ID: 764040
Sample Name:
HHGHJJUILn.exe
Cookbook: default.jbs
Time: 10:56:11
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

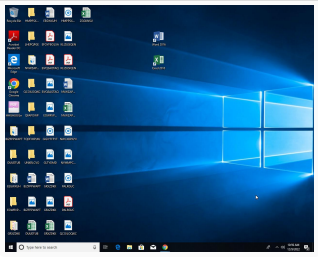
Windows Analysis Report

HHGHJJUILn.exe

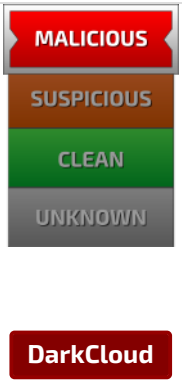
Overview

General Information

Sample Name:	HHGHJJUILn.exe
Analysis ID:	764040
MD5:	103f2ca898f5c72..
SHA1:	aded75bc932ddb..
SHA256:	10633d83edea23.
Tags:	exe
Infos:	



Detection



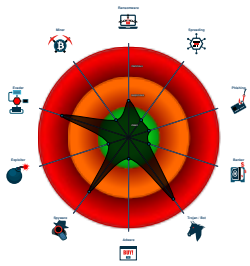
DarkCloud

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

Signatures

- Yara detected DarkCloud
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Writes to foreign memory regions
- Detected potential unwanted applica…
- Tries to steal Crypto Currency Walle…
- Writes or reads registry keys via WMI
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- May check the online IP address of…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- HHGHJJUILn.exe (PID: 5460 cmdline: C:\Users\user\Desktop\HHGHJJUILn.exe MD5: 103F2CA898F5C7285A3651F23D926218)
  - vbc.exe (PID: 5168 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - vbc.exe (PID: 5140 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - vbc.exe (PID: 5132 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - vbc.exe (PID: 4772 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.246767038.0000000000401000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
00000000.00000002.251576631.00000252D012D000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
Process Memory Space: HHGHJJUILn.exe PID: 5460	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x212b6:$s2: AAAAAAAAAAoVT • 0x19769f:$s2: AAAAAAAAAAoVT • 0x2af0d0:$s2: AAAAAAAAAAoVT
Process Memory Space: HHGHJJUILn.exe PID: 5460	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: vbc.exe PID: 4772	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.HHGHJJUILn.exe.252d0175a70.4.unpack	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
0.2.HHGHJJUILn.exe.252d0175a70.4.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x2f958:$s1: Temporary Directory * for • 0x2f994:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x31b98:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x2f940:$s7: CopyHere • 0x2f8fc:$s9: Shell.Application • 0x2fca0:$s9: shell.application • 0x31d0c:$s10: SetRequestHeader • 0x2fa3c:$s12: @TITLE Removing • 0x2fa74:$s13: @RD /S /Q "
0.2.HHGHJJUILn.exe.252d012dbe0.3.unpack	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
0.2.HHGHJJUILn.exe.252d012dbe0.3.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x77b0:$s1: Temporary Directory * for • 0x77ec:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x99f0:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x7798:$s7: CopyHere • 0x7754:$s9: Shell.Application • 0x7af8:$s9: shell.application • 0x9b64:$s10: SetRequestHeader • 0x7894:$s12: @TITLE Removing • 0x78cc:$s13: @RD /S /Q "
4.0.vbc.exe.400000.0.unpack	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Machine Learning detection for sample

Networking

May check the online IP address of the machine

System Summary

Malicious sample detected (through community Yara rule)

Detected potential unwanted application

Writes or reads registry keys via WMI

.NET source code contains very large strings

Data Obfuscation

.NET source code contains potential unpacker

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

Boot Survival

Drops PE files to the user root directory

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected DarkCloud

Yara detected Telegram RAT

Tries to steal Crypto Currency Wallets

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

Yara detected DarkCloud

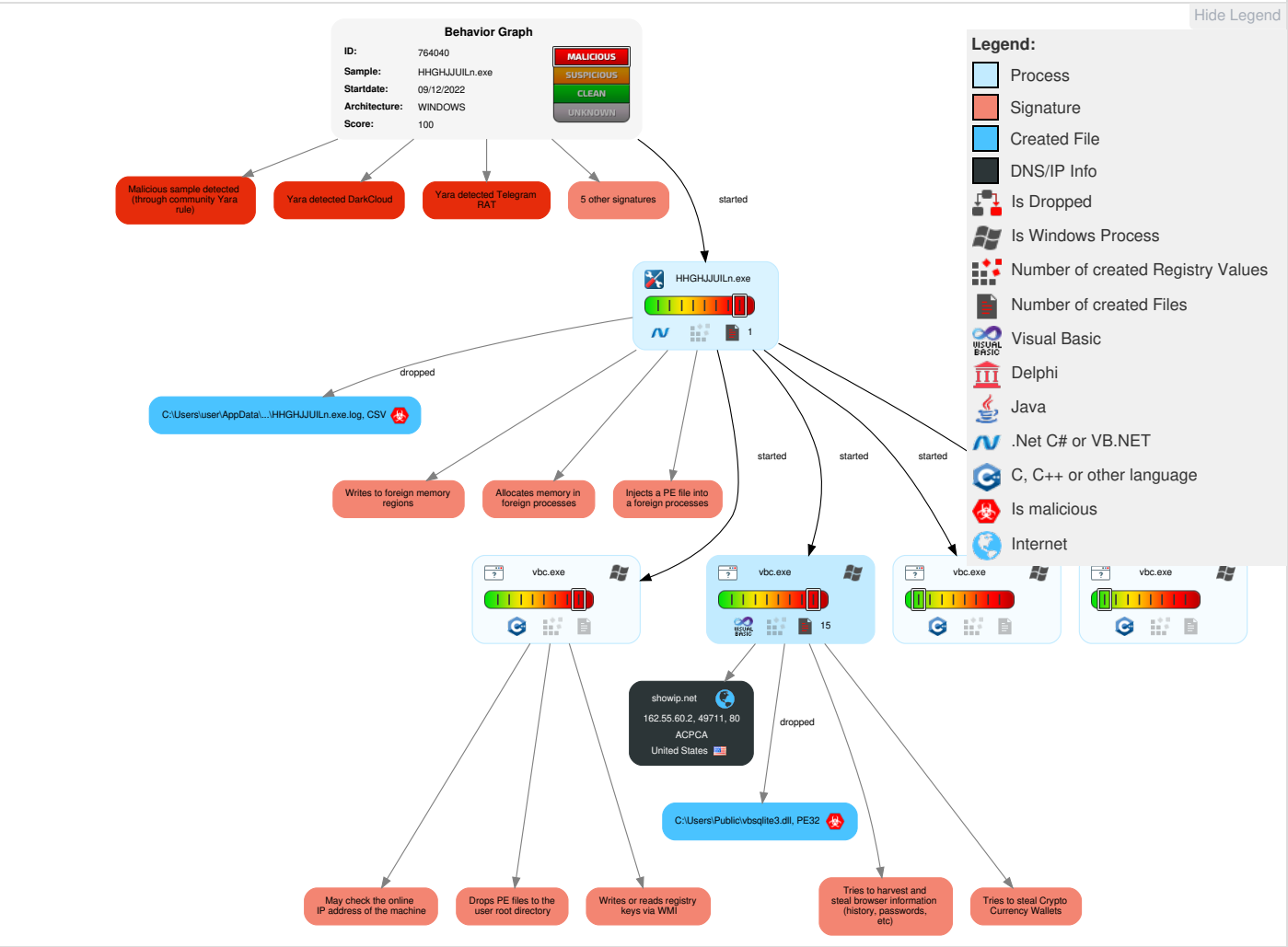
Yara detected Telegram RAT

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	1 Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 1 1 Masquerading	1 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Network Configuration Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 2 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Timestomp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
HHGHJJUILn.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbsqlite3.dll	0%	ReversingLabs		
C:\Users\Public\vbsqlite3.dll	1%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.3.vbc.exe.502d8d0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.HHGHJJUILn.exe.252d012dbe0.3.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.HHGHJJUILn.exe.252d0175a70.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.vbc.exe.502d8d0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
showip.net	162.55.60.2	true	false		high

Contacted URLs

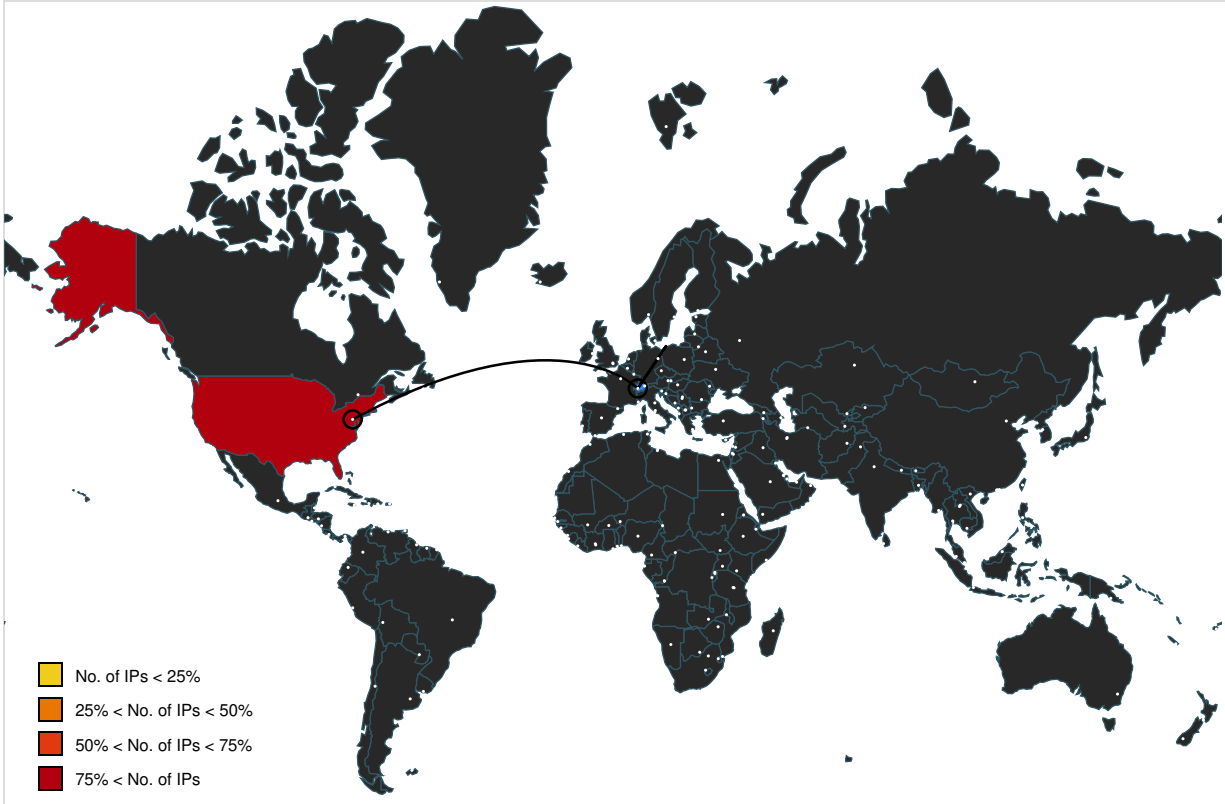
Name	Malicious	Antivirus Detection	Reputation
http://showip.net/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama.4.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	vbc.exe, 00000004.00000003.272068154.00000000050B9000.00000004.00000020.00020000.00000000.sdmp, LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama.4.dr	false		high
http://https://duckduckgo.com/chrome_newtab	vbc.exe, 00000004.00000003.272068154.00000000050B9000.00000004.00000020.00020000.00000000.sdmp, LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama.4.dr	false		high
http://schema.org	vbc.exe, 00000004.00000003.271857889.0000000005087000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000003.271870029.000000000507C000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000003.271831148.0000000005090000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama.4.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	vbc.exe, 00000004.00000003.272068154.00000000050B9000.00000004.00000020.00020000.00000000.sdmp, LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama.4.dr	false		high
http://https://api.telegram.org/bot	HHGHJJUILn.exe, 00000000.00000002.251576631.00000252D012D000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000004.00000000.246767038.0000000000401000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://showip.net/	vbc.exe, 00000004.00000003.271857889.0000000005087000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000003.271870029.000000000507C000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000003.271831148.0000000005090000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.openstreetmap.org/copyright	vbc.exe, 00000004.00000003.271857889.000 0000005087000.00000004.00000020.00020000 .00000000.sdmp, vbc.exe, 00000004.000000 03.281674526.0000000005085000.00000004.0 0000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000003.271870029.00000000050 7C000.00000004.00000020.00020000.0000000 0.sdmp, vbc.exe, 00000004.00000003.27237 1184.0000000005085000.00000004.00000020. 00020000.00000000.sdmp, vbc.exe, 0000000 4.00000003.271831148.0000000005090000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://unpkg.com/leaflet	vbc.exe, 00000004.00000003.271831148.000 0000005090000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	vbc.exe, 00000004.00000003.272068154.000 00000050B9000.00000004.00000020.00020000 .00000000.sdmp, LogvangVfuSkfsNcHkxYKVGc fUjjBLLTgabama.4.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama.4.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	vbc.exe, 00000004.00000003.272068154.000 00000050B9000.00000004.00000020.00020000 .00000000.sdmp, LogvangVfuSkfsNcHkxYKVGc fUjjBLLTgabama.4.dr	false		high
http://www.maxmind.com	vbc.exe, 00000004.00000003.271831148.000 0000005090000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://showip.net/?checkip=	vbc.exe, 00000004.00000003.271857889.000 0000005087000.00000004.00000020.00020000 .00000000.sdmp, vbc.exe, 00000004.000000 03.271870029.000000000507C000.00000004.0 0000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000003.271831148.00000000050 90000.00000004.00000020.00020000.0000000 0.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama.4.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	vbc.exe, 00000004.00000003.272068154.000 00000050B9000.00000004.00000020.00020000 .00000000.sdmp, LogvangVfuSkfsNcHkxYKVGc fUjjBLLTgabama.4.dr	false		high

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
162.55.60.2	showip.net	United States		35893	ACPCA	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764040
Start date and time:	2022-12-09 10:56:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HHGHJJUILn.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:	15
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:	mal100.troj.spyw.evad.winEXE@9/3@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 49.2% (good quality ratio 42.7%) • Quality average: 61.9% • Quality standard deviation: 37.1%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- 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

Time	Type	Description
10:57:25	API Interceptor	1x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\vbsqlite3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	165376
Entropy (8bit):	7.894371604278017
Encrypted:	false
SSDEEP:	3072:eNFwdmspaPg9g9oOavAQBNrPkVdc88GjU+vF6nuxRocX5GOOUleo+c:e8d1/w5KA81IJ8GpF6nuTmOOU
MD5:	073A17B6CFB1112C6C838B2FBA06A657
SHA1:	A54BB22489EAA8C52EB3E512AEE522320530B0BE
SHA-256:	DCFCD16FBF0511D3F2B3792E5493FA22D7291E4BB2EFBFA5ADE5002A04FC2CAB
SHA-512:	5BC8307350BD8BA09FA9EEDDDC62F1DBA65DB62EB09AE64E0ADFF4DFAD0937DBEC5B621F294F5980BF77033FAAC3BFE200945C0280606915EE9A82D34A003B9E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F..p.~.#.~.#.~.#.,!#.~.#.,'#.~.#%..#.~.#.~.#]~.#.,6#.~.#.,1#.~.#.,#.~.#.,&#.~.#.,##.~.#Rich.~.#.....PE..L.....H.....!.....p... .....e.....p.....@.....t..D....r..(....p.....\..... ...g..H.....UPX0.....UPX1.....p.....h.....@....rsrc.... ...p.....I.....@..... ....3.03.UPX!....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\HHGHJJUILn.exe.log

Process:	C:\Users\user\Desktop\HHGHJJUILn.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZiIv:Q3La/KDLI4MWuPTxAIv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

C:\Users\user\AppData\Roaming\A8EC33334FD0FF0355\LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944
MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D5
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.29079911305477
TrID:	• Win64 Executable GUI Net Framework (217006/5) 47.53% • Win64 Executable GUI (202006/5) 44.25% • Win64 Executable (generic) Net Framework (21505/4) 4.71% • Win64 Executable (generic) (12005/4) 2.63% • Generic Win/DOS Executable (2004/3) 0.44%
File name:	HHGHJJUILn.exe
File size:	1631776
MD5:	103f2ca898f5c7285a3651f23d926218
SHA1:	aded75bc932ddb0c9b17f257f82a5be822cab8e6
SHA256:	10633d83edea2308a01d9bcbd507737bf66e93550be49239cd801257f79c7d37
SHA512:	19e9732bd86ca29458d3575db2940c14d33266e6d43fad80523a14a47f2eeaf8a6919534509ece55829a4dbeac269c0f6fafa831665af150b9dcee779d3c500a
SSDEEP:	12288:nGrB8Ut5pnAYxJsBDrYPL32PWfDyVan2bAESn97ahY9ceFl/t7tH8rxnaj2/e/PD:GrBi8rxnajdM2th9VYy
TLSH:	9475BC2A38BA010DB361AD9C6BBCB175910EF7F2163A5C774DF7060A25139F0CB9D626
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....)w..... ....@..... .....K....`.....

File Icon

Icon Hash:	92aca8b2b2a2b286

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xBC772981 [Thu Mar 13 08:46:57 2070 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=DigiCert High Assurance Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/29/2013 5:00:00 PM 1/4/2017 4:00:00 AM
Subject Chain	• CN=Wen Jia Liu, O=Wen Jia Liu, L=Sydney, S=New South Wales, C=AU
Version:	3
Thumbprint MD5:	FB7AAB26B203432685FBC0FF17F24045
Thumbprint SHA-1:	32387AEC09EB287F202E98398189B460F4C61A0D
Thumbprint SHA-256:	E0E85619EEF45FCE4421E4BA581060E43BBBF25911CD757DD081DA425DD1DB51
Serial:	0FF1EF66BD621C65B74B4DE41425717F

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18e000	0x1bfa	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x18ac00	0x3a20	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x18a590	0x1c	.text
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	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

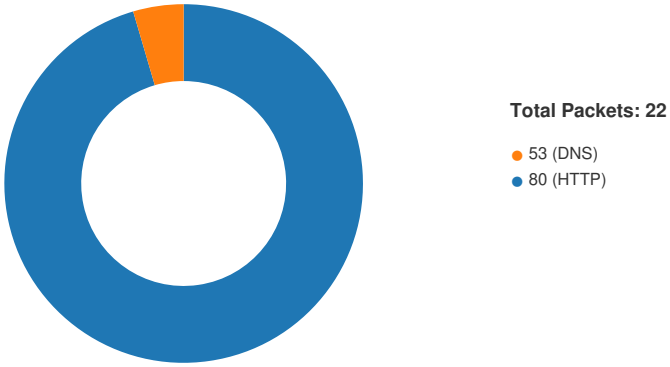
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x188634	0x188800	False	0.2850026124601911	data	4.209755910815595	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.sdata	0x18c000	0x1e8	0x200	False	0.857421875	data	6.638446248926509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x18e000	0x1bfa	0x1c00	False	0.3529575892857143	data	5.504563155253437	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x18e1b0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0x18f258	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0x18f6c0	0x22	data		
RT_VERSION	0x18f6e4	0x32c	data		
RT_MANIFEST	0x18fa10	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:15.916726112 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.940066099 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.940274954 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.942653894 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.964567900 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965302944 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965341091 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965367079 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965387106 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965396881 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965434074 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965460062 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965523005 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965547085 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965570927 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965576887 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965595007 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965595007 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965609074 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965615988 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965636015 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:15.965637922 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965660095 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:15.965668917 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:30.987771988 CET	80	49711	162.55.60.2	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:30.987884998 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:57:46.072297096 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:57:46.072392941 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:58:01.175959110 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:58:01.176172018 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:58:16.280128956 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:58:16.280333996 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:58:31.385688066 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:58:31.386337042 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:58:46.488641977 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:58:46.488744020 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:59:01.591901064 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:59:01.592098951 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:59:05.735914946 CET	49711	80	192.168.2.7	162.55.60.2
Dec 9, 2022 10:59:05.758949995 CET	80	49711	162.55.60.2	192.168.2.7
Dec 9, 2022 10:59:05.759134054 CET	49711	80	192.168.2.7	162.55.60.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:15.882508039 CET	50505	53	192.168.2.7	8.8.8.8
Dec 9, 2022 10:57:15.901057959 CET	53	50505	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 10:57:15.882508039 CET	192.168.2.7	8.8.8.8	0x51cb	Standard query (0)	showip.net	A (IP address)	IN (0x0001)	false

DNS Answers

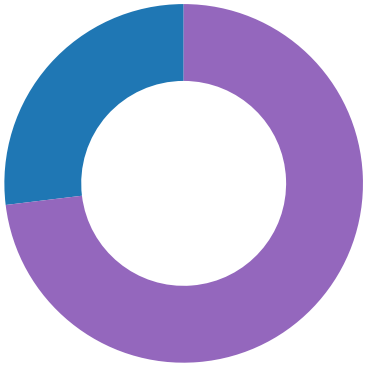
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 10:57:15.901057959 CET	8.8.8.8	192.168.2.7	0x51cb	No error (0)	showip.net		162.55.60.2	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- showip.net

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: HHGHJJUILn.exe PID: **5460**, Parent PID: **3320**

General

Target ID:	0
Start time:	10:57:07
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\HHGHJJUILn.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\HHGHJJUILn.exe
Imagebase:	0x252bdc30000
File size:	1631776 bytes
MD5 hash:	103F2CA898F5C7285A3651F23D926218
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DarkCloud, Description: Yara detected DarkCloud, Source: 00000000.00000002.251576631.00000252D012D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\HHGHJJUILn.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE283E86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\HHGHJJUILn.exe.log	0	226	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0	success or wait	1	7FFE283E8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE27E4B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE27E4B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE27E52625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFE27F212E7	ReadFile

Analysis Process: vbc.exe PID: **5168**, Parent PID: **5460**

General

Target ID:	1
Start time:	10:57:08
Start date:	09/12/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0x8c0000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: **5140**, Parent PID: **5460**

General

Target ID:	2
Start time:	10:57:08
Start date:	09/12/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0x8c0000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: **5132**, Parent PID: **5460**

General

Target ID:	3
Start time:	10:57:08
Start date:	09/12/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0x8c0000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: **4772**, Parent PID: **5460**

General

Target ID:	4
Start time:	10:57:09
Start date:	09/12/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0x8c0000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_DarkCloud, Description: Yara detected DarkCloud, Source: 00000004.00000000.246767038.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\vbsqlite3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA
C:\Users\user\AppData\Roaming\A8EC33334FD0FF0355	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	660ECD38	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43D56A	InternetOpenUrlA
C:\Users\user\AppData\Roaming\A8EC33334FD0FF0355\LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7063A6D2	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\A8EC33334FD0FF0355\LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama	success or wait	1	660ECD92	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbsqlite3.dll	0	165376	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 46 1f fd 70 02 7e fd 23 02 7e fd 23 02 7e fd 23 1c 2c 21 23 00 7e fd 23 1c 2c 27 23 09 7e fd 23 25 fd fd 23 05 7e fd 23 02 7e fd 23 5d 7e fd 23 1c 2c 36 23 01 7e fd 23 1c 2c 31 23 0d 7e fd 23 1c 2c 20 23 03 7e fd 23 1c 2c 26 23 03 7e fd 23 1c 2c 23 23 03 7e fd 23 52 69 63 68 02 7e fd 23 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0b 07 fd 48 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$Fp~#~#~#,!#~#, '#~#%#~#~#]~#,6#~#,1# ~#, #~#,& #~#,##~#Rich~#PELH	success or wait	1	660ED8F8	WriteFile
C:\Users\user\AppData\Roaming\A8EC33334FD0FF0355\LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	7063A6D2	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\A8EC33334FD0FF0355\LogvangVfuSkfsNcHkxYKVGcfUjjBLLTgabama	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	7063A6D2	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly