

ID: 502669
Sample Name:
VolumeConverter.dll
Cookbook: default.jbs
Time: 08:44:09
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report VolumeConverter.dll 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
AV Detection: 4
Data Obfuscation: 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
Contacted IPs 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 8
General 8
File Icon 8
Static PE Info 8
General 9
Entrypoint Preview 9
Data Directories 9
Sections 9
Resources 9
Imports 9
Version Infos 9
Network Behavior 9
Code Manipulations 9
Statistics 9
Behavior 9
System Behavior 10
Analysis Process: loaddll32.exe PID: 6492 Parent PID: 2924 10
General 10
File Activities 10
Analysis Process: cmd.exe PID: 5940 Parent PID: 6492 10
General 10
File Activities 10
Analysis Process: rundll32.exe PID: 6072 Parent PID: 5940 10
General 10
File Activities 11
Disassembly 11
Code Analysis 11

Copyright Joe Security LLC 2021

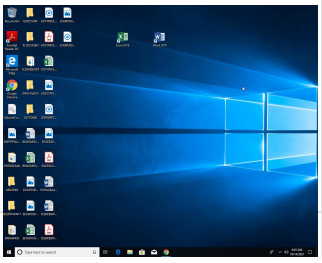
Windows Analysis Report VolumeConverter.dll

Overview

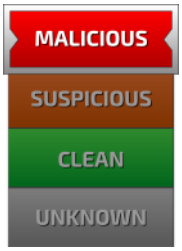
General Information

Sample Name:	VolumeConverter.dll
Analysis ID:	502669
MD5:	fc505773010d767.
SHA1:	6de72a38a4e8dd..
SHA256:	50711c59f53e618.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

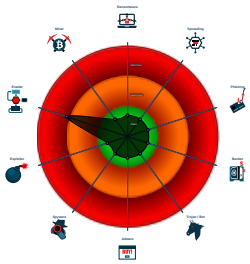


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- .NET source code contains method …
- Uses 32bit PE files
- Program does not show much activi…
- Creates a process in suspended mo…
- Binary contains a suspicious time st…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6492 cmdline: loaddll32.exe 'C:\Users\user\Desktop\VolumeConverter.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5940 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\VolumeConverter.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6072 cmdline: rundll32.exe 'C:\Users\user\Desktop\VolumeConverter.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **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

Copyright Joe Security LLC 2021

AV Detection:



Multi AV Scanner detection for submitted file

Data Obfuscation:



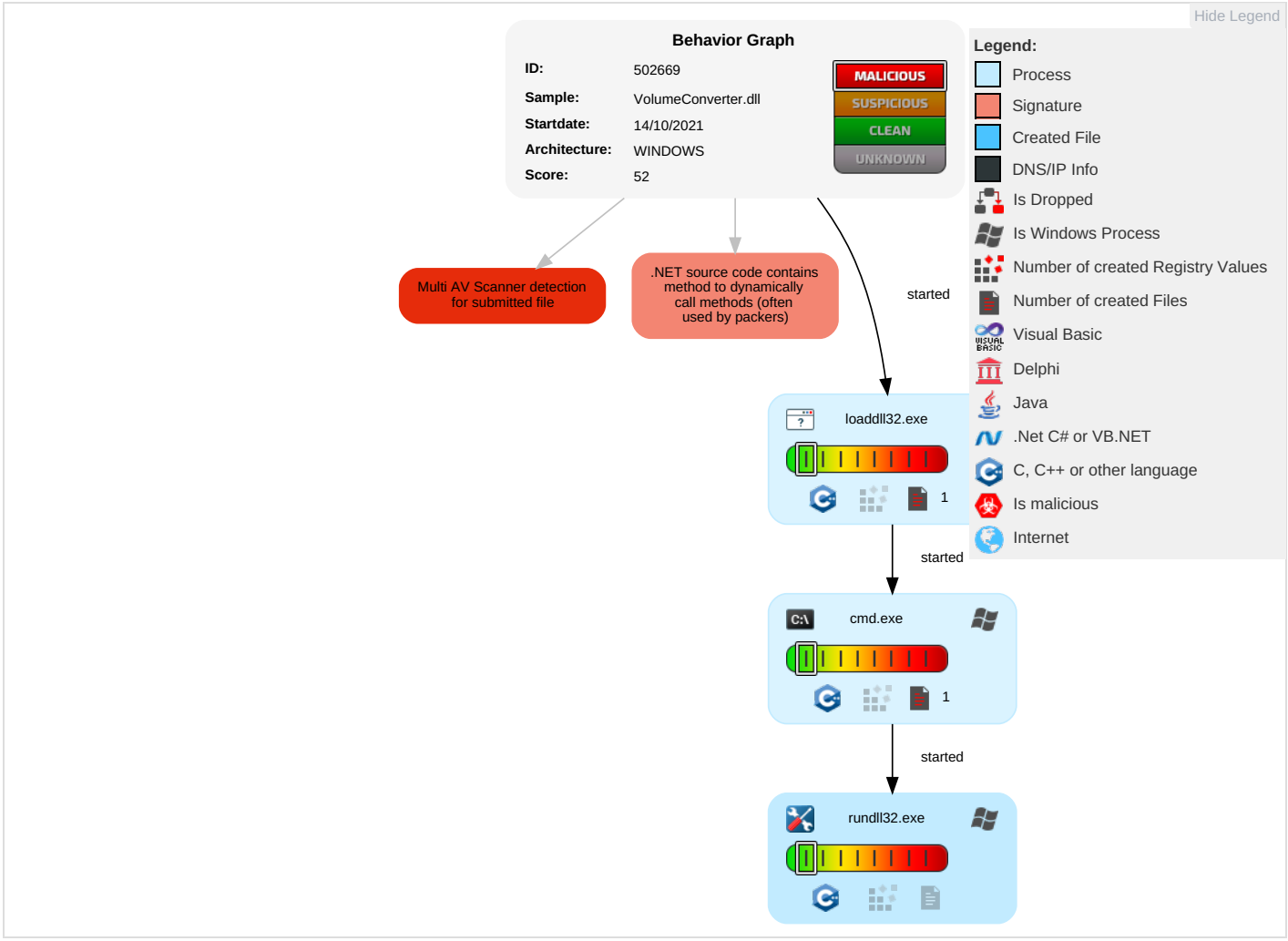
.NET source code contains method to dynamically call methods (often used by packers)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Rundll32 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph

Copyright Joe Security LLC 2021



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
VolumeConverter.dll	28%	Virustotal		Browse
VolumeConverter.dll	7%	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:	33.0.0 White Diamond
Analysis ID:	502669
Start date:	14.10.2021
Start time:	08:44:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VolumeConverter.dll
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:	5
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:	MAL
Classification:	mal52.evad.winDLL@5/0@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: .dll • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:45:07	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Copyright Joe Security LLC 2021

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:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.775670145513336
TrID:	• Win32 Dynamic Link Library (generic) Net Framework (1011504/3) 44.80% • Win32 Dynamic Link Library (generic) (1002004/3) 44.38% • Generic .NET DLL/Assembly (238134/4) 10.55% • Win16/32 Executable Delphi generic (2074/23) 0.09% • Generic Win/DOS Executable (2004/3) 0.09%
File name:	VolumeConverter.dll
File size:	58880
MD5:	fc505773010d767cc1eca83c1df804cb
SHA1:	6de72a38a4e8dd0dade2cae8566fbd885123bb4a
SHA256:	50711c59f53e618c7b3aefabea49f6355ef63ced5c217c3ab2f0be74aa45796c
SHA512:	2a42fd240088569767c04815b94e5856b3b019111af05903a0236e72e3f846bb5bae5fe06c9a7943a1f3855dd1fa1860db1be590677603abadf4f28146c419a
SSDEEP:	768:chZhjyuN7YNRnqIXxHHxV/3kaKPjpygwCV8SveN6K7sVppT2Gsy:chuS7kxxp0aWjrOQtK7stoy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....g.....!..... .....@.. .....`.....`.....

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x40f9ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xE3671BCB [Fri Nov 24 05:42:35 2090 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	dae02f32a21e03ce65412f6e56942daa

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd9d4	0xda00	False	0.488317087156	data	5.88553278046	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0x10000	0x1e8	0x200	False	0.861328125	data	6.61773120421	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0x3a4	0x400	False	0.365234375	data	2.9247083034	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

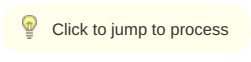
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6492 Parent PID: 2924

General

Start time:	08:45:07
Start date:	14/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\VolumeConverter.dll'
Imagebase:	0xec0000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5940 Parent PID: 6492

General

Start time:	08:45:07
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\VolumeConverter.dll',#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6072 Parent PID: 5940

General

Start time:	08:45:07
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\VolumeConverter.dll',#1
Imagebase:	0x12a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

File Activities

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021