General Info

Add for printing

File name: some_malicious_file.bin
Full analysis: https://app.any.run/tasks/a66178de-7596-4a05-945d-704dbf6b3b90
Verdict: Suspicious activity
Threats: Sodinokibi

Sodinokibi, also called Revil, is dangerous ransomware-type malware. Among other tools, it uses advanced encryption techniques and can operate without connection to control servers. Sodinokibi is among the most complex Ransomware in the world.

Malware Trends Tracker >>>

Analysis date: August 06, 2021 at 09:57:08
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags: ransomware sodinokibi
Indicators:
MIME: application/x-dosexec
File info: PE32 executable (GUI) Intel 80386, for MS Windows
MD5: 890A58F200DFFF23165DF9E1B088E58F
SHA1: 74E3D82F7EE81109E150DC41112CF95B3A4B5307
SHA256: 5F56D5748940E4039053F85978074BDE16D64BD5BA97F6F0026BA8172CB29E93
SSDEEP: 3072:Hp5SexkWi1LbI4eTMlwDCnu/q2GB96W/y:JvGWwbnWJ/yB9

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

Add for printing

MALICIOUS

Sodinokibi keys found
• some_malicious_file.bin.exe (PID: 1632)

Deletes shadow copies
• cmd.exe (PID: 448)

Starts BCDEDIT.EXE to disable recovery
• cmd.exe (PID: 448)

Sodinokibi ransom note found
• some_malicious_file.bin.exe (PID: 1632)

Renames files like Ransomware
• some_malicious_file.bin.exe (PID: 1632)

SUSPICIOUS

Checks supported languages
• some_malicious_file.bin.exe (PID: 1632)
• cmd.exe (PID: 448)
• some_malicious_file.bin.exe (PID: 2256)

Application launched itself
• some_malicious_file.bin.exe (PID: 2256)

Starts CMD.EXE for commands execution
• some_malicious_file.bin.exe (PID: 1632)

Reads the computer name
• some_malicious_file.bin.exe (PID: 2256)
• some_malicious_file.bin.exe (PID: 1632)

Executed as Windows Service
• vssvc.exe (PID: 2196)

Reads Environment values
• some_malicious_file.bin.exe (PID: 1632)

Creates files in the program directory
• some_malicious_file.bin.exe (PID: 1632)

Creates files like Ransomware instruction
• some_malicious_file.bin.exe (PID: 1632)

INFO

Checks supported languages
• vssadmin.exe (PID: 412)
• vssvc.exe (PID: 2196)
• bcdedit.exe (PID: 3140)
• bcdedit.exe (PID: 2940)

Reads the computer name
• vssadmin.exe (PID: 412)
• vssvc.exe (PID: 2196)

Dropped object may contain TOR URL's
• some_malicious_file.bin.exe (PID: 1632)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

Malware configuration

Add for printing

No Malware configuration.

Static information

Add for printing

TRiD

.exe | Win32 Executable MS Visual C++ (generic) (42.2)
.exe | Win64 Executable (generic) (37.3)
.dll | Win32 Dynamic Link Library (generic) (8.8)
.exe | Win32 Executable (generic) (6)
.exe | Generic Win/DOS Executable (2.7)

EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2019:06:10 17:29:32+02:00
PEType:	PE32
LinkerVersion:	14
CodeSize:	41984
InitializedDataSize:	122368
UninitializedDataSize:	0
EntryPoint:	0x36e6
OSVersion:	5.1
ImageVersion:	0
SubsystemVersion:	5.1
Subsystem:	Windows GUI

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	10-Jun-2019 15:29:32

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	5
Time date stamp:	10-Jun-2019 15:29:32
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE
	IMAGE_FILE_EXECUTABLE_IMAGE

Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x000000D0

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x0000A2D4	0x0000A400	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.55748
.rdata	0x0000C000	0x0000F650	0x0000F800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	6.43997
.data	0x0001C000	0x0000179C	0x00001600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.68881
.s7bz	0x0001E000	0x0000C800	0x0000C800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	5.09537
.reloc	0x0002B000	0x0000054C	0x00000600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	6.21532

Video and screenshots

Add for printing

All screenshots are available in the full report

All screenshots are available in the full report

Processes

Add for printing

Total processes	Monitored processes	Malicious processes	Suspicious processes
47	7	2	0

Behavior graph

Click at the process to see the details

Specs description

Process information

PID	CMD	Path	Indicators	Parent process
2256	"C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe"	C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe	—	Explorer.EXE

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

Modules

Images

- c:\users\admin\appdata\local\temp\some_malicious_file.bin.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\user32.dll
- c:\windows\system32\gdi32.dll
- c:\windows\system32\lpk.dll
- c:\windows\system32\usp10.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\imm32.dll

Previous 1 2 3 4 5 6 Next

1632	"C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe"	C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe		some_malicious_file.bin.exe

Information

User: admin Integrity Level: HIGH

Modules

Images

c:\users\admin\appdata\local\temp\some_malicious_file.bin.exe

c:\windows\system32\ntdll.dll

c:\windows\system32\kernel32.dll

c:\windows\system32\kernelbase.dll

c:\windows\system32\user32.dll

c:\windows\system32\gdi32.dll

c:\windows\system32\lpk.dll

c:\windows\system32\usp10.dll

c:\windows\system32\msvcrt.dll

c:\windows\system32\imm32.dll

Previous 1 2 3 4 5 6 7 8 Next

448 "C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures C:\Windows\System32\cmd.exe – some_malicious_file.bin.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: HIGH Description: Windows Command Processor
Exit code: 0 Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)

Modules

Images

c:\windows\system32\cmd.exe

c:\windows\system32\ntdll.dll

c:\windows\system32\kernel32.dll

c:\windows\system32\kernelbase.dll

c:\windows\system32\winbrand.dll

c:\windows\system32\msvcrt.dll

c:\windows\system32\user32.dll

c:\windows\system32\gdi32.dll

c:\windows\system32\lpk.dll

c:\windows\system32\usp10.dll

Previous 1 2 Next

412 vssadmin.exe Delete Shadows /All /Quiet C:\Windows\system32\vssadmin.exe – cmd.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: HIGH Description: Command Line Interface for Microsoft® Volume Shadow Copy Service
Exit code: 0 Version: 6.1.7600.16385 (win7_rtm.090713-1255)

Modules

Images

c:\windows\system32\vssadmin.exe

c:\windows\system32\ntdll.dll

c:\windows\system32\kernel32.dll

c:\windows\system32\kernelbase.dll

c:\windows\system32\advapi32.dll

c:\windows\system32\msvcrt.dll

c:\windows\system32\sechost.dll

c:\windows\system32\rpcrt4.dll

c:\windows\system32\atl.dll

c:\windows\system32\user32.dll

Previous 1 2 3 Next

2196 C:\Windows\system32\vssvc.exe C:\Windows\system32\vssvc.exe – services.exe

Information

User: SYSTEM Company: Microsoft Corporation
Integrity Level: SYSTEM Description: Microsoft® Volume Shadow Copy Service
Exit code: 0 Version: 6.1.7600.16385 (win7_rtm.090713-1255)

Modules

Images

c:\windows\system32\vssvc.exe

c:\windows\system32\ntdll.dll

c:\windows\system32\kernel32.dll

c:\windows\system32\kernelbase.dll

c:\windows\system32\advapi32.dll

c:\windows\system32\msvcrt.dll

c:\windows\system32\sechost.dll

c:\windows\system32\rpcrt4.dll

c:\windows\system32\user32.dll

c:\windows\system32\gdi32.dll

Previous 1 2 3 4 5 Next

3140 bcdedit /set {default} recoveryenabled No C:\Windows\system32\bcdedit.exe – cmd.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: HIGH Description: Boot Configuration Data Editor
Exit code: 0 Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)

Modules

Images

c:\windows\system32\bcdedit.exe

c:\windows\system32\ntdll.dll

c:\windows\system32\kernel32.dll

c:\windows\system32\kernelbase.dll

c:\windows\system32\msvcrt.dll

c:\windows\system32\advapi32.dll

c:\windows\system32\sechost.dll

c:\windows\system32\rpcrt4.dll

2940 bcdedit /set {default} bootstatuspolicy ignoreallfailures C:\Windows\system32\bcdedit.exe – cmd.exe

Information

User: admin Company: Microsoft Corporation

Integrity Level: HIGH Description: Boot Configuration Data Editor

Exit code: 0 Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)

Modules

Images

c:\windows\system32\bcdedit.exe

c:\windows\system32\kernel32.dll

c:\windows\system32\ntdll.dll

c:\windows\system32\msvcrt.dll

c:\windows\system32\advapi32.dll

c:\windows\system32\kernelbase.dll

c:\windows\system32\sechost.dll

c:\windows\system32\rpcrt4.dll

Registry activity

Add for printing

Total events	Read events	Write events	Delete events
1 298	1 274	24	0

Modification events

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: ProxyBypass
Value: 1

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: IntranetName
Value: 1

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: UNCAsIntranet
Value: 1

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: AutoDetect
Value: 0

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: sub_key
Value: D60DFF40440F390ED2DDF04B674C2FBBF07D35FA4B2EF7FC981CA8377A2BF44D

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: pk_key
Value: A054B93237ABB4991F4D4127409DFE56199E41D2D4FB654B44FCFD2CC293574E

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: sk_key
Value: 21EC3DCD7CCDE44E3E8309A8EB21AB161D239F53E961D2D850F0A2C61ABCC72B68F255CDAA980757CDF704068AB5D0B2513945A65100B033DFDD1CCC95B84BCC2CCD5215EF30662F643401FC2B820833EF326B4258187496

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: 0_key
Value: 271E3C6EEED34F5B46C096C489E20C2A9CC4B2858D789C762C8AEB06B9D254527E2FBF66CFB2E30E46AA5E5E7666062C6F59A838194BB96EAC89EDCB7E7A7F312947A5497A464669702156826EAA5FBA1CD04149DCA6BC6B

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: rnd_ext
Value: .9m32i

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: stat
Value: 0F83496322982F82C26DC318E5E6A25B8A54348343F70518B1A469E95A33E127CE450B8E57DADA32E9A6ACC8866D6221FA5182EC8855E1DE9C64CB5B73BC40439BB800ED8B75A3EC0680A4BE093AAC28890EA45961454333877EE1F12EA89A3D6B74315E105FDEA4B496CAC8FCCFED854CFDE3CD292403CD0300758412E4040A38063555D133D7AE168F73829163C935E0A99371BEB3CA0BC596604CC363F04580529A0764ED08DA60C9F7C5007A0E04F9437F1922CC99DCEB2FA514A8A555C4BCD33E5B35DA0F7361F5D08117B4CE3A1AE5AB6C19563610C9A6D825C468A1D664D15578030F588A4744AEFBD4E202E5C7C1E10A7ACA260CE303FA6A45435B5C90F0C04300564745E9CC613CC09A8CD7A3FEAB597734F4F0D70F3EF6DD671A3D00ABE6D9959E69749FFAA5DE5E42F6E9C0B6C7746D114CD4021AE823896EF360A1533F48FD7C8F6E9E23E10A9C808C29F9D23626D38755F73F7F6686DC772161686848D065BA3AAB3263ED966ACFB624A607D8EBE8218F19CE25183D71FAB28151D66B9056C81F31694052C6C0EDC044A596CA6FB56FEAD8287AFF5C32C629A7C64E543DCE21BEC4EE32D862B783AF4A26BF0BD33298865A2FD7B5832928332B554F76EDA9EC8ABA6FF78A8AE2E048A4C373EF9E3C8FF58F81B20CE350C8CA0AFCA9EA62D2AC7BED7B567BB0DE582BA340BE72E5914ACCBC68F2839285C5381D8516240F3617B6CA3E0D228636C855BE81C8BAAD20C3B179EFDC4888F676D3BA19C66EB2033CFC383A7897FF75CFA9C21851DDD1F23AF639E00CDD0032C6F1829DD25C8D40457E653811CCDA38F0966362724616A1C3DA320E4FB735DCA468F4F8B1B26B6293E65FAAD690440D5D86DF509C825DE1EED6D454F66A361F2D75922BC2983D67BD82115D22FCB47C66756F0888F262B938D0E1912D1CFD059919DB8209B30D6E04AA487FB68FAF8527973CAF700CCC89514EED7D31D1CF3B08DEAE32ECF3ABD6C47B1BC183EB35629D8C13ED2FE7B26312A99A8E05E955AAC86C9AE8E4E1653ED6F05C1E4092AC67430640783A65DEA121E4EE4B20BB2FAEF067E7CBADA69284EF6D02DBACCCBF4E22E92096B981C3E463E6691AF10F2DCA499C43C6D8A634DBBF94F06B916D377D323B5A768CD3EAA1C324A1D32BE3AADCA380FB0A8F9FDF13D6734AD04B6CC0DB7090A1B25DB64484314AC26C7149117C74C42B238E7086D5E5

Previous 1 2 Next 10

Files activity

Add for printing

Executable files	Suspicious files	Text files	Unknown types
0	263	1	4

Dropped files

PID	Process	Filename	Type
1632	some_malicious_file.bin.exe	C:\recovery\345b46fe-a9f9-11e7-a83c-e8a4f72b1d33\Winre.wim MD5: — SHA256: —	—
1632	some_malicious_file.bin.exe	C:\Recovery\345b46fe-a9f9-11e7-a83c-e8a4f72b1d33\Winre.wim.9m32i MD5: — SHA256: —	—
1632	some_malicious_file.bin.exe	C:\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\admin\.oracle_jre_usage\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\recovery\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\program files\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\administrator\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\admin\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\recovery\345b46fe-a9f9-11e7-a83c-e8a4f72b1d33\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary

Download PCAP, analyze network streams, HTTP content and a lot more at the full report

Previous 1 2 3 4 5 6 7 ... 28 Next 10

Network activity

Add for printing

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	4	4	0

HTTP requests

No HTTP requests

Download PCAP, analyze network streams, HTTP content and a lot more at the full report

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1632	some_malicious_file.bin.exe	50.87.136.52:443	craftingalegacy.com	Unified Layer	US	suspicious
1632	some_malicious_file.bin.exe	78.46.1.42:443	g2mediainc.com	Hetzner Online GmbH	DE	suspicious
1632	some_malicious_file.bin.exe	104.21.87.185:443	vipcarrental.ae	Cloudflare Inc	US	suspicious
1632	some_malicious_file.bin.exe	134.119.253.108:443	brinkdoepke.eu	Host Europe GmbH	DE	suspicious

DNS requests

Domain	IP	Reputation
craftingalegacy.com	50.87.136.52	suspicious
g2mediainc.com	78.46.1.42	suspicious
brinkdoepke.eu	134.119.253.108	suspicious
vipcarrental.ae	104.21.87.185 172.67.145.154	malicious

Threats

No threats detected

Debug output strings

Add for printing

No debug info

General Info

Add for printing

File name: some_malicious_file.bin
Full analysis: https://app.any.run/tasks/a66178de-7596-4a05-945d-704dbf6b3b90
Verdict: Suspicious activity
Threats: Sodinokibi

Sodinokibi, also called Revil, is dangerous ransomware-type malware. Among other tools, it uses advanced encryption techniques and can operate without connection to control servers. Sodinokibi is among the most complex Ransomware in the world.

Malware Trends Tracker >>>

Analysis date: August 06, 2021, 08:57:08
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags: ransomware sodinokibi

Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	890A58F200DFFF23165DF9E1B088E58F
SHA1:	74E3D82F7EE81109E150DC41112CF95B3A4B5307
SHA256:	5F56D5748940E4039053F85978074BDE16D64BD5BA97F6F0026BA8172CB29E93
SSDEEP:	3072:Hp5SexkWi1LbI4eTMlwDCnu/q2GB96W/y:JvGWwbnWJ/yB9

Software environment set and analysis options

Behavior activities

Add for printing

MALICIOUS

Sodinokibi keys found
- some_malicious_file.bin.exe (PID: 1632)

Deletes shadow copies
- cmd.exe (PID: 448)

Starts BCDEDIT.EXE to disable recovery
- cmd.exe (PID: 448)

Sodinokibi ransom note found
- some_malicious_file.bin.exe (PID: 1632)

Renames files like Ransomware
- some_malicious_file.bin.exe (PID: 1632)

SUSPICIOUS

Checks supported languages
- some_malicious_file.bin.exe (PID: 1632)
- cmd.exe (PID: 448)
- some_malicious_file.bin.exe (PID: 2256)

Application launched itself
- some_malicious_file.bin.exe (PID: 2256)

Starts CMD.EXE for commands execution
- some_malicious_file.bin.exe (PID: 1632)

Reads the computer name
- some_malicious_file.bin.exe (PID: 2256)
- some_malicious_file.bin.exe (PID: 1632)

Executed as Windows Service
- vssvc.exe (PID: 2196)

Reads Environment values
- some_malicious_file.bin.exe (PID: 1632)

Creates files in the program directory
- some_malicious_file.bin.exe (PID: 1632)

Creates files like Ransomware instruction
- some_malicious_file.bin.exe (PID: 1632)

INFO

Checks supported languages
- vssadmin.exe (PID: 412)
- vssvc.exe (PID: 2196)
- bcdedit.exe (PID: 3140)
- bcdedit.exe (PID: 2940)

Reads the computer name
- vssadmin.exe (PID: 412)
- vssvc.exe (PID: 2196)

Dropped object may contain TOR URL's
- some_malicious_file.bin.exe (PID: 1632)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

Malware configuration

Add for printing

No Malware configuration.

Static information

Add for printing

TRiD

.exe	|	Win32 Executable MS Visual C++ (generic) (42.2)
.exe	|	Win64 Executable (generic) (37.3)
.dll	|	Win32 Dynamic Link Library (generic) (8.8)
.exe	|	Win32 Executable (generic) (6)
.exe	|	Generic Win/DOS Executable (2.7)

EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2019:06:10 17:29:32+02:00
PEType:	PE32
LinkerVersion:	14
CodeSize:	41984
InitializedDataSize:	122368
UninitializedDataSize:	0
EntryPoint:	0x36e6
OSVersion:	5.1
ImageVersion:	0
SubsystemVersion:	5.1
Subsystem:	Windows GUI

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	10-Jun-2019 15:29:32

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x000000D0

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	5
Time date stamp:	10-Jun-2019 15:29:32
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x0000A2D4	0x0000A400	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.55748
.rdata	0x0000C000	0x0000F650	0x0000F800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	6.43997
.data	0x0001C000	0x0000179C	0x00001600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.68881
.s7bz	0x0001E000	0x0000C800	0x0000C800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	5.09537
.reloc	0x0002B000	0x0000054C	0x00000600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	6.21532

Video and screenshots

Add for printing


All screenshots are available in the full report

All screenshots are available in the full report

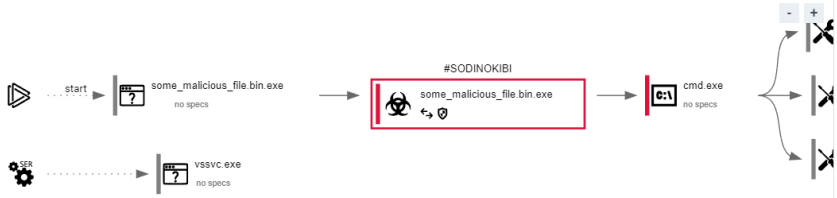
Processes

Add for printing

Total processes	Monitored processes	Malicious processes	Suspicious processes
47	7	2	0

Behavior graph

Click at the process to see the details



Specs description

Process information

PID	CMD	Path	Indicators	Parent process
2256	"C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe"	C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe	–	Explorer.EXE

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

Modules

Images

- c:\users\admin\appdata\local\temp\some_malicious_file.bin.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\user32.dll
- c:\windows\system32\gdi32.dll
- c:\windows\system32\lpk.dll
- c:\windows\system32\usp10.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\imm32.dll

Previous 1 2 3 4 5 6 Next

1632	"C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe"	C:\Users\admin\AppData\Local\Temp\some_malicious_file.bin.exe		some_malicious_file.bin.exe

Information

User: admin Integrity Level: HIGH

Modules

Images

- c:\users\admin\appdata\local\temp\some_malicious_file.bin.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\user32.dll
- c:\windows\system32\gdi32.dll
- c:\windows\system32\lpk.dll
- c:\windows\system32\usp10.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\imm32.dll

Previous 1 2 3 4 5 6 7 8 Next

448	"C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures	C:\Windows\System32\cmd.exe	–	some_malicious_file.bin.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: HIGH Description: Windows Command Processor

Exit code: 0 Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)

Modules

Images
c:\windows\system32\cmd.exe
c:\windows\system32\ntdll.dll
c:\windows\system32\kernel32.dll
c:\windows\system32\kernelbase.dll
c:\windows\system32\winbrand.dll
c:\windows\system32\msvcrt.dll
c:\windows\system32\user32.dll
c:\windows\system32\gdi32.dll
c:\windows\system32\lpk.dll
c:\windows\system32\usp10.dll

Previous 1 2 Next

412 vssadmin.exe Delete Shadows /All /Quiet C:\Windows\system32\vssadmin.exe – cmd.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: HIGH Description: Command Line Interface for Microsoft® Volume Shadow Copy Service
Exit code: 0 Version: 6.1.7600.16385 (win7_rtm.090713-1255)

Modules

Images
c:\windows\system32\vssadmin.exe
c:\windows\system32\ntdll.dll
c:\windows\system32\kernel32.dll
c:\windows\system32\kernelbase.dll
c:\windows\system32\advapi32.dll
c:\windows\system32\msvcrt.dll
c:\windows\system32\sechost.dll
c:\windows\system32\rpcrt4.dll
c:\windows\system32\atl.dll
c:\windows\system32\user32.dll

Previous 1 2 3 Next

2196 C:\Windows\system32\vssvc.exe C:\Windows\system32\vssvc.exe – services.exe

Information

User: SYSTEM Company: Microsoft Corporation
Integrity Level: SYSTEM Description: Microsoft® Volume Shadow Copy Service
Exit code: 0 Version: 6.1.7600.16385 (win7_rtm.090713-1255)

Modules

Images
c:\windows\system32\vssvc.exe
c:\windows\system32\ntdll.dll
c:\windows\system32\kernel32.dll
c:\windows\system32\kernelbase.dll
c:\windows\system32\advapi32.dll
c:\windows\system32\msvcrt.dll
c:\windows\system32\sechost.dll
c:\windows\system32\rpcrt4.dll
c:\windows\system32\user32.dll
c:\windows\system32\gdi32.dll

Previous 1 2 3 4 5 Next

3140 bcdedit /set {default} recoveryenabled No C:\Windows\system32\bcdedit.exe – cmd.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: HIGH Description: Boot Configuration Data Editor
Exit code: 0 Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)

Modules

Images
c:\windows\system32\bcdedit.exe
c:\windows\system32\ntdll.dll
c:\windows\system32\kernel32.dll
c:\windows\system32\kernelbase.dll
c:\windows\system32\msvcrt.dll
c:\windows\system32\advapi32.dll
c:\windows\system32\sechost.dll
c:\windows\system32\rpcrt4.dll

2940 bcdedit /set {default} bootstatuspolicy ignoreallfailures C:\Windows\system32\bcdedit.exe – cmd.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: HIGH Description: Boot Configuration Data Editor
Exit code: 0 Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)

Modules

Images
c:\windows\system32\bcdedit.exe
c:\windows\system32\kernel32.dll
c:\windows\system32\ntdll.dll

c:\windows\system32\msvcrt.dll

c:\windows\system32\advapi32.dll

c:\windows\system32\kernelbase.dll

c:\windows\system32\sechost.dll

c:\windows\system32\rpcrt4.dll

Registry activity

Add for printing

Total events	Read events	Write events	Delete events
1 298	1 274	24	0

Modification events

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: ProxyBypass
Value: 1

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: IntranetName
Value: 1

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: UNCAsIntranet
Value: 1

(PID) Process: (2256) some_malicious_file.bin.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: AutoDetect
Value: 0

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: sub_key
Value: D60DFF40440F390ED2DDF04B674C2FBBF07D35FA4B2EF7FC981CA8377A2BF44D

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: pk_key
Value: A054B93237ABB4991F4D4127409DFE56199E41D2D4FB654B44FCFD2CC293574E

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: sk_key
Value: 21EC3DCD7CCDE44E3E8309A8EB21AB161D239F53E961D2D850F0A2C61ABCC72B68F255CDAA980757CDF704068AB5D0B2513945A65100B033DFDD1CCC95B84BCC2CCD5215EF30662F643401FC2B820833EF326B4258187496

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: 0_key
Value: 271E3C6EEED34F5B46C096C489E20C2A9CC4B2858D789C762C8AEB06B9D254527E2FBF66CFB2E30E46AA5E5E7666062C6F59A838194BB96EAC89EDCB7E7A7F312947A5497A46466970215682 6EAA5FBA1CD04149DCA6BC6B

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: rnd_ext
Value: .9m32i

(PID) Process: (1632) some_malicious_file.bin.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\recfg
Operation: write Name: stat
Value: 0F83496322982F82C26DC318E5E6A25B8A54348343F70518B1A469E95A33E127CE450B8E57DADA32E9A6ACC8866D6221FA5182EC8855E1DE9C64CB5B73BC40439BB800ED8B75A3EC0680A4BE093AAC28890EA45961454333877EE1F12EA89A3D6B74315E105FDEA4B496CAC8FCCFED854CFDEE3CD292403CDD300758412E4040A3806355D133D7AE168F73829163C93E0A99371BEB3CA08C596604CC363F04580529A0764EDD8DA60C9F7C5007A00E04F9437F1922CC9DDCEB2FA514A8A555C4BCD33E5B35DA0F7361F5D08117B4CE3A1AE5AB6C19563610C9A6D825C46BA1D664D15578030F588A4744AEFBD4E202E5C7C1E10A7ACA260CE303FA6A45435B5C90F0C04300564745E9CC613CC09A8CD7A3FEAB59773F4F0D70F3EF6DD671A3D00ABE6D9959E6749FFAA5DE5E42F6E9C0B6C7746D114CD4021AE823896EF360A1533F48FD7C8F6E9E23E10A9CB08C29F9D23626D38755F73F7F5686DC772161686848D065BA3AAB3263ED966ACFB624A607D8EBE218F19CE25183D71FAB28151D668B9056C81F31694052C6C0EDC044A596CA6FB56FEAD8287AFF5C32C629A7C64E543DCE21BEC4EE32D862B783AF4A26BF0BD33298865A2FD7B5832928332B554F76EDA9EC8ABA6FF78A8AE2E048A4C373EF9E3C8FF58F81B20CE350C8CA0AFCA9EA62D2AC7BED7B567BB0DE582BA340BE72E5914ACCBC68F2839285C5381D851624DF3617B6CA3E0D228636C855BE81C8BAAD20C3B179EFDC4888F676D3BA19C86EB2033CFC383A7897FF75CFA9C21851DDD1F23AF633E00CDD0032C6F1829DD25C8D40457E653811CCDA38F096636724616A1C3DA320E4FB735DCA46BF4F8B1B26B6293E65FAAD6904405D86DF509C825DE1ED6D454F66A361F2D75922BC2983D67BD82115D22FCB47C66756F0888F262B938D0E1912D1CFD059919DB8209B3D06E04AA487FB68FAF8527973CAF700CCC895514EED731D1CF3B08DEAE32ECF3ABD6C47B1BC183EB35629D8C13ED2FE7B26312A99A8E05E955AAC86C9AEBE4E1653ED6F05C1E4092AC6743064078 3A65DEA121E4EE4B20BB2FAEF067E7CBADA69284EF6D02DBACCCBF4E22E92096B981C3E463E6691AF10F2DCA499C43C6D8A634DBBF94F06B916D377D323B5A768CD3EAA1C324A1D32BE3AADCA380FB0A8F9FDF13D6734AD04B6CC0DB7090A1B25DB64484314AC26C7149117C74C42B238E7086D5E5

Previous 1 2 Next 10

Files activity

Add for printing

Executable files	Suspicious files	Text files	Unknown types
0	263	1	4

Dropped files

PID	Process	Filename	Type
1632	some_malicious_file.bin.exe	C:\recovery\345b46fe-a9f9-11e7-a83c-e8a4f72b1d33\Winre.wim MD5: — SHA256: —	—
1632	some_malicious_file.bin.exe	C:\Recovery\345b46fe-a9f9-11e7-a83c-e8a4f72b1d33\Winre.wim.9m32i MD5: — SHA256: —	—
1632	some_malicious_file.bin.exe	C:\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\admin\.oracle_jre_usage\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\recovery\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\program files\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\administrator\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary
1632	some_malicious_file.bin.exe	C:\users\admin\9m32i-readme.txt MD5: 37395B5FFFEADB0246DF67B4CAA08F7D SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3	binary

1632	some_malicious_file.bin.exe	C:\recovery\345b46fe-a9f9-11e7-a83c-e8a4f72b1d33\9m32i-readme.txt	binary
		MD5: 37395B5FFFEADB0246DF67B4CAA08F7D	SHA256: 29A7964EC2E7F030A877BC7A7ECB9FFBAF232A9C13029B9714B62D6D69DB8BA3

Download PCAP, analyze network streams, HTTP content and a lot more at the full report

Previous 1 2 3 4 5 6 7 ... 28 Next 10

Network activity

Add for printing

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	4	4	0

HTTP requests

No HTTP requests

Download PCAP, analyze network streams, HTTP content and a lot more at the full report

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1632	some_malicious_file.bin.exe	50.87.136.52:443	craftingalegacy.com	Unified Layer	US	suspicious
1632	some_malicious_file.bin.exe	78.46.1.42:443	g2mediainc.com	Hetzner Online GmbH	DE	suspicious
1632	some_malicious_file.bin.exe	104.21.87.185:443	vipcarrental.ae	Cloudflare Inc	US	suspicious
1632	some_malicious_file.bin.exe	134.119.253.108:443	brinkdoepke.eu	Host Europe GmbH	DE	suspicious

DNS requests

Domain	IP	Reputation
craftingalegacy.com	50.87.136.52	suspicious
g2mediainc.com	78.46.1.42	suspicious
brinkdoepke.eu	134.119.253.108	suspicious
vipcarrental.ae	104.21.87.185 172.67.145.154	malicious

Threats

No threats detected

Debug output strings

Add for printing

No debug info