ID: 753424
Sample Name: 1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg
Cookbook: default.jbs
Time: 19:58:34
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

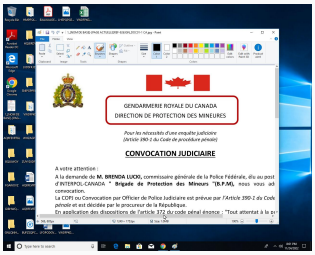
Windows Analysis Report

1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg

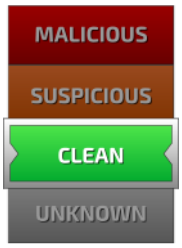
Overview

General Information

Sample Name:	1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg
Analysis ID:	753424
MD5:	1323ef9f42f3b9a..
SHA1:	2b41b9f531e194..
SHA256:	b854673b66dc36..



Detection

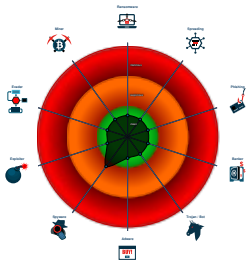


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Queries the volume information (nam…
- Creates files inside the system direc…

Classification



Analysis Advice

Sample is a picture (JPEG, PNG, GIF etc), nothing to analyze

Sample has a GUI, but Joe Sandbox has not found any clickable buttons, likely more UI automation may extend behavior

Process Tree

- **System is w10x64**
- mspaint.exe (PID: 6104 cmdline: mspaint.exe "C:\Users\user\Desktop\1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg" MD5: B59CF145BBAE39672321768B33A01CFA)
- **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

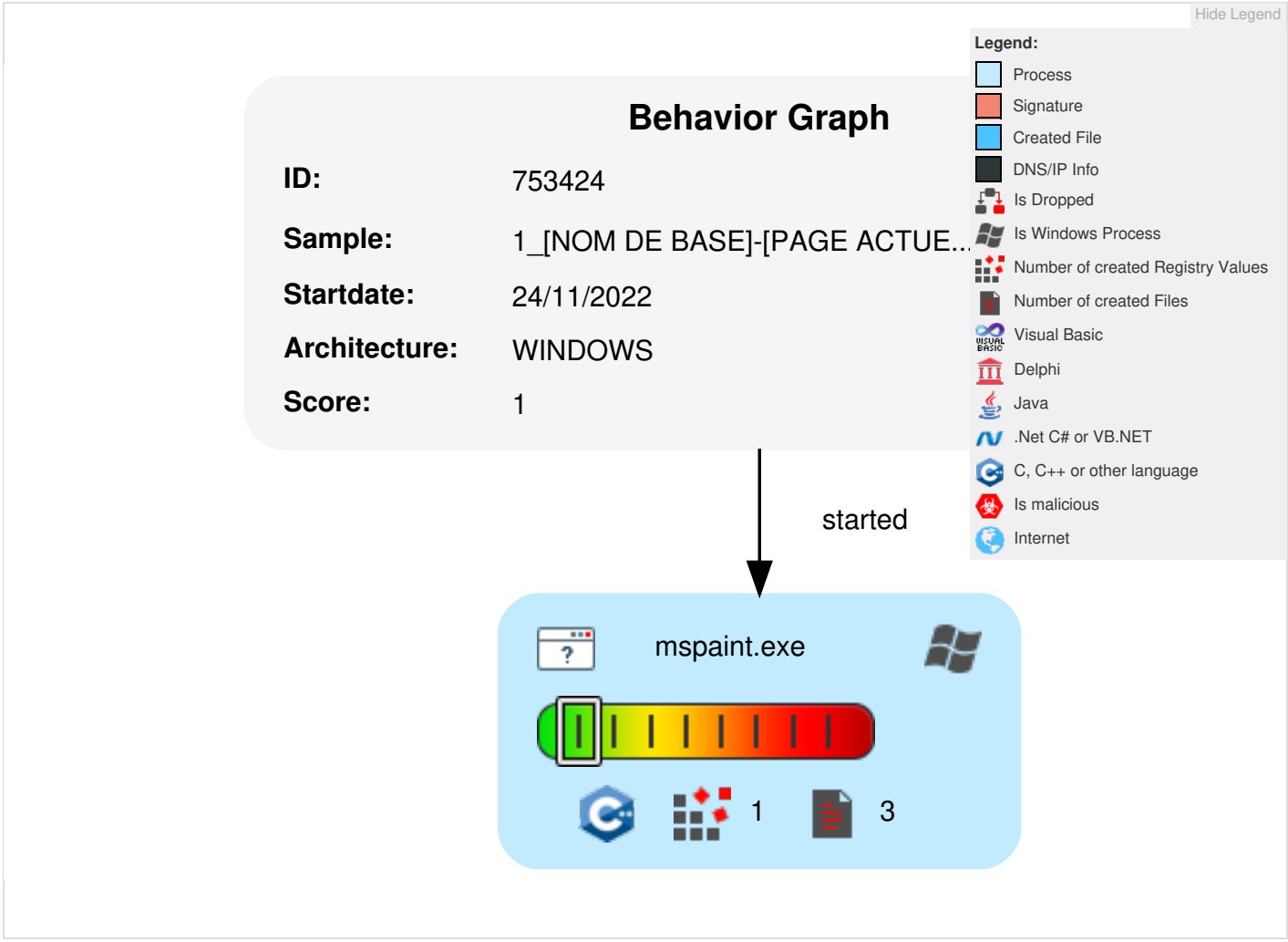
Joe Sandbox Signatures

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 Process Discovery	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	1 File and Directory 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 1 System Information Discovery	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

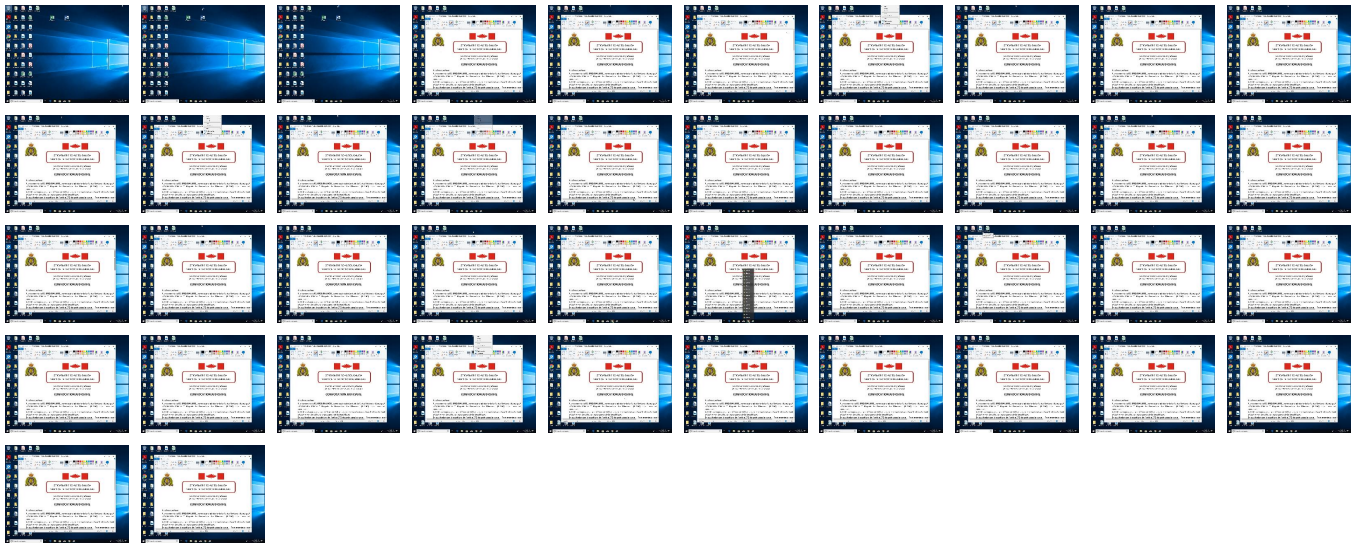
Behavior Graph

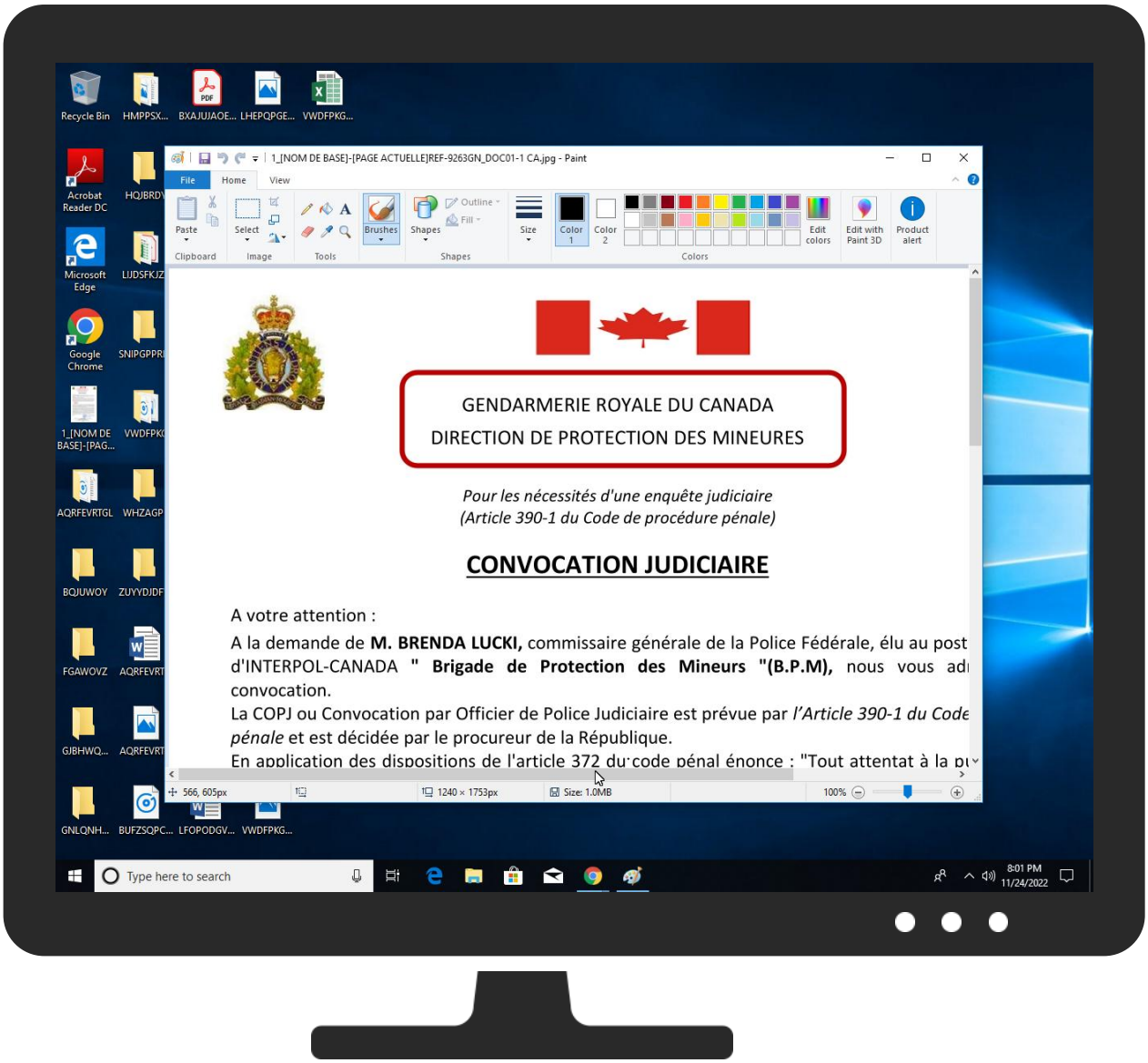


Screenshots

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
1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg	0%	ReversingLabs		
1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg	0%	Virustotal		Browse

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:	36.0.0 Rainbow Opal
Analysis ID:	753424
Start date and time:	2022-11-24 19:58:34 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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.winJPG@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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 209.197.3.8, 8.241.126.121, 8.248.143.254, 8.238.88.254, 8.238.85.126, 67.26.75.254
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:00:09	API Interceptor	439x Sleep call for process: mspaint.exe modified

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:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1240x1753, components 3
Entropy (8bit):	7.720722799240155
TrID:	• JFIF JPEG Bitmap (4007/3) 50.02% • JPEG Bitmap (3003/1) 37.49% • MP3 audio (1001/1) 12.50%
File name:	1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg
File size:	1049884
MD5:	1323ef9f42f3b9a3faa0b80406c3ae8e
SHA1:	2b41b9f531e1944cca49f2599095251c2bb33d6b
SHA256:	b854673b66dc36a8b3c719fde697bb45db3b3c3eae19608d267ad5359631105f
SHA512:	8eda347d278aa045adf21ed73a94c14e2924a69c8c1ee838e1dced748c4e8d7b4fee4186c364de9c1533e07885f64ab9198012b49f261d387fbdc363ebc92790
SSDEEP:	24576:Wui4pu+k3U2kD+5kWa0LYzyG6JneXJReYf1+yILOesCmwa:Zu+k3d1kcVG6JneXDeajIPsxwa
TLSH:	3C2501539C0C8A23A98C53A9BD630D6C7B1A061C96CA72FD05621DCA3FCD7354C9E67E
File Content Preview:	......JFIF.....C.....C.....".....}.....!1A..Qa."q.2....

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: mspaint.exe PID: 6104, Parent PID: 2304

General

Target ID:	0
Start time:	19:59:26
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\mspaint.exe
Wow64 process (32bit):	true
Commandline:	mspaint.exe "C:\Users\user\Desktop\1_[NOM DE BASE]-[PAGE ACTUELLE]REF-9263GN_DOC01-1 CA.jpg"
Imagebase:	0x220000
File size:	6589440 bytes
MD5 hash:	B59CF145BBAE39672321768B33A01CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly