ID: 736950
Sample Name:
XPLHpP8RVc.exe
Cookbook: default.jbs
Time: 12:22:00
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

XPLHpP8RVc.exe

Overview

General Information

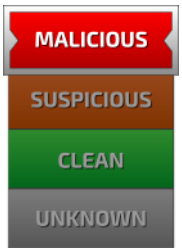
Sample Name:	XPLHpP8RVc.exe
Analysis ID:	736950
MD5:	d63bcf05b6e5f94..
SHA1:	9b9e999a161963.
SHA256:	de6e79d80d5cc9..
Tags:	exe

Errors

⚠ No process behavior to analyse as no analysis process or sample was found

⚠ Corrupt sample or wrongly selected analyzer. Details: C000007B

Detection

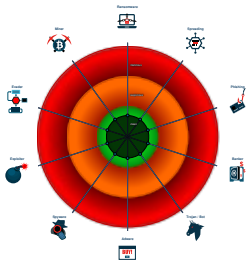


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- PE file has a writeable .text section
- Uses 32bit PE files
- PE file does not import any functions
- PE file contains an invalid checksum
- PE file overlay found
- Entry point lies outside standard sec…
- PE file contains sections with non-s…

Classification



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

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

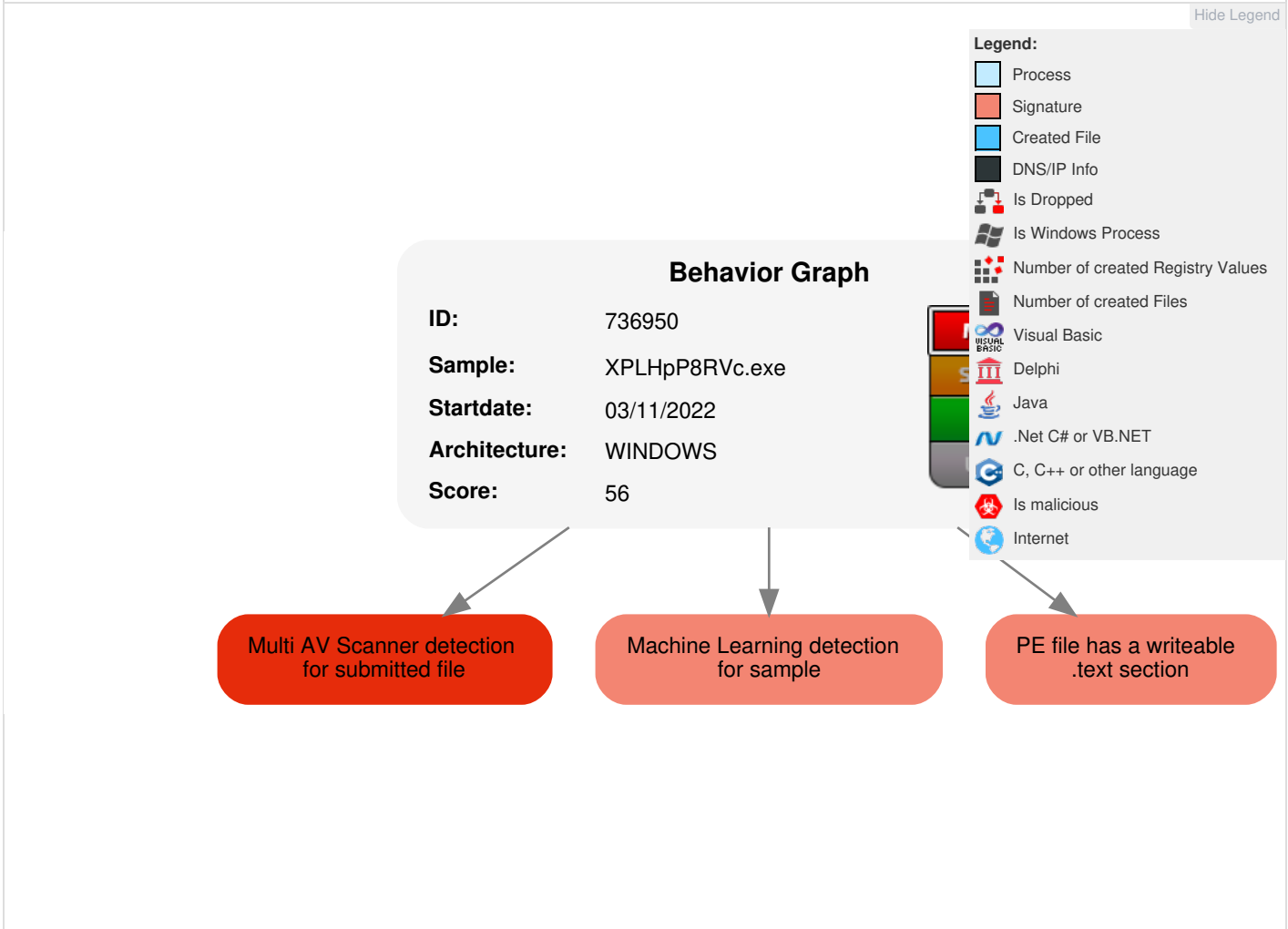
System Summary

PE file has a writeable .text section

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 Software Packing	OS Credential Dumping	System Service 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	1 Obfuscated Files or Information	LSASS Memory	Application Window 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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
XPLHpP8RVc.exe	38%	ReversingLabs	Win32.Trojan.Mikey	
XPLHpP8RVc.exe	28%	Virustotal		Browse
XPLHpP8RVc.exe	100%	Joe Sandbox ML		

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:	736950
Start date and time:	2022-11-03 12:22:00 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XPLHpP8RVc.exe
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:	0
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.winEXE@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .exe • Unable to launch sample, stop analysis

Errors

- No process behavior to analyse as no analysis process or sam ple was found
- Corrupt sample or wrongly sele cted analyzer. Details: C000007B

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:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.65926133234532
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	XPLHpP8RVc.exe

File size:	2398737
MD5:	d63bcf05b6e5f943213930ec13433edd
SHA1:	9b9e999a1619630297d3633555b3ca186d9b124d
SHA256:	de6e79d80d5cc90b9958e261e2e2c9c2eadda70c27daa171f406fc75fa967f8a
SHA512:	a7d9f37a338386dfcf760fb5cdcc792bef8d75c7500b0f677e2b411258e9ed8a617de93a3de0e4a1266f05c2c807b11750eb950eefeb91f17effdb43441ea6c7
SSDEEP:	49152:HWi9hA41soZEaAyefPTsusL53MPwKRjnig0wziDjXvBuyTtamjU8v1+8Ng+:79hl1soZEaAy8T058PwKRjnigfArEyTX
TLSH:	CDB5171967F34836C9722BF0C42552E4DE55D7283BBC010E1AF23AA83A337D9553EE5A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...GJ..GJ..GJ...J..GJ...J..GJ..FJ5.GJ...J..GJ...Ja.GJ...JD.GJ...J..GJRich..GJ.....PE..L...p.[c.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x71ff23
Entrypoint Section:	.sedata
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x635B9370 [Fri Oct 28 08:31:44 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3230e9	0x1a4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x324000	0x400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1e8000	0x1e8000	False	0.45711779985271517	data	6.3271988418278635	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.sedata	0x1e9000	0x13a000	0x13a000	False	0.7854236395773005	data	7.756485763720028	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x323000	0x1000	0x600	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x324000	0x1000	0x400	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.sedata	0x325000	0x1000	0x1000	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

No system behavior

Disassembly

No disassembly