ID: 756309
Sample Name: OMHGCG.exe
Cookbook: default.jbs
Time: 00:44:09
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

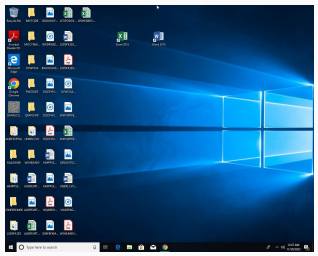
Windows Analysis Report

OMHGCG.exe

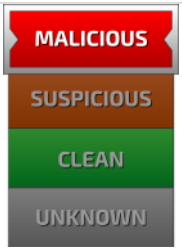
Overview

General Information

Sample Name:	OMHGCG.exe
Analysis ID:	756309
MD5:	fae47086c34007..
SHA1:	00caba8b2c7d23..
SHA256:	00973673a54cfd..
Tags:	exe LodaRat
Infos:	



Detection



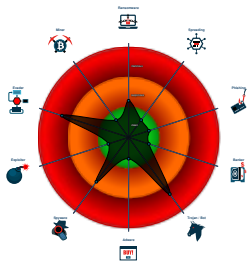
LodaRAT

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected LodaRAT
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Uses schtasks.exe or at.exe to add…
- Uses dynamic DNS services
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- OMHGCG.exe (PID: 3460 cmdline: C:\Users\user\Desktop\OMHGCG.exe MD5: FAE47086C34007307F6E2CD0C47A97D8)
  - cmd.exe (PID: 3100 cmdline: C:\Windows\system32\cmd.exe /c schtasks /create /tn ZFZRCN.exe /tr C:\Users\user\AppData\Roaming\Windata\update.exe /sc minute /mo 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2136 cmdline: schtasks /create /tn ZFZRCN.exe /tr C:\Users\user\AppData\Roaming\Windata\update.exe /sc minute /mo 1 MD5: 15FF7D8324231381BAD48A052F85DF04)
- update.exe (PID: 4124 cmdline: C:\Users\user\AppData\Roaming\Windata\update.exe MD5: FAE47086C34007307F6E2CD0C47A97D8)
- update.exe (PID: 5112 cmdline: "C:\Users\user\AppData\Roaming\Windata\update.exe" MD5: FAE47086C34007307F6E2CD0C47A97D8)
- update.exe (PID: 676 cmdline: "C:\Users\user\AppData\Roaming\Windata\update.exe" MD5: FAE47086C34007307F6E2CD0C47A97D8)
- update.exe (PID: 588 cmdline: "C:\Users\user\AppData\Roaming\Windata\update.exe" MD5: FAE47086C34007307F6E2CD0C47A97D8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: OMHGCG.exe PID: 3460	JoeSecurity_LodaRAT	Yara detected LodaRAT	Joe Security	
Process Memory Space: OMHGCG.exe PID: 3460	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: update.exe PID: 4124	JoeSecurity_LodaRAT	Yara detected LodaRAT	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
Process Memory Space: update.exe PID: 4124	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: update.exe PID: 5112	JoeSecurity_LodaRAT	Yara detected LodaRAT	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

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Networking

Uses dynamic DNS services

Data Obfuscation

Detected unpacking (changes PE section rights)

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Stealing of Sensitive Information

Yara detected LodaRAT

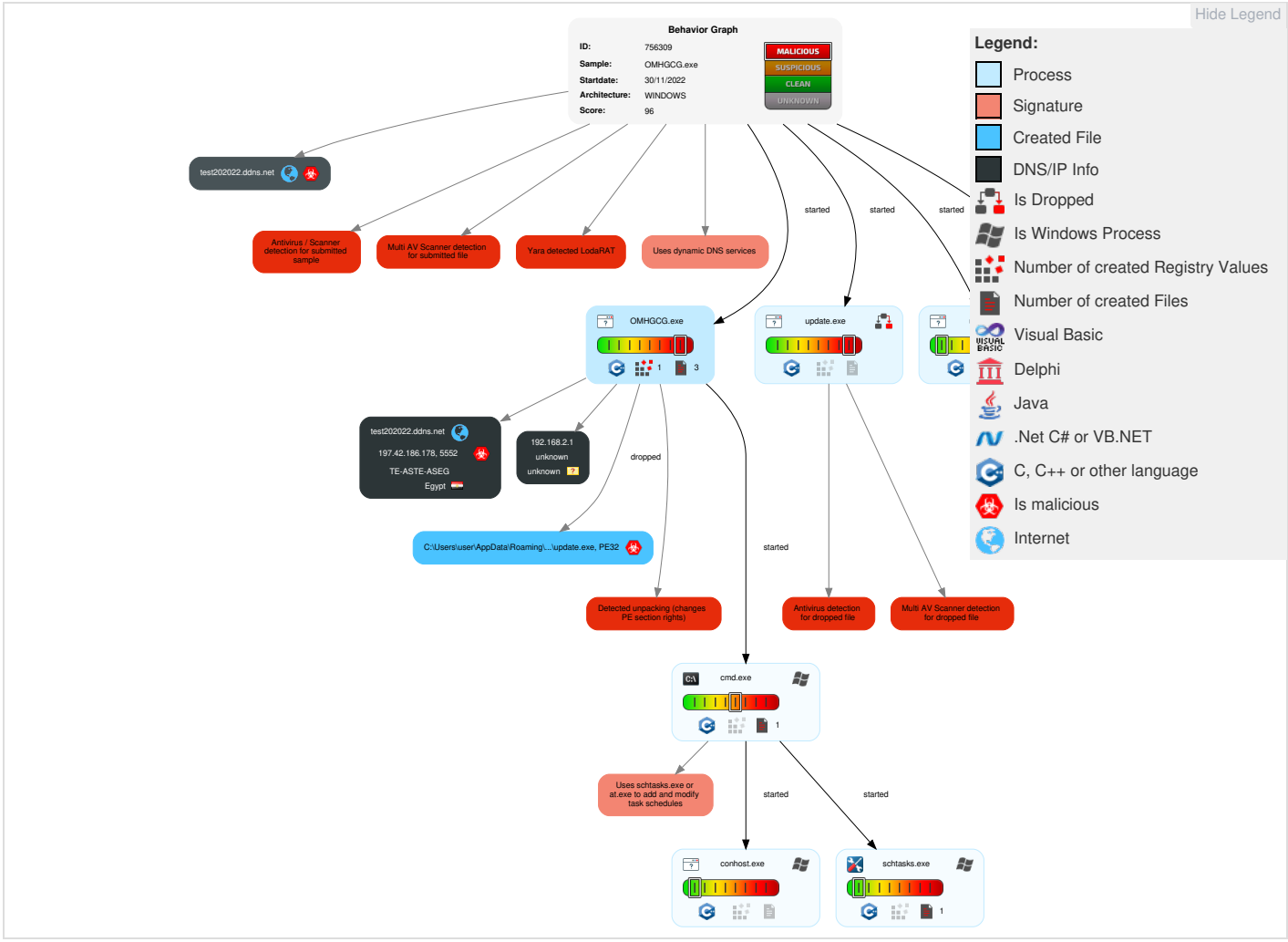
Remote Access Functionality

Yara detected LodaRAT

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
2 Valid Accounts	1 Windows Management Instrumentation	2 Valid Accounts	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	3 1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Native API	1 Scheduled Task/Job	2 Valid Accounts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	3 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	2 1 Registry Run Keys / Startup Folder	2 1 Access Token Manipulation	3 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 2 Process Injection	1 1 Software Packing	NTDS	1 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Scheduled Task/Job	1 Masquerading	LSA Secrets	1 4 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	2 1 Registry Run Keys / Startup Folder	2 Valid Accounts	Cached Domain Credentials	2 Virtualization/Sandbox Evasion	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 Virtualization/Sandbox Evasion	DCSync	3 Process Discovery	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	2 1 Access Token Manipulation	Proc Filesystem	1 1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 2 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

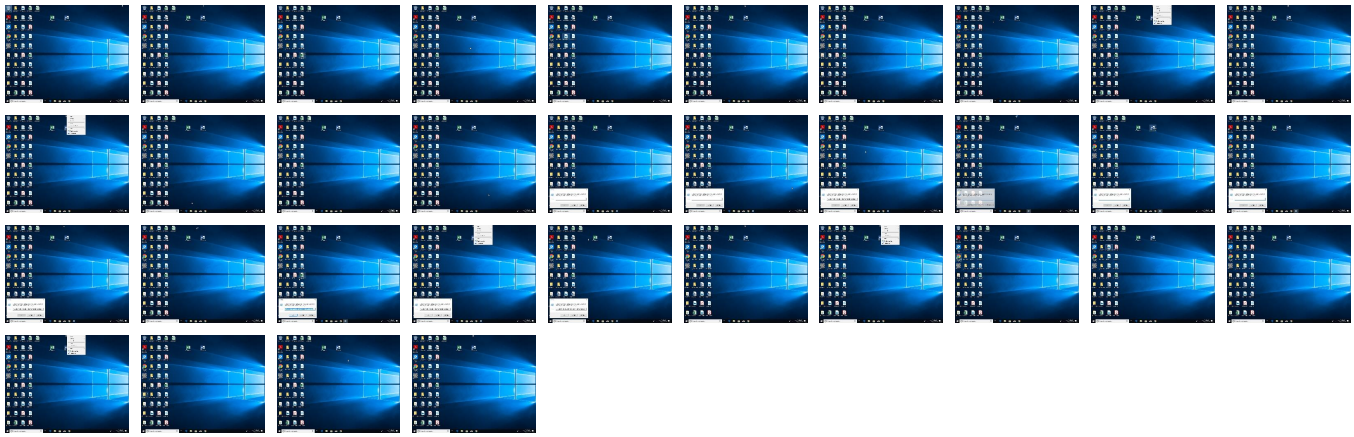
Behavior Graph



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
OMHGCG.exe	75%	ReversingLabs	Win32.Backdoor.LoadaRat	
OMHGCG.exe	56%	Virustotal		Browse
OMHGCG.exe	100%	Avira	HEUR/AGEN.1215448	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Windata\update.exe	100%	Avira	HEUR/AGEN.1215448	
C:\Users\user\AppData\Roaming\Windata\update.exe	75%	ReversingLabs	Win32.Backdoor.LoadaRat	
C:\Users\user\AppData\Roaming\Windata\update.exe	56%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230522		Download File
15.2.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230522		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
18.2.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230522		Download File
13.0.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230747		Download File
14.0.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230747		Download File
18.0.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230747		Download File
0.0.OMHGCG.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230747		Download File
13.2.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230522		Download File
15.0.update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230747		Download File
0.2.OMHGCG.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230522		Download File

Domains

Source	Detection	Scanner	Label	Link
test202022.ddns.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

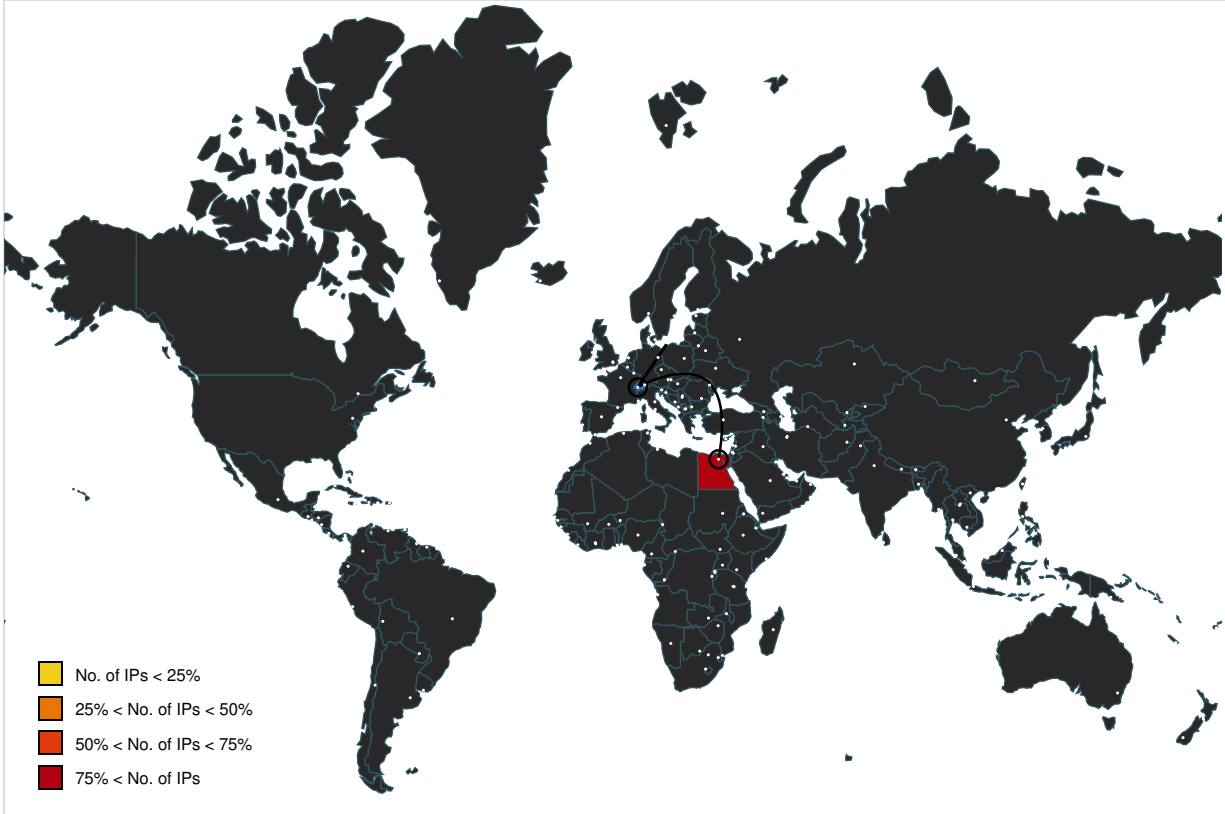
Name	IP	Active	Malicious	Antivirus Detection	Reputation
test202022.ddns.net	197.42.186.178	true	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/files/beta/autoit/archive/sqlite/SQLite3	OMHGCG.exe, 00000000.00000002.514752018.00000000040C6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.autoitscript.com/autoit3/files/beta/autoit/archive/sqlite/SQLite3%%	update.exe, 0000000D.00000003.475219101.0000000003D0F000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000D.00000003.475148079.0000000003D09000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000D.00000002.478947115.0000000003D12000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.493084290.0000000003CDC000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491837776.0000000003CD4000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491729664.0000000003CCC000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491878276.0000000003CD9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://checkip.amazonaws.com/D	update.exe, 0000000E.00000003.491908903.0000000003CA7000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491857087.0000000003CA0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.autoitscript.com/autoit3/files/beta/autoit/archive/sqlite/SQLite3GK	update.exe, 0000000F.00000002.514401378.0000000003DA0000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ip-score.com/checkip/	OMHGCG.exe, 00000000.00000002.513500694.0000000003F40000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000D.00000003.477067833.0000000003B9B000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.492835145.0000000003B69000.00000004.00000800.00020000.00000000.sdmp, update.exe, 00000012.00000002.513247187.0000000003B00000.00000004.00000800.00020000.00000000.sdmp	false		high
http://checkip.amazonaws.com/	OMHGCG.exe, 00000000.00000002.514343033.000000000404A000.00000004.00000800.00020000.00000000.sdmp, OMHGCG.exe, 00000000.00000002.515666003.00000000041DC000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000D.00000002.478932417.0000000003CFE000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000D.00000003.475182772.0000000003CF7000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491301522.0000000003DEE000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491570140.0000000003DF7000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491376732.0000000003DEF000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000002.494453244.0000000003DF7000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000E.00000003.491443893.0000000003DF7000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000F.00000002.515363500.0000000003ED7000.00000004.00000800.00020000.00000000.sdmp, update.exe, 0000000F.00000002.514337061.0000000003D8B000.00000004.00000800.00020000.00000000.sdmp, update.exe, 00000012.00000002.515327441.0000000003D9A000.00000004.00000800.00020000.00000000.sdmp, update.exe, 00000012.00000002.514281424.0000000003C53000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.autoitscript.com/autoit3/files/beta/autoit/archive/sqlite/SQLite3D	update.exe, 00000012.00000002.514281424.0000000003C53000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.42.186.178	test202022.ddns.net	Egypt		8452	TE-ASTE-ASEG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756309
Start date and time:	2022-11-30 00:44:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OMHGCG.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:	19
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:	mal96.troj.evad.winEXE@10/2@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 39% (good quality ratio 36.4%) • Quality average: 78.6% • Quality standard deviation: 29.4%
HCA Information:	• Successful, ratio: 96% • 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, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsp.digicert.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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
00:45:55	Task Scheduler	Run new task: ZFZRCN.exe path: C:\Users\user\AppData\Roaming\Windata\update.exe

Time	Type	Description
00:45:58	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ZFZRCN "C:\Users\user\AppData\Roaming\Windata\update.exe"
00:46:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ZFZRCN "C:\Users\user\AppData\Roaming\Windata\update.exe"
00:46:15	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ZFZRCN.lnk

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\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ZFZRCN.lnk

Process:	C:\Users\user\Desktop\OMHGCG.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Icon number=4, Archive, ctime=Wed Nov 30 07:45:52 2022, mtime=Wed Nov 30 07:45:53 2022, atime=Wed Nov 30 07:45:53 2022, length=808241, window=hide
Category:	dropped
Size (bytes):	1805
Entropy (8bit):	3.4195022525575456
Encrypted:	false
SSDEEP:	24:8ygGZ269og0e+99MN+AqbtE2+s9T4Ilz4MgCMGm:8ygGs69j0X9MFe9r9MIlg4
MD5:	C50C4CE22B18FE22B2A0A28684091135
SHA1:	C3F03BB947554CD05A2275AF8688355F3BCF93ED
SHA-256:	1E1A4E8FCB9D420A6EE765E6CEA8B088B073676D0B529C4787C181973DB84F7A
SHA-512:	8A17806F59058F49354E3F7087E5446214010F5691DCD3393D3850A083C0A80CCD1EAAD876AEB02382CF2DF155858A4BC660443051AE3DA298C4C4C6DD39D73
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...Sv.'.....a.'.....a.'....1U.....:..DG..Yr?.D..U..k0.&...&.....-..=.Z.....'.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny.~U.E.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny.~U.E.....Y.....D1,.R.o.a.m.i.n.g.....V.1.....~U.E..Windata.@.....~U.E~U.E.....W.....N#..W.i.n.d.a.t.a.....`.2.1U..~U.E .update.exe..F.....~U.E~U.E.....z.....u.p.d.a.t.e...e.x.e.....`.....-....._.....\h.....C:\Users\user\AppData\Roaming\Windata\update.exe..!.....\.....\.....\.....\.....\.....\.W.i.n.d.a.t.a.\.u.p.d.a.t.e...e.x.e.).".C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.W.i.n.d.a.t.a.\."...C.:.\.W.i.n.d.o.w.s.\.S.y.s.W.O.W.6.4.\.s.h.e.l.l.3.2...d.l.l.....%SystemRoot%\SysWOW64\shell32.dll.....

C:\Users\user\AppData\Roaming\Windata\update.exe

Process:	C:\Users\user\Desktop\OMHGCG.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	808241

Entropy (8bit):	7.961034418901167
Encrypted:	false
SSDEEP:	24576:CaGph/owsamHkWmY9LTJX6x/XcT7O3O3rozC:SOw+Hkc9LTasT7OebN
MD5:	FAE47086C34007307F6E2CD0C47A97D8
SHA1:	00CABA8B2C7D23A2ACC78F54155DB976D902F2C4
SHA-256:	00973673A54CFD2A206C7695FA86077D1A1803629D7207B1E5FB295255A25AE2
SHA-512:	5A113874D5DCFB4CA3CE47C50027C01505586B9B0FE033243707A4F4CCE13A7638FF697B958B64E086A28F5489231BF113F7E0393737D5CD2F70CD0D0E8BA80
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 75% • Antivirus: Virustotal, Detection: 56%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q.....y.....i.....}...N.....d.....`.....m.....g... .Rich.....PE..L....%O.....#.....p.....P.....`.....@.....@.....@.....~..... .....aHc.....P.....Security.p...`...I.....@....rsrc.....p.....@..... ....3.96.UPX!....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.961034418901167
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	OMHGCG.exe
File size:	808241
MD5:	fae47086c34007307f6e2cd0c47a97d8
SHA1:	00caba8b2c7d23a2acc78f54155db976d902f2c4
SHA256:	00973673a54cfd2a206c7695fa86077d1a1803629d7207b1e5fb295255a25ae2
SHA512:	5a113874d5dcfb4ca3ce47c50027c01505586b9b0fe033243707a4f4cce13a7638ff697b958b64e086a28f5489231bf113f7e0393737d5cd2f70cd0d0e8ba80b
SSDEEP:	24576:CaGph/owsamHkWmY9LTJX6x/XcT7O3O3rozC:SOw+Hkc9LTasT7OebN
TLSH:	4F0523898E8C4239DE5804B95A616880C4233FF70725EBA45E0A51F53EF7BB4FD4E293
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.).....Q.....y.....i.....}....N.....d.....`.....m.....g.....Rich.....PE..L..

File Icon

Icon Hash:	569fd2978684d563

Static PE Info

General

Entrypoint:	0x4bc980
Entrypoint Section:	Security
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4F25BAEC [Sun Jan 29 21:32:28 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0

Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	05fc725b9ed37e995841bfab7c978eef

Entrypoint Preview
Instruction
pushad
mov esi, 00476000h
lea edi, dword ptr [esi-00075000h]
push edi
or ebp, FFFFFFFFh
jmp 00007F204CE5B242h
nop
nop
nop
nop
nop
nop
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
add ebx, ebx
jne 00007F204CE5B239h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F204CE5B21Fh
mov eax, 00000001h
add ebx, ebx
jne 00007F204CE5B239h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
add ebx, ebx
jnc 00007F204CE5B23Dh
jne 00007F204CE5B25Ah
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F204CE5B251h
dec eax
add ebx, ebx
jne 00007F204CE5B239h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
jmp 00007F204CE5B206h
add ebx, ebx
jne 00007F204CE5B239h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
jmp 00007F204CE5B284h
xor ecx, ecx
sub eax, 03h
jc 00007F204CE5B243h

Instruction
shl eax, 08h
mov al, byte ptr [esi]
inc esi
xor eax, FFFFFFFFh
je 00007F204CE5B2A7h
sar eax, 1
mov ebp, eax
jmp 00007F204CE5B23Dh
add ebx, ebx
jne 00007F204CE5B239h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F204CE5B1FEh
inc ecx
add ebx, ebx
jne 00007F204CE5B239h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F204CE5B1F0h
add ebx, ebx
jne 00007F204CE5B239h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jnc 00007F204CE5B221h
jne 00007F204CE5B23Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F204CE5B216h
add ecx, 02h
cmp ebp, FFFFFB00h
adc ecx, 02h
lea edx, dword ptr [eax+eax]

Rich Headers

Programming Language:	• [C] VS2010 SP1 build 40219 • [C++] VS2010 SP1 build 40219 • [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [ASM] VS2010 SP1 build 40219 • [RES] VS2010 SP1 build 40219 • [LNK] VS2010 SP1 build 40219

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc7ee8	0x38c	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbd000	0xaee8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
aHc	0x1000	0x75000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
Security	0x76000	0x47000	0x46c00	False	0.988615972835689	, Monaural	7.899875991527048	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xbd000	0xc000	0xb400	False	0.7865451388888889	data	6.6623772013775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbd44c	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128, 16 important colors	English	Great Britain
RT_ICON	0xbd578	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	Great Britain
RT_ICON	0xbd6a4	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	Great Britain
RT_ICON	0xbd7d0	0xa2a8	Device independent bitmap graphic, 100 x 200 x 32, image size 41600	English	Great Britain
RT_MENU	0xb5a68	0x50	data	English	Great Britain
RT_DIALOG	0xb5ab8	0xfc	data	English	Great Britain
RT_STRING	0xb5bb8	0x530	data	English	Great Britain
RT_STRING	0xb60e8	0x690	data	English	Great Britain
RT_STRING	0xb6778	0x4d0	data	English	Great Britain
RT_STRING	0xb6c48	0x5fc	data	English	Great Britain
RT_STRING	0xb7248	0x65c	data	English	Great Britain
RT_STRING	0xb78a8	0x388	data	English	Great Britain
RT_STRING	0xb7c30	0x158	data	English	United States
RT_GROUP_ICON	0xc7a7c	0x14	data	English	Great Britain
RT_GROUP_ICON	0xc7a94	0x14	data	English	Great Britain
RT_GROUP_ICON	0xc7aac	0x14	data	English	Great Britain
RT_GROUP_ICON	0xc7ac4	0x14	data	English	Great Britain
RT_VERSION	0xc7adc	0x19c	data	English	Great Britain
RT_MANIFEST	0xc7c7c	0x26c	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	GetAce
COMCTL32.dll	ImageList_Remove
COMDLG32.dll	GetSaveFileNameW
GDI32.dll	LineTo
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect
MPR.dll	WNetGetConnectionW
ole32.dll	CoInitialize
OLEAUT32.dll	VariantInit
PSAPI.DLL	EnumProcesses
SHELL32.dll	DragFinish
USER32.dll	GetDC

Copyright Joe Security LLC 2022

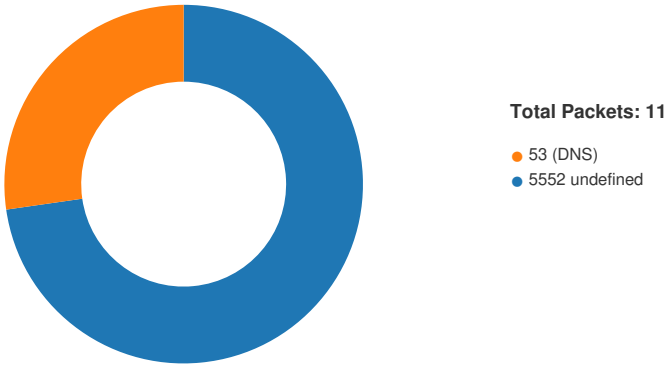
DLL	Import
USERENV.dll	LoadUserProfileW
VERSION.dll	VerQueryValueW
WININET.dll	FtpOpenFileW
WINMM.dll	timeGetTime
WSOCK32.dll	recv

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:46:03.792799950 CET	49701	5552	192.168.2.3	197.42.186.178
Nov 30, 2022 00:46:06.792308092 CET	49701	5552	192.168.2.3	197.42.186.178
Nov 30, 2022 00:46:12.808238983 CET	49701	5552	192.168.2.3	197.42.186.178
Nov 30, 2022 00:46:36.509052038 CET	49702	5552	192.168.2.3	197.42.186.178
Nov 30, 2022 00:46:39.513783932 CET	49702	5552	192.168.2.3	197.42.186.178
Nov 30, 2022 00:46:45.514239073 CET	49702	5552	192.168.2.3	197.42.186.178
Nov 30, 2022 00:47:06.796238899 CET	49703	5552	192.168.2.3	197.42.186.178
Nov 30, 2022 00:47:09.781981945 CET	49703	5552	192.168.2.3	197.42.186.178

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:46:03.749135971 CET	49977	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:46:03.769726992 CET	53	49977	8.8.8.8	192.168.2.3
Nov 30, 2022 00:46:35.337589025 CET	57840	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:46:35.359222889 CET	53	57840	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:47:06.775429010 CET	57990	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:47:06.794569969 CET	53	57990	8.8.8.8	192.168.2.3

DNS Queries

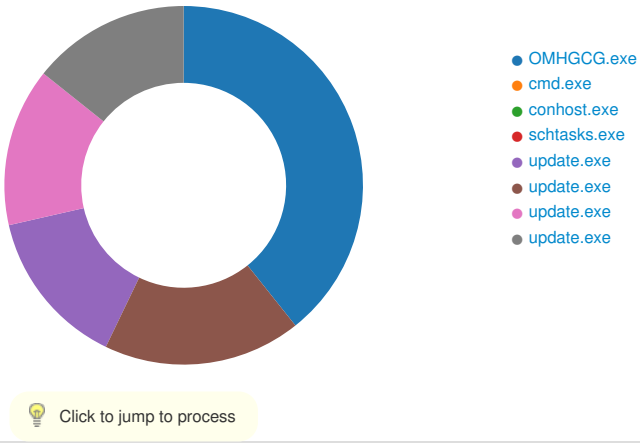
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:46:03.749135971 CET	192.168.2.3	8.8.8.8	0xc832	Standard query (0)	test202022 .ddns.net	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:46:35.337589025 CET	192.168.2.3	8.8.8.8	0xec01	Standard query (0)	test202022 .ddns.net	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:47:06.775429010 CET	192.168.2.3	8.8.8.8	0xf4f8	Standard query (0)	test202022 .ddns.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
Nov 30, 2022 00:46:03.769726992 CET	8.8.8.8	192.168.2.3	0xc832	No error (0)	test202022 .ddns.net		197.42.186.178	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:46:35.359222889 CET	8.8.8.8	192.168.2.3	0xec01	No error (0)	test202022 .ddns.net		197.42.186.178	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:47:06.794569969 CET	8.8.8.8	192.168.2.3	0xf4f8	No error (0)	test202022 .ddns.net		197.42.186.178	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: OMHGCG.exe PID: **3460**, Parent PID: **3452**

General

Target ID:	0
Start time:	00:45:02
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\OMHGCG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OMHGCG.exe

Copyright Joe Security LLC 2022

Imagebase:	0x400000
File size:	808241 bytes
MD5 hash:	FAE47086C34007307F6E2CD0C47A97D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	ZFZRCN	unicode	"C:\Users\user\AppData\Roaming\Windata\update.exe"	success or wait	1	46BC64	RegSetValueExW

Analysis Process: cmd.exe PID: **3100**, Parent PID: **3460**

General

Target ID:	10
Start time:	00:45:53
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c schtasks /create /tn ZFZRCN.exe /tr C:\Users\user\AppData\Roaming\Windata\update.exe /sc minute /mo 1
Imagebase:	0xb0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5304**, Parent PID: **3100**

General

Target ID:	11
Start time:	00:45:54
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **2136**, Parent PID: **3100**

General

Target ID:	12
Start time:	00:45:54
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /tn ZFZRCN.exe /tr C:\Users\user\AppData\Roaming\Windata\update.exe /sc minute /mo 1
Imagebase:	0x1170000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: update.exe PID: **4124**, Parent PID: **1080**

General

Target ID:	13
Start time:	00:45:56
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\Windata\update.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Windata\update.exe
Imagebase:	0x400000
File size:	808241 bytes
MD5 hash:	FAE47086C34007307F6E2CD0C47A97D8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 75%, ReversingLabs • Detection: 56%, Virustotal, Browse
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	6	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	4096	success or wait	1	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	6	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	471040	success or wait	1	41DC0F	ReadFile

Analysis Process: update.exe PID: **5112**, Parent PID: **3452**

General

Target ID:	14
Start time:	00:46:06
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\Windata\update.exe

Copyright Joe Security LLC 2022

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Windata\update.exe"
Imagebase:	0x400000
File size:	808241 bytes
MD5 hash:	FAE47086C34007307F6E2CD0C47A97D8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	6	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	4096	success or wait	1	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	5	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	512	success or wait	1	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	471040	success or wait	1	41DC0F	ReadFile

Analysis Process: update.exe PID: **676**, Parent PID: **3452**

General

Target ID:	15
Start time:	00:46:15
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\Windata\update.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Windata\update.exe"
Imagebase:	0x400000
File size:	808241 bytes
MD5 hash:	FAE47086C34007307F6E2CD0C47A97D8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	6	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	4096	success or wait	1	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	6	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	471040	success or wait	1	41DC0F	ReadFile

Analysis Process: update.exe PID: **588**, Parent PID: **3452**

General

Target ID:	18
Start time:	00:46:25
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\Windata\update.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Windata\update.exe"
Imagebase:	0x400000
File size:	808241 bytes

MD5 hash:	FAE47086C34007307F6E2CD0C47A97D8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	6	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	4096	success or wait	1	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	65536	success or wait	6	41DC0F	ReadFile
C:\Users\user\AppData\Roaming\Windata\update.exe	unknown	471040	success or wait	1	41DC0F	ReadFile

Disassembly

No disassembly