ID: 679249
Sample Name: HDPh51eN5s
Cookbook: default.jbs
Time: 13:13:10
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

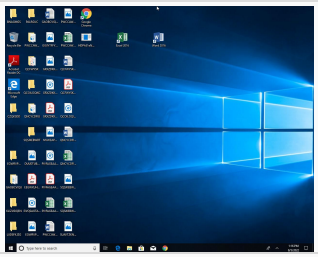
Windows Analysis Report

HDPh51eN5s

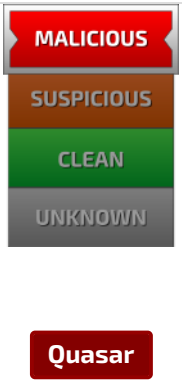
Overview

General Information

Sample Name:	HDPh51eN5s (renamed file extension from none to exe)
Analysis ID:	679249
MD5:	1fb5d967f92174e..
SHA1:	76fbd5b8815497..
SHA256:	740634ecedd318..
Tags:	exe
Infos:	



Detection

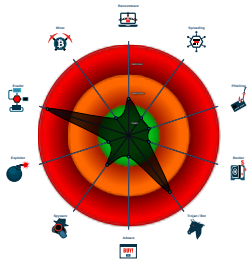


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Sigma detected: Schedule system p…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for drop…
- Yara detected Quasar RAT
- Connects to many ports of the same…
- Machine Learning detection for sam…
- Machine Learning detection for drop…
- Hides that the sample has been dow…
- Drops executables to the windows d…

Classification



Process Tree

- **System is w10x64**
- HDPh51eN5s.exe (PID: 4684 cmdline: "C:\Users\user\Desktop\HDPh51eN5s.exe" MD5: 1FB5D967F92174E0BBB15262F8CD209F)
  - schtasks.exe (PID: 2916 cmdline: "schtasks" /create /tn "Google Update" /sc ONLOGON /tr "C:\Users\user\Desktop\HDPh51eN5s.exe" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - MpCmdRun.exe (PID: 4276 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
        - conhost.exe (PID: 1320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RuntimeBroker.exe (PID: 5824 cmdline: C:\Windows\system32\Windows\RuntimeBroker.exe MD5: 1FB5D967F92174E0BBB15262F8CD209F)
    - schtasks.exe (PID: 6276 cmdline: "schtasks" /create /tn "Google Update" /sc ONLOGON /tr "C:\Windows\system32\Windows\RuntimeBroker.exe" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
      - conhost.exe (PID: 6328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- HDPh51eN5s.exe (PID: 6020 cmdline: C:\Users\user\Desktop\HDPh51eN5s.exe MD5: 1FB5D967F92174E0BBB15262F8CD209F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.401638486.0000000012E41000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
00000000.00000002.277374012.00000000134FA000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.251870111.000000001584C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
00000006.00000003.289424719.0000000015501000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
00000000.00000002.303504388.000000001C3E0000.00000004.08000000.00040000.00000000.sdmp	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x41b939:$x1: Quasar.Common.Messages • 0x41d00b:$x1: Quasar.Common.Messages
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.HDPh51eN5s.exe.1c3e0000.3.raw.unpack	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x41b939:$x1: Quasar.Common.Messages • 0x41d00b:$x1: Quasar.Common.Messages
0.2.HDPh51eN5s.exe.1c3e0000.3.raw.unpack	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
0.2.HDPh51eN5s.exe.1c3e0000.3.unpack	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x419d39:$x1: Quasar.Common.Messages • 0x41b40b:$x1: Quasar.Common.Messages
0.2.HDPh51eN5s.exe.1c3e0000.3.unpack	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Schedule system process

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Quasar RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Connects to many ports of the same IP (likely port scanning)

E-Banking Fraud

Yara detected Quasar RAT

System Summary

Malicious sample detected (through community Yara rule)

PE file contains section with special chars

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Stealing of Sensitive Information

Yara detected Quasar RAT

Remote Access Functionality

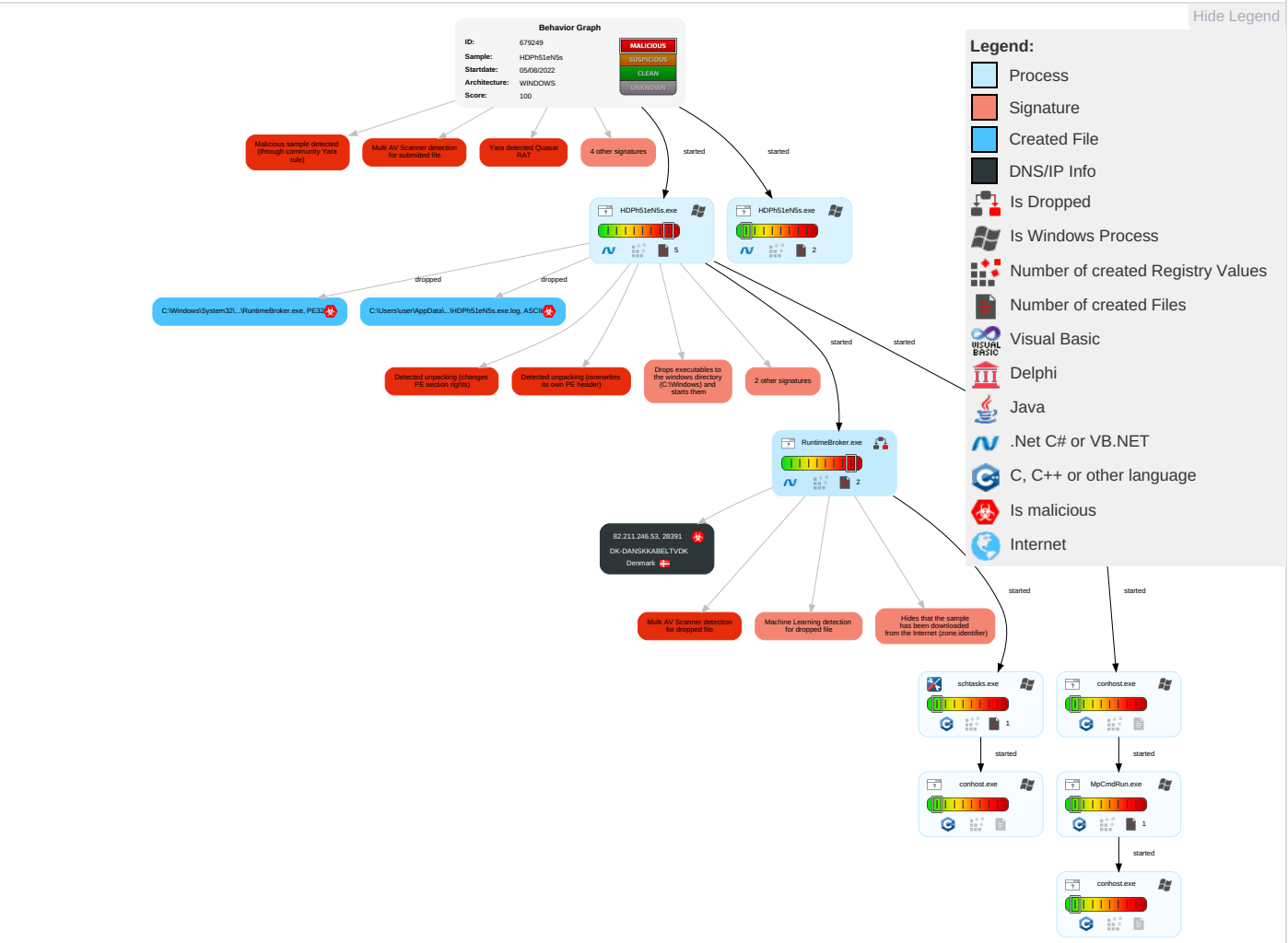
Yara detected Quasar RAT

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	1 Scheduled Task/Job	1 1 Process Injection	1 2 1 Masquerading	OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	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	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	3 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	Remote System 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	System Owner/User 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 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

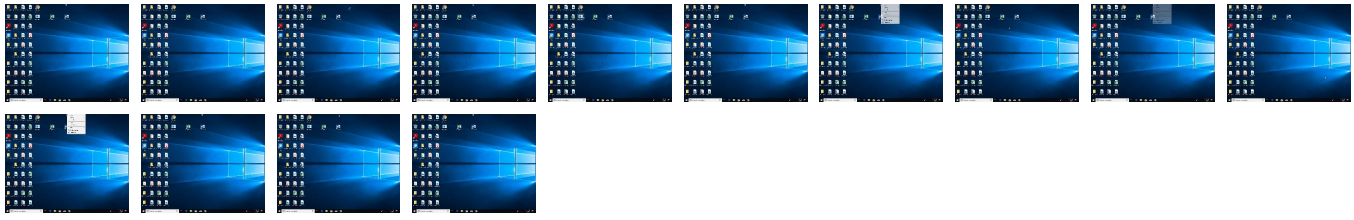
Behavior Graph



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
HDPh51eN5s.exe	36%	Virustotal		Browse
HDPh51eN5s.exe	31%	Metadefender		Browse
HDPh51eN5s.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.Perseus	
HDPh51eN5s.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\System32\Windows\RuntimeBroker.exe	100%	Joe Sandbox ML		
C:\Windows\System32\Windows\RuntimeBroker.exe	36%	Virustotal		Browse
C:\Windows\System32\Windows\RuntimeBroker.exe	31%	Metadefender		Browse
C:\Windows\System32\Windows\RuntimeBroker.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.Perseus	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.HDPh51eN5s.exe.ac0000.0.unpack	100%	Avira	HEUR/AGEN.1230577		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://go.michv	0%	Avira URL Cloud	safe	

Domains and IPs

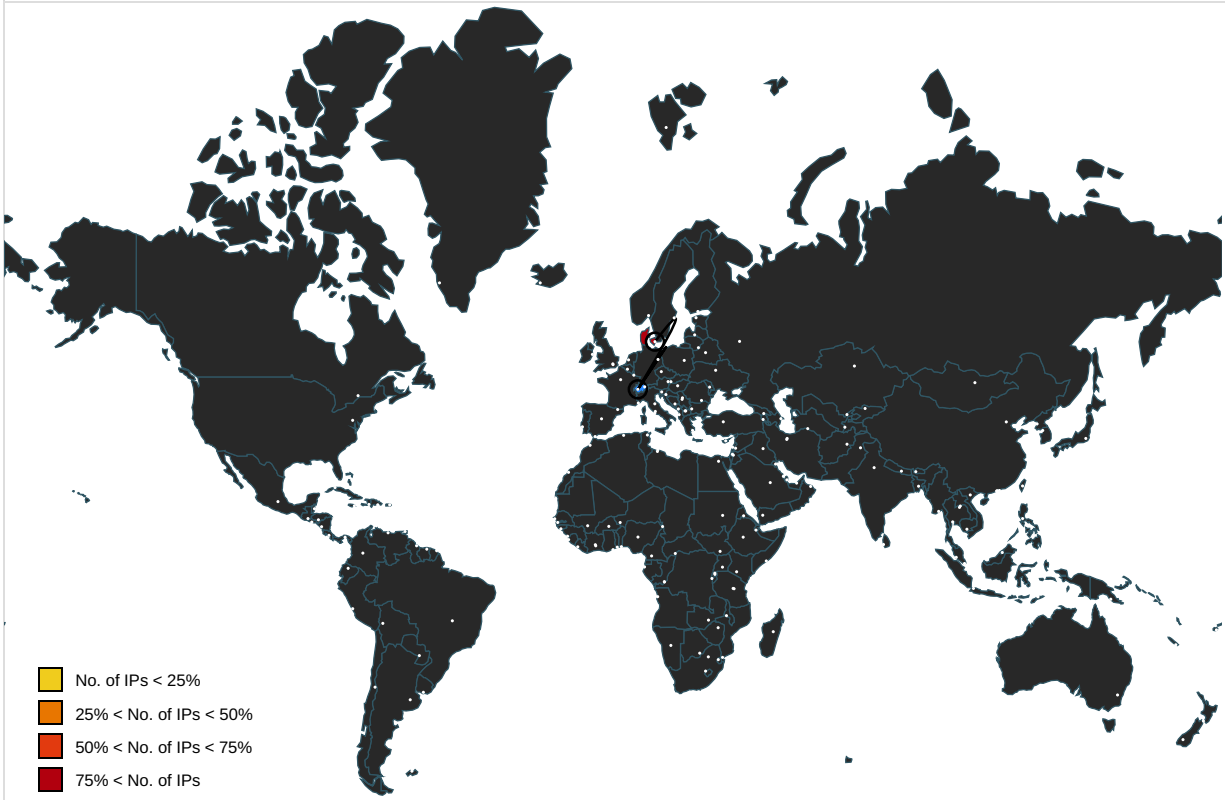
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://go.michv	HDPh51eN5s.exe, 00000007.00000002.388973873.0000000001084000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	HDPh51eN5s.exe, 00000000.00000002.270816823.00000000033A1000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000006.00000002.512755863.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.211.246.53	unknown	Denmark		15516	DK-DANSKKABELTVDK	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679249
Start date and time: 05/08/202213:13:10	2022-08-05 13:13:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HDPh51eN5s (renamed file extension from none to 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:	30
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.evad.winEXE@12/3@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 63% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:14:22	Task Scheduler	Run new task: Google Update path: C:\Users\user\Desktop\HDPh51eN5s.exe
13:15:43	API Interceptor	1x Sleep call for process: MpCmdRun.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\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\HDPh51eN5s.exe.log

Process:	C:\Users\user\Desktop\HDPh51eN5s.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1281
Entropy (8bit):	5.367899416177239
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1Q
MD5:	7115A3215A4C22EF20AB9AF4160EE8F5
SHA1:	A4CAB34355971C1FBAABECEFA91458C4936F2C24
SHA-256:	A4A689E8149166591F94A8C84E99BE744992B9E80BDB7A0713453EB6C59BBBB2
SHA-512:	2CEF2BCD284265B147ABF300A4D26AD1AAC743EFE0B47A394FB614B6843A60B9F918E56261A56334078D0D9681132F3403FB734EE66E1915CF76F29411D5CE2(
Malicious:	**true**
Reputation:	moderate, very likely benign file
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..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1654798503046924
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zw+b:j+s+v+b+P+m+0+Q+q+3+b
MD5:	2633F0F310DC0DDE5E42973AFEAF7F89
SHA1:	53FDDBA449DF28F68130EB11AF56BB3EE7300FF4
SHA-256:	8DE4072D371AD5704889A0539F005D9587226DB4686EF0C774266BB1754A1E85
SHA-512:	62B3F96C6C3308AA0232DC1F53BD8415934E0EB525223DBC8AAC86FAEB6953DF65E59501A274FA3169914E56855C7C90016D26CEDE2AAE90E50567A271EA58(7
Malicious:	false
Reputation:	low
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

C:\Windows\System32\Windows\RuntimeBroker.exe

Process:	C:\Users\user\Desktop\HDPh51eN5s.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	6171136
Entropy (8bit):	6.610162822007531
Encrypted:	false
SSDEEP:	98304:5Po4eyejblyJFeBLgYcNBUsBtzOevoMlda05+8pbVTnVp8DW1db7LAm0xVHzd6Wy:640sHwwakZpX1aYGHMaBq9DR5y03HQiB
MD5:	1FB5D967F92174E0BBB15262F8CD209F
SHA1:	76FBD5B88154976887B5099C21666CA3BE2CD76E
SHA-256:	740634ECEDD318AC8F84C360F5D253FF836C5E60DA6542C65A140B17B4BA8024
SHA-512:	A0FF48D7E219C71828D0CBDE56F59AF7326DFF4DA021789CEFC68D1EA90EA467EB98B7418070A3007A63F58AD5987DC9EFFE79BC143A33C5ECBE1A963A708E A9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 36%, Browse • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 77%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..b.....p].....n.].. .....@.. .....^.....^. ..@.....].S.....]..... ....H.....text...tn].. ...p]..... ..`.rsrc.....]....t]....@..@.reloc.....].....]....@..B5+VE3vdj(.....]....]....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.610162822007531
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	HDPh51eN5s.exe
File size:	6171136
MD5:	1fb5d967f92174e0bbb15262f8cd209f
SHA1:	76fbd5b88154976887b5099c21666ca3be2cd76e
SHA256:	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024
SHA512:	a0ff48d7e219c71828d0cbde56f59af7326dff4da021789cefc68d1ea90ea467eb98b7418070a3007a63f58ad5987dc9effe79bc143a33c5ecbe1a963a708ea9
SSDEEP:	98304:5Po4eyejblyJFeBLgYcNBUsBtzOevoMlda05+8pbVTnVp8DW1db7LAm0xVHzd6Wy:640sHwwakZpX1aYGHMaBq9DR5y03HQiB
TLSH:	F15612A2A5449898FEFA0230F0E57B2CC3F53783B5ED686E0ECD194511A5A88FD3558F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..b.....p].....n.].. .....@.. .....^.....^...@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x9d8e6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE

Time Stamp:	0x62E1125A [Wed Jul 27 10:24:26 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [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	0x5d8e18	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5da000	0xc00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5dc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x2000	0x8	.text
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	0x5d6e74	0x5d7000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x5da000	0xc00	0xc00	False	0.3567708333333333	data	5.263389654594389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5dc000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
5+VE3vdj	0x5de000	0xa728	0xa800	False	0.8907412574404762	data	7.584538152941798	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x5da0a0	0x2e4	data		
RT_MANIFEST	0x5da384	0x6d7	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:15:12.682216883 CEST	49775	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:15:15.745399952 CEST	49775	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:15:21.745737076 CEST	49775	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:15:37.654670000 CEST	49780	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:15:40.669297934 CEST	49780	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:15:46.701088905 CEST	49780	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:16:02.128798962 CEST	49812	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:16:05.140202999 CEST	49812	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:16:11.140929937 CEST	49812	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:16:27.001981974 CEST	49840	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:16:30.079967976 CEST	49840	28391	192.168.2.3	82.211.246.53
Aug 5, 2022 13:16:36.080517054 CEST	49840	28391	192.168.2.3	82.211.246.53

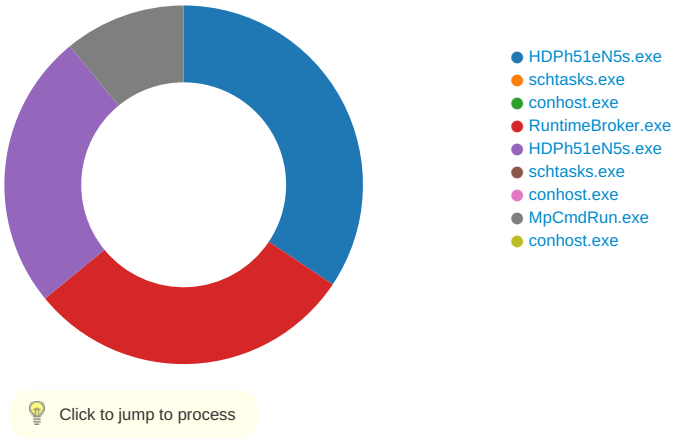
ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 5, 2022 13:15:22.296092033 CEST	82.211.246.53	192.168.2.3	8da	(Host unreachable)	Destination Unreachable
Aug 5, 2022 13:15:39.636266947 CEST	82.211.246.53	192.168.2.3	8da	(Host unreachable)	Destination Unreachable
Aug 5, 2022 13:15:42.646208048 CEST	82.211.246.53	192.168.2.3	8da	(Host unreachable)	Destination Unreachable
Aug 5, 2022 13:16:11.306586981 CEST	82.211.246.53	192.168.2.3	8da	(Host unreachable)	Destination Unreachable
Aug 5, 2022 13:16:36.306998014 CEST	82.211.246.53	192.168.2.3	8da	(Host unreachable)	Destination Unreachable

Statistics

Behavior



System Behavior

Analysis Process: HDPh51eN5s.exe PID: **4684**, Parent PID: **5404**

General

Target ID:	0
Start time:	13:14:05
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\HDPh51eN5s.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\HDPh51eN5s.exe"
Imagebase:	0xac0000
File size:	6171136 bytes
MD5 hash:	1FB5D967F92174E0BBB15262F8CD209F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000000.00000002.277374012.00000000134FA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000000.00000003.251870111.000000001584C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MAL_QuasarRAT_May19_1, Description: Detects QuasarRAT malware, Source: 00000000.00000002.303504388.000000001C3E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000000.00000002.303504388.000000001C3E0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: schtasks.exe PID: **2916**, Parent PID: **4684**

General

Target ID:	4
Start time:	13:14:20
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	"schtasks" /create /tn "Google Update" /sc ONLOGON /tr "C:\Users\user\Desktop\HDPh51eN5s.exe" /rl HIGHEST /f
Imagebase:	0x7ff744f70000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
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: **5672**, Parent PID: **2916**

General

Target ID:	5
Start time:	13:14:21
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: RuntimeBroker.exe PID: **5824**, Parent PID: **4684**

General

Target ID:	6
Start time:	13:14:21
Start date:	05/08/2022
Path:	C:\Windows\System32\Windows\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Windows\RuntimeBroker.exe
Imagebase:	0x620000
File size:	6171136 bytes
MD5 hash:	1FB5D967F92174E0BBB15262F8CD209F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000006.00000003.289424719.0000000015501000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, Virustotal, Browse • Detection: 31%, Metadefender, Browse • Detection: 77%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC60B9F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC60B9F1E9	unknown

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	7FFC60A6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC60A6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60A72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60A6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC60A6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5F9CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5F9CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.ServiceModel\479b3517e01a68c8dc3205b04d25d863\System.ServiceModel.ni.dll.aux	unknown	3948	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Runtime92aa12#\5be3331dc99f83f7338fe65ac942ad9f\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Accessibility\053d7928abe50e911f11f88a6e79aa8d\Accessibility.ni.dll.aux	unknown	300	success or wait	1	7FFC60B412E7	ReadFile

Analysis Process: HDPh51eN5s.exe PID: 6020, Parent PID: 848

General

Target ID:	7
Start time:	13:14:23

Start date:	05/08/2022
Path:	C:\Users\user\Desktop\HDPh51eN5s.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\HDPh51eN5s.exe
Imagebase:	0x510000
File size:	6171136 bytes
MD5 hash:	1FB5D967F92174E0BBB15262F8CD209F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000007.00000002.401638486.0000000012E41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC60B9F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC60B9F1E9	unknown

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	7FFC60A6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC60A6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60A72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60A6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC60A6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC60B412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5F9CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5F9CB526	ReadFile

Analysis Process: schtasks.exe PID: **6276**, Parent PID: **5824**

General

Target ID:	18

Start time:	13:14:48
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	"schtasks" /create /tn "Google Update" /sc ONLOGON /tr "C:\Windows\system32\Windows\RuntimeBroker.exe" /rl HIGHEST /f
Imagebase:	0x7ff744f70000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
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: 6328, Parent PID: 6276

General

Target ID:	19
Start time:	13:14:48
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: MpCmdRun.exe PID: 4276, Parent PID: 5672

General

Target ID:	24
Start time:	13:15:42
Start date:	05/08/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

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
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	------------------------------------- ------------------------------------- -----------	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 41 00 75 00 67 00 20 00 0e 20 30 00 35 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 33 00 3a 00 31 00 35 00 3a 00 34 00 33 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Fri Aug 05 2022 13:15 :43	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 41 00 75 00 67 00 20 00 0e 20 30 00 35 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 33 00 3a 00 31 00 35 00 3a 00 34 00 33 00 0d 00 0a 00	MpCmdRun: End Time: Fri Aug 05 2022 13:15:43	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: **1320**, Parent PID: **4276**

General

Target ID:	26
Start time:	13:15:42
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly