

JOESandbox Cloud BASIC



ID: 715099

Sample Name: BILL #
965415965285.jpg

Cookbook: default.jbs

Time: 16:19:06

Date: 03/10/2022

Version: 36.0.0 Rainbow Opal

Table of Contents


Table of Contents	2
Windows Analysis Report BILL # 965415965285.jpg	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Analysis Advice	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	4
Joe Sandbox Signatures	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
World Map of Contacted IPs	7
General Information	7
Warnings	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
Network Behavior	8
Statistics	9
System Behavior	9
Analysis Process: mspaint.exePID: 5632, Parent PID: 1016	9
General	9
File Activities	9
Registry Activities	9
Disassembly	9

Windows Analysis Report

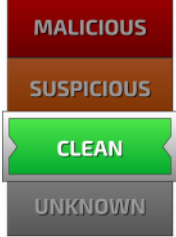
BILL # 965415965285.jpg

Overview

General Information

Sample Name:	BILL # 965415965285.jpg
Analysis ID:	715099
MD5:	4eb6cc54e959e6..
SHA1:	49b2179a340258.
SHA256:	0e24066d7f4fd81.
	

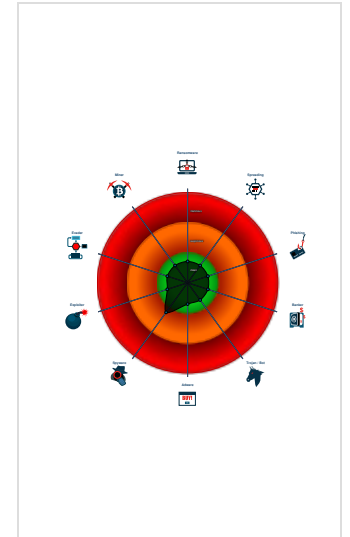
Detection

	
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: 5632 cmdline: mspaint.exe "C:\Users\user\Desktop\BILL # 965415965285.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	 Masquerading	OS Credential Dumping	 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	 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	  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

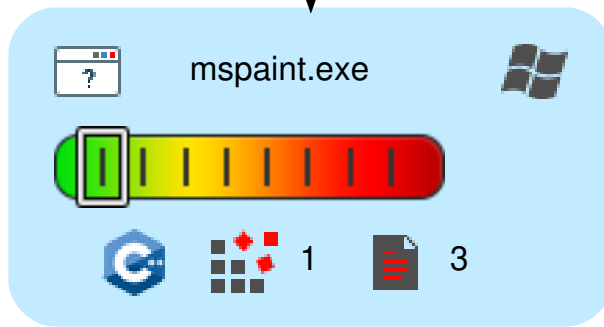
Behavior Graph

Behavior Graph

ID: 715099
Sample: BILL # 965415965285.jpg
Startdate: 03/10/2022
Architecture: WINDOWS
Score: 1

- 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

started



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
BILL # 965415965285.jpg	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:	36.0.0 Rainbow Opal
Analysis ID:	715099
Start date and time:	2022-10-03 16:19:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BILL # 965415965285.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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win.JPG@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none">• 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 domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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


 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:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4], baseline, precision 8, 2453x3177, components 4
Entropy (8bit):	7.08825795435992
TrID:	<ul style="list-style-type: none">JFIF-EXIF JPEG Bitmap (5003/1) 35.03%JFIF JPEG Bitmap (4007/3) 28.06%JPEG Bitmap (3003/1) 21.03%HSC music composer song (1267/141) 8.87%MP3 audio (1001/1) 7.01%
File name:	BILL # 965415965285.jpg
File size:	1497856
MD5:	4eb6cc54e959e6d6b4f8d5f4723a3e7b
SHA1:	49b2179a34025829ea932f56bba5a14c8e9c70f0
SHA256:	0e24066d7f4fd81120add0e0833fe89b6adfe66d65187cb69c863f90b092a99b
SHA512:	3efead65d3ab07c061b1a3a5ba19ecd95ec2bd6292e73b1487b6216b7c33bed1f0176f010e19ff595dc0d03579caad97e8fb7c954ff09f0631b7e88204e23b53
SSDEEP:	24576:N/yEI7qrraXb4a8F1GPxqYZXNQncQDs83B9q5KrKg:N/FluraLhKG8HNBDHB5rKg
TLSH:	AE65EF2C53E298E5CA4C82715C859B384D984DF35B65BA0733EFBD2C33B6E939742126
File Content Preview:JFIF.....Adobe.d.....Exif..MM.*.....J.i.....T.....>..... ...

Network Behavior

 No network behavior found

Statistics

 No statistics

System Behavior

Analysis Process: mspaint.exe PID: 5632, Parent PID: 1016

General

Target ID:	0
Start time:	16:20:03
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\mspaint.exe
Wow64 process (32bit):	true
Commandline:	mspaint.exe "C:\Users\user\Desktop\BILL # 965415965285.jpg"
Imagebase:	0xe00000
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