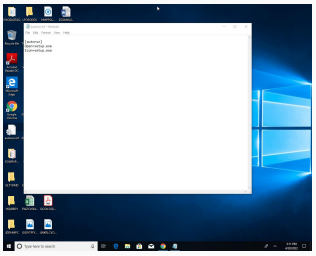
Windows Analysis Report

autorun.inf

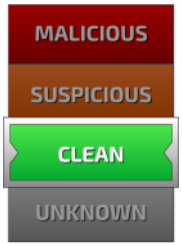
Overview

General Information

Sample Name:	autorun.inf
Analysis ID:	612089
MD5:	05b84abc08bda0..
SHA1:	7c12e7193fdf6c2..
SHA256:	d409d2c95ffd569..



Detection

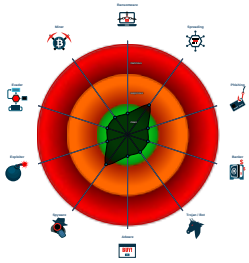


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Queries the volume information (nam…
- May infect USB drives

Classification



Process Tree

- **System is w10x64**
- notepad.exe (PID: 6360 cmdline: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\autorun.inf MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

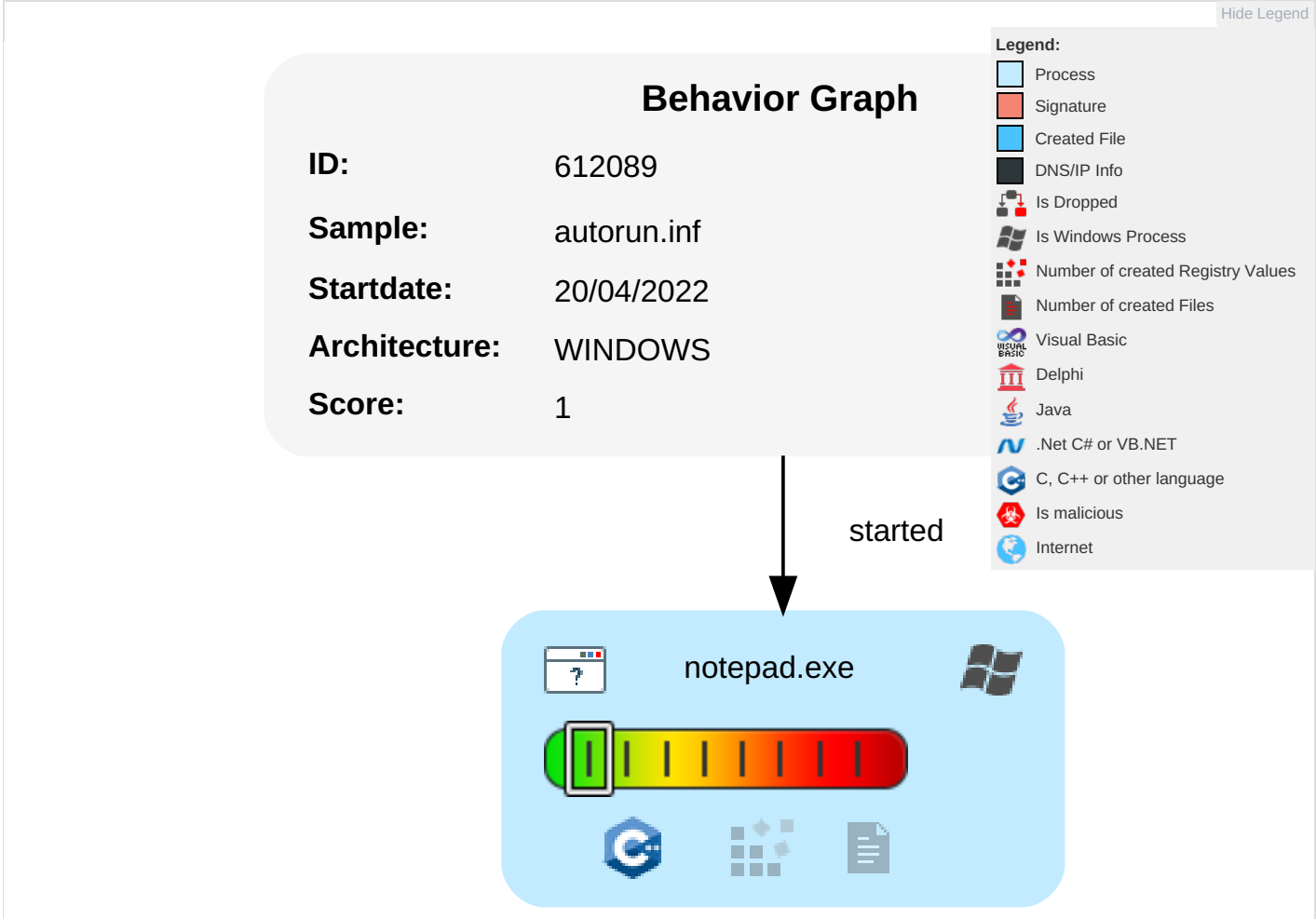
Joe Sandbox Signatures

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
1 Replication Through Removable Media	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	1 Peripheral Device Discovery	1 Replication Through Removable Media	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	1 1 System Information Discovery	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

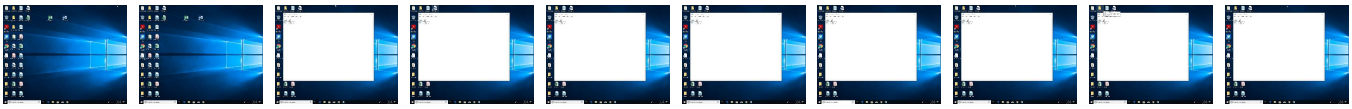
Behavior Graph

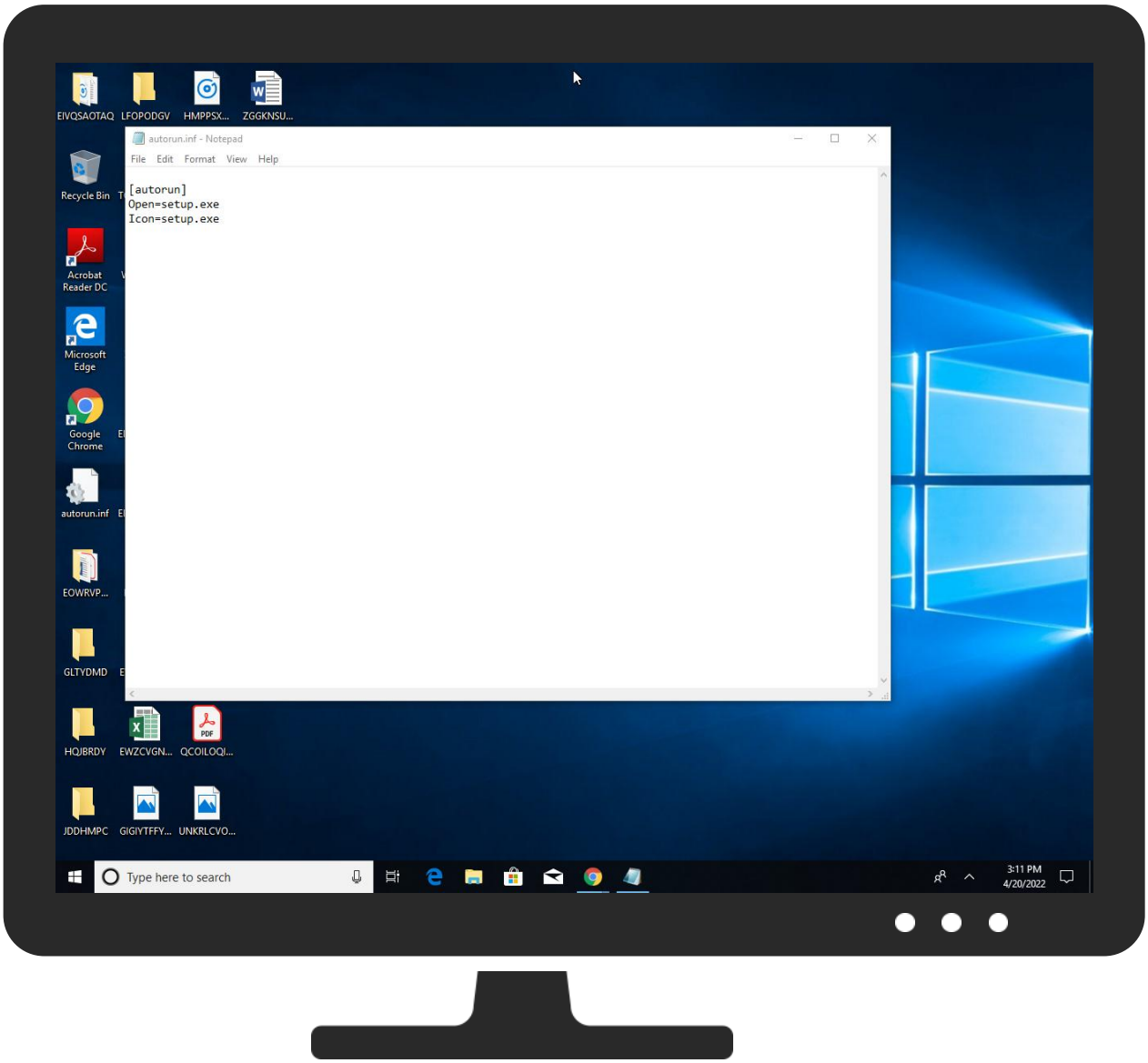


Screenshots

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
autorun.inf	0%	Metadefender		Browse
autorun.inf	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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	612089
Start date and time: 20/04/202215:07:11	2022-04-20 15:07:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	autorun.inf
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
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	24
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.winINF@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:	• Found application associated with file extension: .inf • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, query.prod.cms.rt.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- VT rate limit hit for: autorun.inf

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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):	3.9559627259379075
TrID:	
File name:	autorun.inf
File size:	47
MD5:	05b84abc08bda0f18e44fd5e526752f1
SHA1:	7c12e7193fdf6c2f1d6305a5d7010ad1403dad81
SHA256:	d409d2c95ffd569d2205797915057d6289048ffa3543014aaff39f5a3f72b7a9

SHA512:	7fc363cd2d3200baec07ff7c4f968e42c81c99ac9862798b11ac885337856e98739a72ffc1adb7a99e01ee38eca1b0201c1c3509e76d94e97aafcbda50ce868a
SSDEEP:	3:tPt1qVudVL4C7A2VL40:tPt1qwXL4CEyL40
TLSH:	
File Content Preview:	..[autorun]..Open=setup.exe..Icon=setup.exe....

File Icon

Icon Hash:	74f0e4e0e2e5e2ec

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: notepad.exe PID: **6360**, Parent PID: **5584**

General

Target ID:	0
Start time:	15:09:47
Start date:	20/04/2022
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\autorun.inf
Imagebase:	0x7ff601e30000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly