ID: 324352
Sample Name: javac.exe
Cookbook: default.jbs
Time: 13:49:28
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

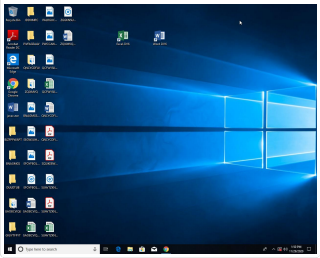
Analysis Report javac.exe

Overview

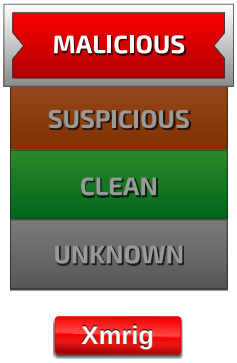
General Information

Sample Name:	javac.exe
Analysis ID:	324352
MD5:	bbf20caee8bfce4..
SHA1:	71a8569ce45770..
SHA256:	03100a76bca9d9..

Most interesting Screenshot:



Detection

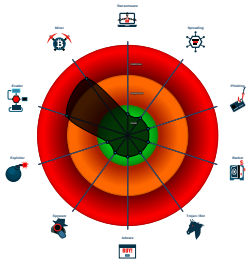


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Xmrig cryptocurrency…
- Found strings related to Crypto-Minin…
- Machine Learning detection for samp…
- Potential time zone aware malware
- Contains functionality to dynamically…
- PE file contains strange resources
- Program does not show much activi…
- Sample execution stops while proce…
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- javac.exe (PID: 6636 cmdline: 'C:\Users\user\Desktop\javac.exe' MD5: BBF20CAEE8BFCE48F883A65B779DEC71)
  - conhost.exe (PID: 6644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.203735977.00007FF755A51000.00000040.00020000.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
Process Memory Space: javac.exe PID: 6636	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	

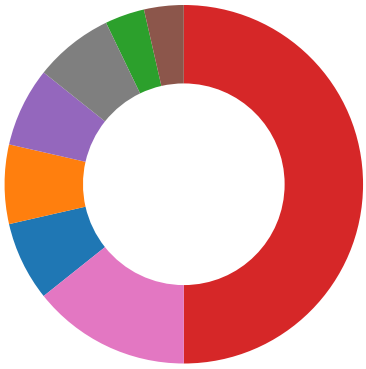
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.javac.exe.7ff755a50000.0.unpack	MAL_XMR_Miner_May19_1	Detects Monero Crypto Coin Miner	Florian Roth	• 0x37ee80:$x1: donate.ssl.xmrig.com • 0x37f2f1:$x2: * COMMANDS 'h' hashrate, 'p' pause, 'r' resume • 0x379ec8:$s1: [%s] login error code: %d
0.2.javac.exe.7ff755a50000.0.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Bitcoin Miner:

Yara detected Xmrig cryptocurrency miner

Found strings related to Crypto-Mining

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion:

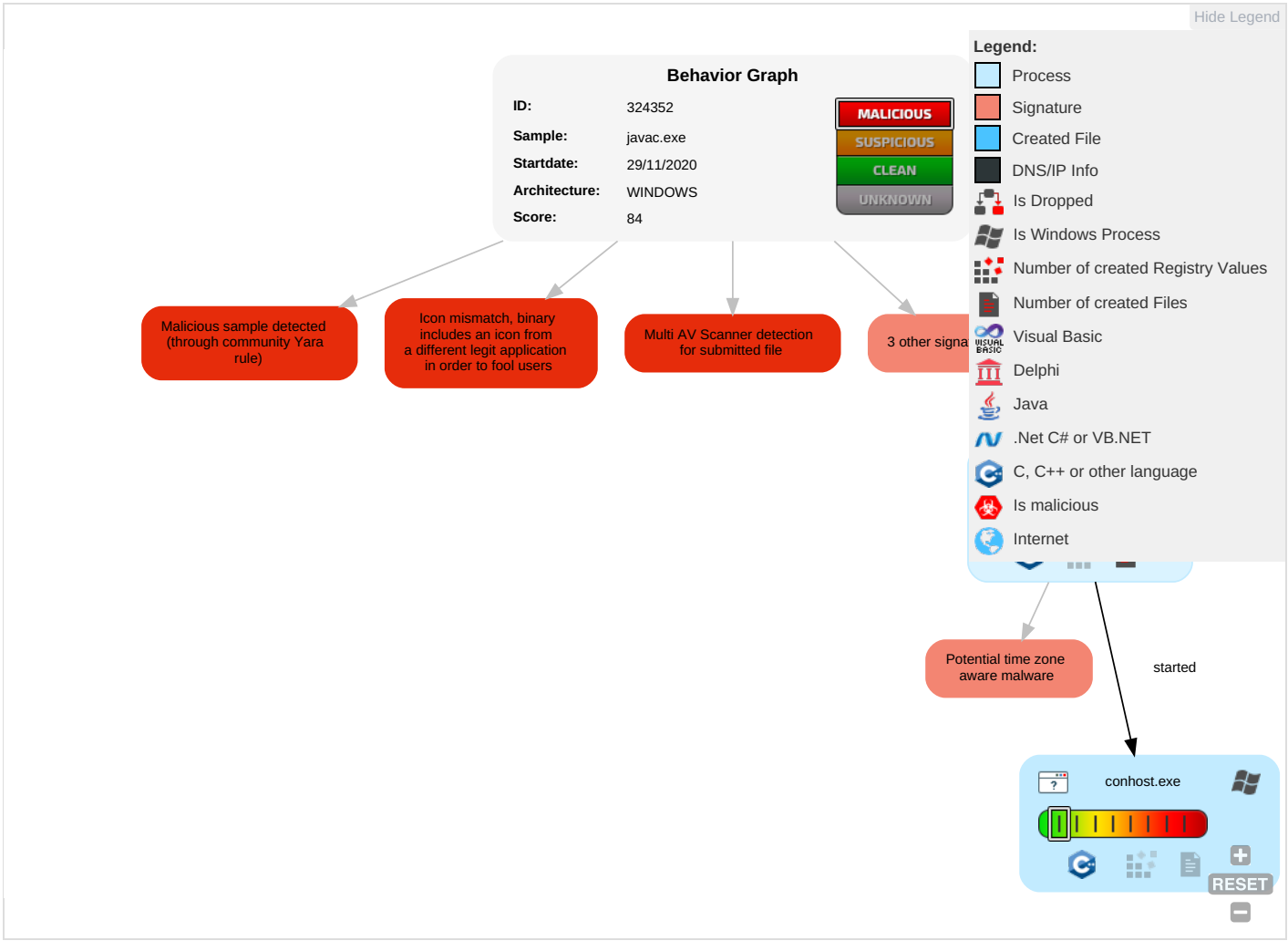
Potential time zone aware malware

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	Imp

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Imp
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mod Sys Par
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Dev Loc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Del Dev Dat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Car Billi Fra

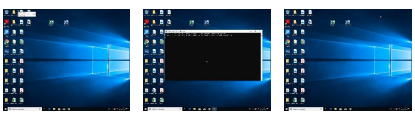
Behavior Graph



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
javac.exe	58%	Virustotal		Browse
javac.exe	22%	Metadefender		Browse
javac.exe	66%	ReversingLabs	Win64.Trojan.CoinMiner	
javac.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://xmrig.com/wizardSIGTERM	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://xmrig.com/wizard	0%	Virustotal		Browse
http://https://xmrig.com/wizard	0%	Avira URL Cloud	safe	
http://https://xmrig.com/docs/algorithms	0%	Virustotal		Browse
http://https://xmrig.com/docs/algorithms	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://xmrig.com/wizardSIGTERM	javac.exe, 00000000.00000002.203735977.00007FF755A51000.00000040.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://xmrig.com/wizard	javac.exe, 00000000.00000002.203688180.0000018E0D84B000.00000004.00000020.sdmp, javac.exe, 00000000.00000002.203707251.0000018E0D86D000.00000004.00000020.sdmp, ConDrv.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://xmrig.com/docs/algorithms	javac.exe, 00000000.00000002.203735977.00007FF755A51000.00000040.00020000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324352
Start date:	29.11.2020
Start time:	13:49:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	javac.exe
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:	2
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:	mal84.evad.mine.winEXE@2/1@0/0
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 100% (good quality ratio 25%) • Quality average: 14.5% • Quality standard deviation: 25.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

\Device\ConDrv	
Process:	C:\Users\user\Desktop\javac.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	168
Entropy (8bit):	5.252968524433859
Encrypted:	false
SSDEEP:	3:oVXVpxFBoXbTTOWXp5vGKLQCSKzcovo9VpxFBoW+pEJAFd8CQIMQDKeBJrXMXMIY:o9GnCWXpFG25zZvy4g6QIR/BJrXMnGTJ
MD5:	D581D2AA3DBA6FBE81A0145388397820
SHA1:	EE1778795109B01B46622B8E75E6A5C634B9F464
SHA-256:	A964F0660EA9448E758EBA4592569ACF43BADCF9E03FCD52FFE11CA41E4F138E
SHA-512:	EAD5E6CC543F284A0FF4297D9221A180718E2C37EE47E093D500EE7F373DC53E878CFCBFF6C5F4C64018EB96232A0453D0BC437EEAD839B3A41ACA776212D10
Malicious:	false
Reputation:	low
Preview:	[2020-11-29 13:50:15.943] unable to open "C:\Users\user\Desktop\config.json"....[2020-11-29 13:50:15.946] no valid configuration found, try https://xmrig.com/wizard...

Static File Info

General

File type:	PE32+ executable (console) x86-64, for MS Windows
Entropy (8bit):	7.822537418293464
TrID:	• Win64 Executable Console (202006/5) 81.26% • UPX compressed Win32 Executable (30571/9) 12.30% • Win64 Executable (generic) (12005/4) 4.83% • Generic Win/DOS Executable (2004/3) 0.81% • DOS Executable Generic (2002/1) 0.81%
File name:	javac.exe
File size:	1778688
MD5:	bbf20caee8bfce48f883a65b779dec71
SHA1:	71a8569ce4577016e1bc78eb27daab94ba6d9ce3
SHA256:	03100a76bca9d9ac984cccdf0cf7eef82bb2f1d20751538addc4405e35de4c00
SHA512:	6dc63993fb76fd526a86dd3d20516ab0f403d53e05057857ae9c93ff6c3320439becb40b3245e31c566d762df1a02e3fce515a1d813699b8338a3e7884a16d3d
SSDEEP:	24576:F0TMMpBJ1SFrJx/XIiJJVBfe0hsCI6ZEdNnsnCAjgysZyyIvbHY5V018c:FyMwBJcfTJznsCdErnFAjjyIvbHT8
File Content Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....g...g...g.....g.....g.....9g..m....g.....g.....g.....gg..0....g.....g...g...f..v....e..0...%g..0....g..0....g.

File Icon

Icon Hash:	1080888c8c828010

Static PE Info

General

Entrypoint:	0x14077a2b0
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5ED9180E [Thu Jun 4 15:49:34 2020 UTC]
TLS Callbacks:	0x4077a561, 0x1
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	49f1a89d440efc2bee91781377805550

Entrypoint Preview

Instruction
push ebx
push esi
push edi
push ebp
dec eax
lea esi, dword ptr [FFE78D45h]
dec eax

Instruction
lea edi, dword ptr [esi-005F2000h]
dec eax
lea eax, dword ptr [edi+00683648h]
push dword ptr [eax]
mov dword ptr [eax], D412B057h
push eax
push edi
xor ebx, ebx
xor ecx, ecx
dec eax
or ebp, FFFFFFFFh
call 00007FF5508FB795h
add ebx, ebx
je 00007FF5508FB744h
rep ret
mov ebx, dword ptr [esi]
dec eax
sub esi, FFFFFFFCh
adc ebx, ebx
mov dl, byte ptr [esi]
rep ret
dec eax
lea eax, dword ptr [edi+ebp]
cmp ecx, 05h
mov dl, byte ptr [eax]
jbe 00007FF5508FB763h
dec eax
cmp ebp, FFFFFFFCh
jnbe 00007FF5508FB75Dh
sub ecx, 04h
mov edx, dword ptr [eax]
dec eax
add eax, 04h
sub ecx, 04h
mov dword ptr [edi], edx
dec eax
lea edi, dword ptr [edi+04h]
jnc 00007FF5508FB731h
add ecx, 04h
mov dl, byte ptr [eax]
je 00007FF5508FB752h
dec eax
inc eax
mov byte ptr [edi], dl
sub ecx, 01h
mov dl, byte ptr [eax]
dec eax
lea edi, dword ptr [edi+01h]
jne 00007FF5508FB732h
rep ret
cld
inc ecx
pop ebx
jmp 00007FF5508FB74Ah
dec eax
inc esi
mov byte ptr [edi], dl
dec eax
inc edi
mov dl, byte ptr [esi]
add ebx, ebx
jne 00007FF5508FB74Ch
mov ebx, dword ptr [esi]
dec eax

Instruction
sub esi, FFFFFFFCh
adc ebx, ebx
mov dl, byte ptr [esi]
jc 00007FF5508FB728h
lea eax, dword ptr [ecx+01h]
jmp 00007FF5508FB749h
dec eax
inc ecx
call ebx
adc eax, eax
inc ecx
call ebx
adc eax, eax
add ebx, ebx
jne 00007FF5508FB74Ch
mov ebx, dword ptr [esi]
dec eax
sub esi, FFFFFFFCh
adc ebx, ebx
mov dl, byte ptr [esi]
jnc 00007FF5508FB726h
sub eax, 03h
jc 00007FF5508FB75Bh
shl eax, 08h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7a536c	0x2e0	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x77b000	0x2a36c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x71a000	0x1e558	UPX1
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7a564c	0x20	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x77a588	0x28	UPX1
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x77a5e8	0x130	UPX1
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	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x5f2000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x5f3000	0x188000	0x187800	False	0.982420627794	data	7.93362082097	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x77b000	0x2b000	0x2a800	False	0.144870174632	data	4.51391620298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x77b2b4	0x242e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x77d6e8	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x78df14	0x94a8	data	English	United States
RT_ICON	0x7973c0	0x5488	data	English	United States
RT_ICON	0x79c84c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967183	English	United States
RT_ICON	0x7a0a78	0x25a8	data	English	United States
RT_ICON	0x7a3024	0x10a8	data	English	United States
RT_ICON	0x7a40d0	0x988	data	English	United States
RT_ICON	0x7a4a5c	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_GROUP_ICON	0x7a4ec8	0x84	data	English	United States
RT_VERSION	0x7a4f50	0x298	data	English	United States
RT_MANIFEST	0x7a51ec	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
ADVAPI32.dll	LsaClose
bcrypt.dll	BCryptGenRandom
CRYPT32.dll	CertOpenStore
IPHLPAPI.DLL	GetAdaptersAddresses
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect
PSAPI.DLL	GetProcessMemoryInfo
SHELL32.dll	SHGetSpecialFolderPathA
USER32.dll	ShowWindow
USERENV.dll	GetUserProfileDirectoryW
WS2_32.dll	send

Version Infos

Description	Data
LegalCopyright	Copyright (C) 2016-2020 microsoft.com
FileVersion	5.10.0
CompanyName	www.microsoft.com
ProductName	svchost
ProductVersion	5.10.0
FileDescription	svchost
OriginalFilename	xmrig.exe
Translation	0x0000 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

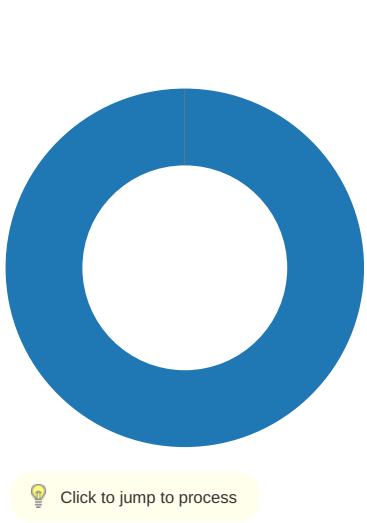
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: javac.exe PID: 6636 Parent PID: 5744

General

Start time:	13:50:15
Start date:	29/11/2020
Path:	C:\Users\user\Desktop\javac.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\javac.exe'
Imagebase:	0x7ff755a50000
File size:	1778688 bytes
MD5 hash:	BBF20CAEE8BFCE48F883A65B779DEC71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000000.00000002.203735977.00007FF755A51000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	81	5b 32 30 32 30 2d 31 31 2d 32 39 20 31 33 3a 35 30 3a 31 35 2e 39 34 33 5d 20 75 6e 61 62 6c 65 20 74 6f 20 6f 70 65 6e 20 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 63 6f 6e 66 69 67 2e 6a 73 6f 6e 22 2e 0d 0a	[2020-11-29 13:50:15.943] unable to open "C:\Users\user\Desktop\config.json"....	success or wait	1	7FF755D0D8A1	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	87	5b 32 30 32 30 2d 31 31 2d 32 39 20 31 33 3a 35 30 3a 31 35 2e 39 34 36 5d 20 6e 6f 20 76 61 6c 69 64 20 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 66 6f 75 6e 64 2c 20 74 72 79 20 68 74 74 70 73 3a 2f 2f 78 6d 72 69 67 2e 63 6f 6d 2f 77 69 7a 61 72 64 0d 0d 0a	[2020-11-29 13:50:15.946] no valid configuration found, try https://xmrig.com/wizard...	success or wait	1	7FF755D0D8A1	WriteFile

Analysis Process: conhost.exe PID: 6644 Parent PID: 6636

General

Start time:	13:50:15
Start date:	29/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis