ID: 388089
Sample Name: SBG-1100319PurchaseOrder.exe
Cookbook: default.jbs
Time: 21:36:31
Date: 15/04/2021
Version: 31.0.0 Emerald

Table of Contents

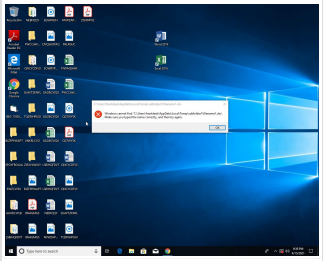
Analysis Report SBG-1100319PurchaseOrder.exe

Overview

General Information

Sample Name:	SBG-1100319PurchaseOrder.exe
Analysis ID:	388089
MD5:	2dd62d78b9f7e9c.
SHA1:	151d4cd68958df3.
SHA256:	c63a3f86be406a1.
Tags:	exe RAT RemcosRAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

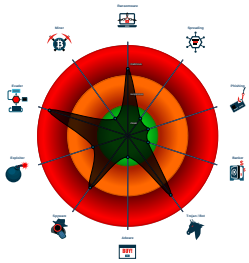
Remcos GuLoader

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

Signatures

- Found malware configuration
- Potential malicious icon found
- Sigma detected: Remcos
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Creates autostart registry keys with …
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- SBG-1100319PurchaseOrder.exe (PID: 6224 cmdline: 'C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe' MD5: 2DD62D78B9F7E9C5529502E085B55756)
  - SBG-1100319PurchaseOrder.exe (PID: 6352 cmdline: 'C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe' MD5: 2DD62D78B9F7E9C5529502E085B55756)
- wscript.exe (PID: 7152 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - filename1.exe (PID: 5936 cmdline: C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe MD5: 2DD62D78B9F7E9C5529502E085B55756)
    - filename1.exe (PID: 5516 cmdline: C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe MD5: 2DD62D78B9F7E9C5529502E085B55756)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=1685231EC8E4EC43&resid=1685231EC8E4EC43%2"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.341786606.000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000002.00000002.501532840.000000000562000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: filename1.exe PID: 5516	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	

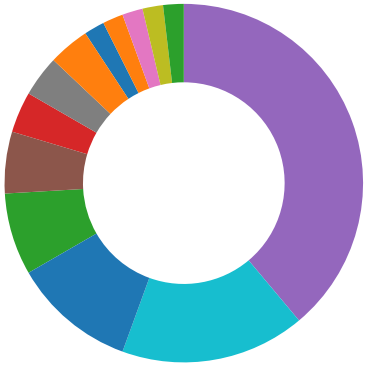
Source	Rule	Description	Author	Strings
Process Memory Space: filename1.exe PID: 5516	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: SBG-1100319PurchaseOrder.exe PID: 6224	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Remcos

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Potential malicious icon found

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Boot Survival:

Creates autostart registry keys with suspicious values (likely registry only malware)

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

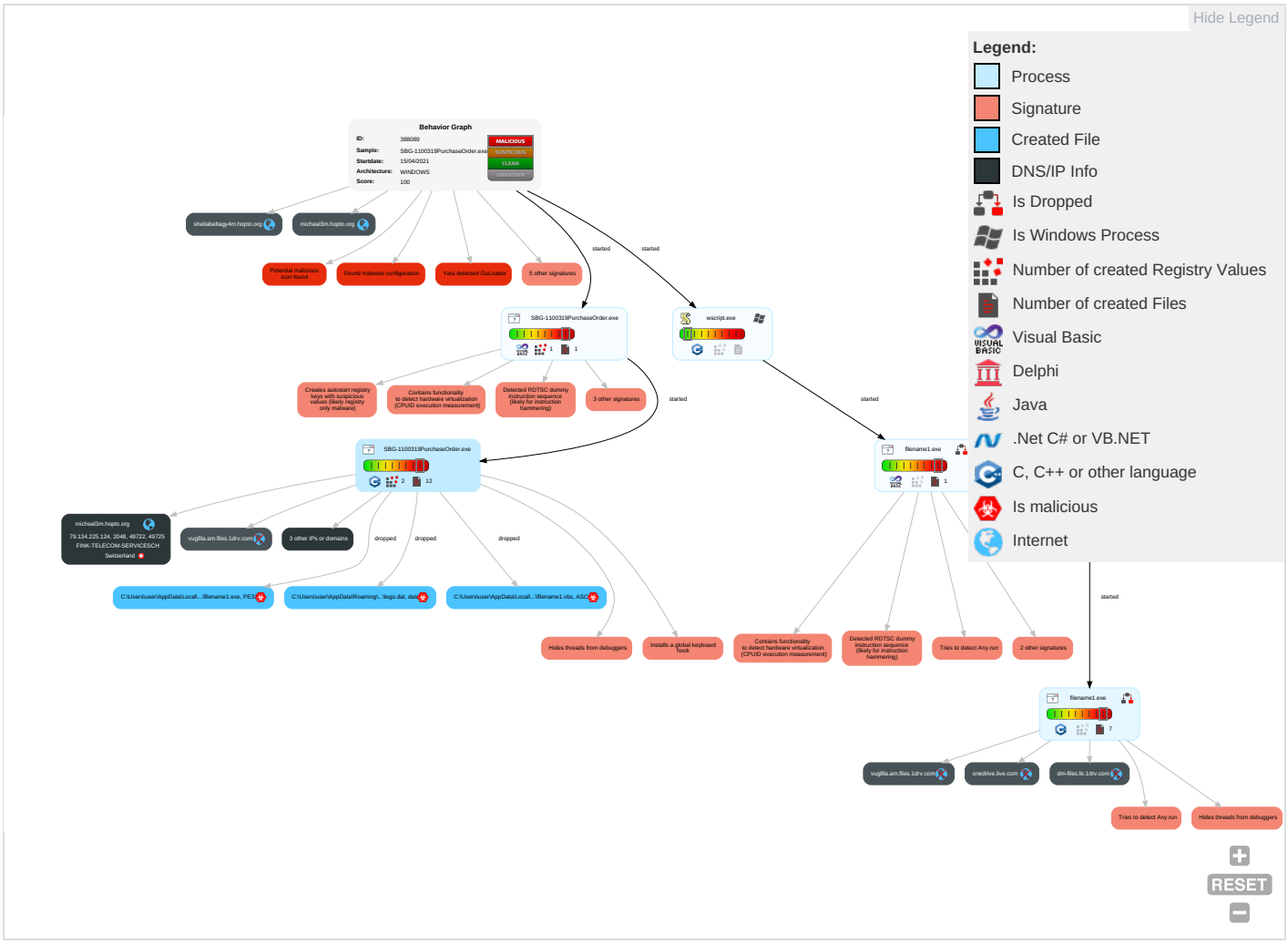
Contains functionality to hide a thread from the debugger

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Scripting 1 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1	Input Capture 1 1 1	Security Software Discovery 7 2 1	Remote Services	Input Capture 1 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Information Discovery 3 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com

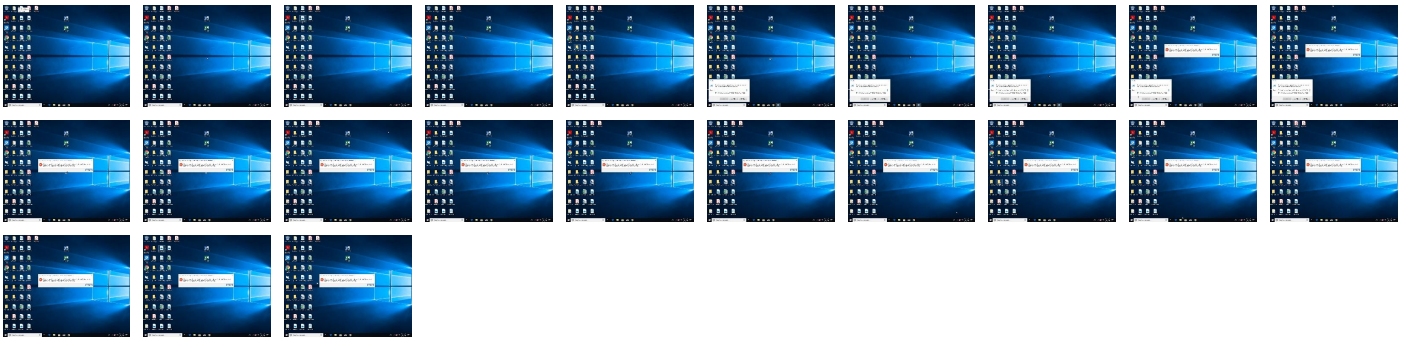
Behavior Graph

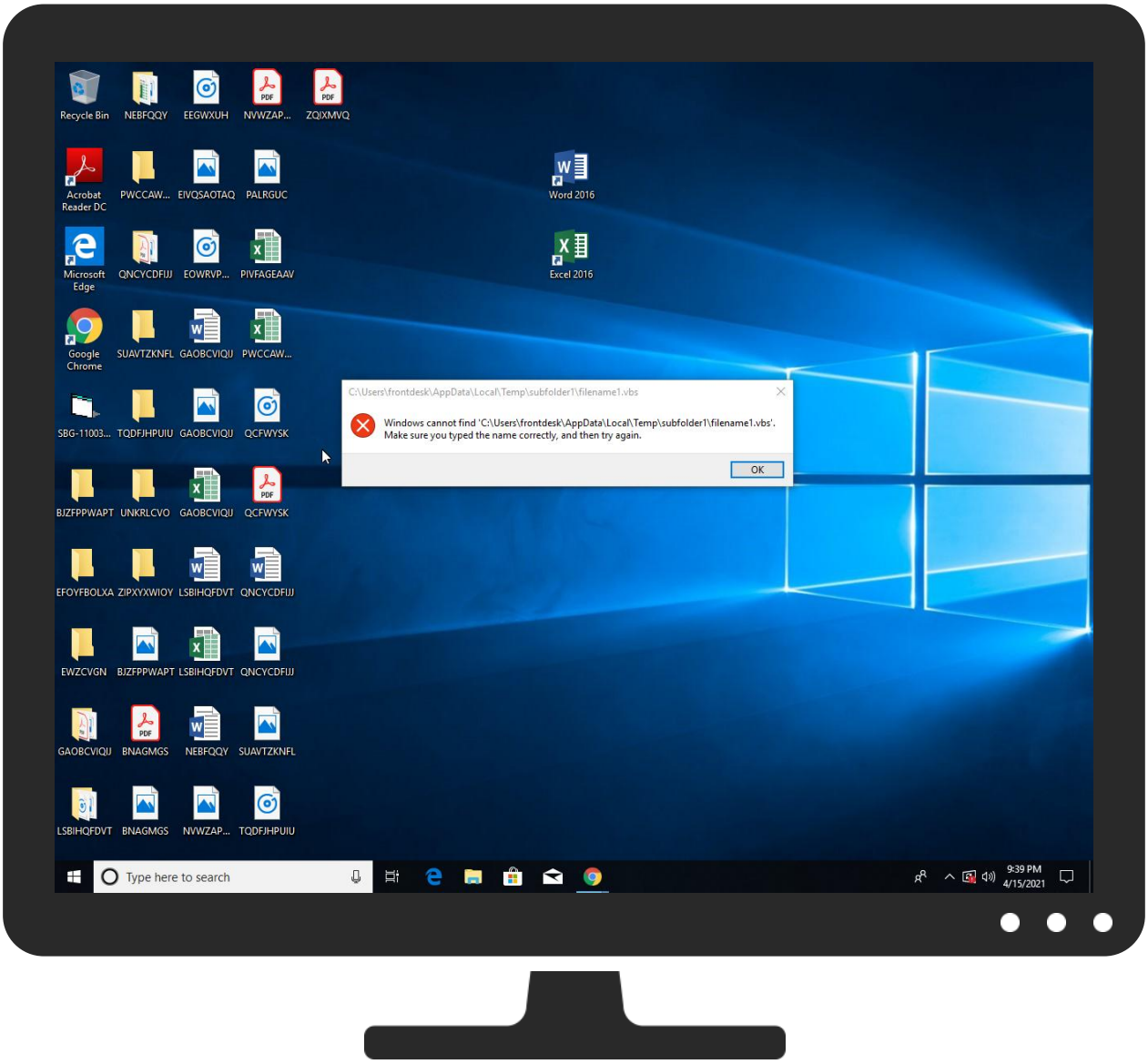


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
micheal3m.hopto.org	1%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sheilabeltagy4m.hopto.org	79.134.225.124	true	false		unknown
micheal3m.hopto.org	79.134.225.124	true	false	• 1%, Virustotal, Browse	unknown
onedrive.live.com	unknown	unknown	false		high
vug8la.am.files.1drv.com	unknown	unknown	false		high

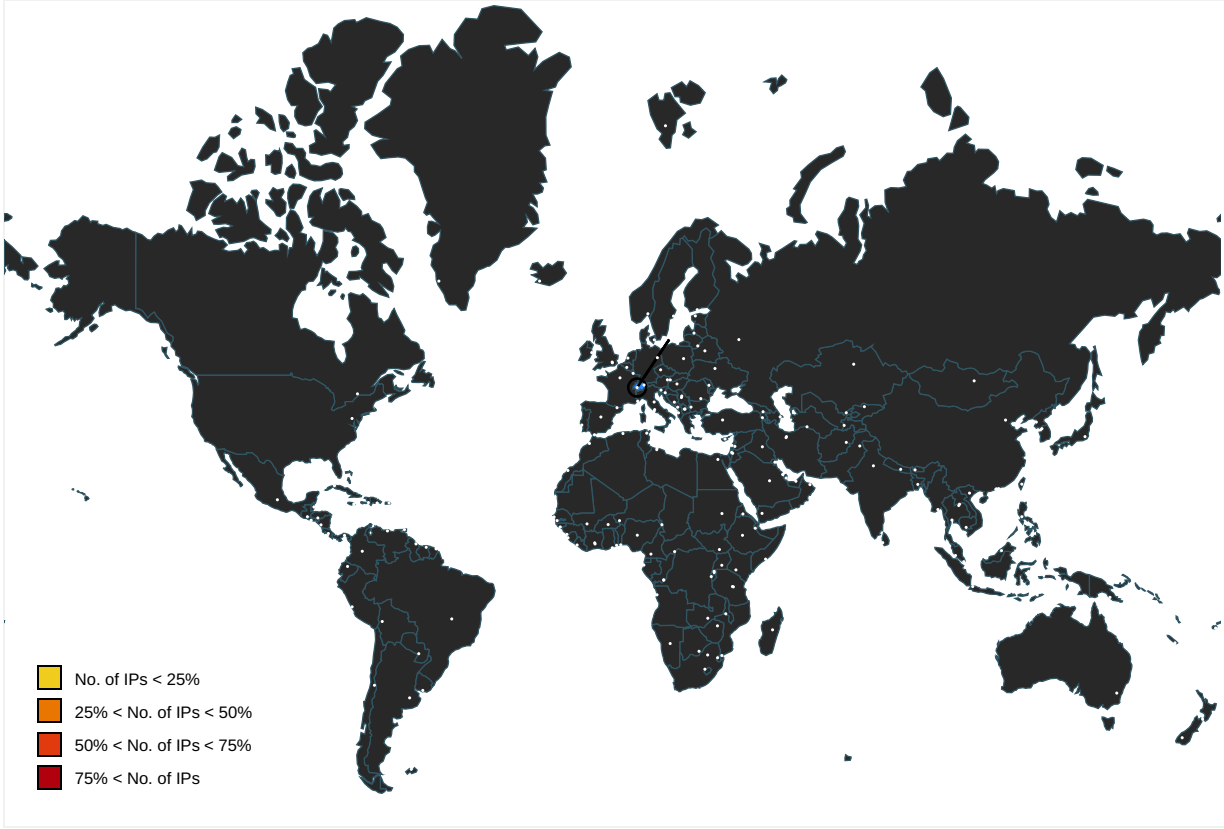
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=1685231EC8E4EC43&resid=1685231EC8E4EC43%2	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/b	SBG-1100319PurchaseOrder.exe, 00000002.00000002.502105694.000000000929000.00000004.00000020.sdmp	false		high
http://https://vug8la.am.files.1drv.com/y4mT1QYIp_fyTE8Fy0lLLYF_0s99rPZfbzgWA1b5QlZt4eQwn4RVNktZv9qdlLB64Ai	SBG-1100319PurchaseOrder.exe, 00000002.00000002.502229070.000000000971000.00000004.00000020.sdmp, SBG-1100319PurchaseOrder.exe, 00000002.00000002.502196213.000000000095A000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/download?cid=1685231EC8E4EC43&resid=1685231EC8E4EC43%21505&authkey=ANKqoxx	SBG-1100319PurchaseOrder.exe, filename1.exe, 0000000D.00000002.341786606.0000000000560000.00000040.00000001.sdmp	false		high
http://https://vug8la.am.files.1drv.com/	SBG-1100319PurchaseOrder.exe, 00000002.00000003.345228305.000000000971000.00000004.00000001.sdmp, SBG-1100319PurchaseOrder.exe, 00000002.00000002.502175655.000000000094A000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/	SBG-1100319PurchaseOrder.exe, 00000002.00000002.502105694.000000000929000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.124	sheilabeltagy4m.hopto.org	Switzerland		6775	FINK-TELECOM-SERVICESCH	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	388089
Start date:	15.04.2021
Start time:	21:36:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SBG-1100319PurchaseOrder.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.rans.troj.spyw.evad.winEXE@8/3@62/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 4.8% (good quality ratio 4.8%) • Quality average: 56% • Quality standard deviation: 6.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.82.209.183, 52.255.188.83, 104.43.193.48, 92.122.145.220, 104.43.139.144, 23.57.80.111, 13.107.42.13, 13.107.42.12, 2.20.142.209, 2.20.142.210, 51.103.5.159, 20.82.210.154, 23.32.238.177, 23.32.238.234, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, au.download.windowsupdate.com.edgesuite.net, odc-dm-files-geo.onedrive.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, l-0004.l-msedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, odc-dm-files.onedrive.akadns.net.l-0003.dc-msedge.net.l-0003.l-msedge.net, wns.notify.trafficmanager.net, l-0003.l-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, odc-dm-files-brs.onedrive.akadns.net, client.wns.windows.com, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
21:37:39	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs

Time	Type	Description
21:37:48	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.124	RFQ234.exe	Get hash	malicious	Browse	
	SURE.exe	Get hash	malicious	Browse	
	remps1.ps1	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	kYXjS6Oc3S.exe	Get hash	malicious	Browse	• 79.134.225.40
	eK1KiJlz3l.exe	Get hash	malicious	Browse	• 79.134.225.40
	80tzo8FG3d.exe	Get hash	malicious	Browse	• 79.134.225.40
	SecuriteInfo.com.Trojan.PackedNET.658.8528.exe	Get hash	malicious	Browse	• 79.134.225.62
	perchase order.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	New Order.exe	Get hash	malicious	Browse	• 79.134.225.125
	New Tender04,pdf.exe	Get hash	malicious	Browse	• 79.134.225.70
	list3503-purchase-order-12-04-21.pdf.jar	Get hash	malicious	Browse	• 79.134.225.104
	list3503-purchase-order-12-04-21.pdf.jar	Get hash	malicious	Browse	• 79.134.225.104
	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe	Get hash	malicious	Browse	• 79.134.225.30
	PR0078966.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 79.134.225.21
	JQEl8bosea.exe	Get hash	malicious	Browse	• 79.134.225.30
	YfceI5MZX4.exe	Get hash	malicious	Browse	• 79.134.225.30
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	OjAJYVQ7iK.exe	Get hash	malicious	Browse	• 79.134.225.112
	TSskTqG9V9.exe	Get hash	malicious	Browse	• 79.134.225.30
	Files Specification.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	J62DQ7fO0b.exe	Get hash	malicious	Browse	• 79.134.225.30
	oE6O5K1emC.exe	Get hash	malicious	Browse	• 79.134.225.30

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe

Process:	C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	204800
Entropy (8bit):	5.671059123248846
Encrypted:	false

C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe	
SSDEEP:	3072:hPLl4Y52bzb2z50FdSfZaa0e5+YghusL5PEqJ:hPLl4Y5s6ziKfx0eERV
MD5:	2DD62D78B9F7E9C5529502E085B55756
SHA1:	151D4CD68958DF35AE706CC232627A05E923307F
SHA-256:	C63A3F86BE406A11E8F7760403E407A97441753205F8CEF432FD634856CA2992
SHA-512:	9B7D8EE135DCA77460B5E2D566C2B42F68D5B97918F6D9C2F4BDF6F89D6C46B8001482123880D46137A59EF04BEC89498F728D018D4CC8FC57F56FBDFB70534
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B..B..L^...B...`...B...d...B..Rich.B.....PE..L.....#J..... .....0.....@.....0.....t...(... .....(... .....d.....text..... . .`.data.....@....rsrc..... .....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs	
Process:	C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	120
Entropy (8bit):	4.938880835346308
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRD0nacwRE2J5xAIjuHdIRQM:jFqhv9IcNwi23faGqM
MD5:	8E21029138080630E1FCF8A6B4DA0159
SHA1:	B0B4C5CB0A53268829CB4FF33FBD906568FCD54B
SHA-256:	E692E45BD1482FA4C1932955B196BE0AA212EB792AFB65CDB85EA457EE5258B5
SHA-512:	1DCA2EE27776CEA53BADB8431D32613E65C62AD9E2C9A36552BD6F7D56AE6039E745C39136360A8509290650B3AFAE7D17C278F033750FEC186C853E41774C7
Malicious:	**true**
Reputation:	low
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe")

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe
File Type:	data
Category:	dropped
Size (bytes):	402
Entropy (8bit):	3.608276114189592
Encrypted:	false
SSDEEP:	6:llKkRmfxl55YcIeeDAlgRfebW/33flO1CfSMlW8g1UEZ+lX1FKDDcNebW/G:bZDecXbWnlOQqkXg1Q1FAccbWe
MD5:	0549758588F8B85AAC20868F10523E34
SHA1:	AE76F042B448277EF3CBACC63D7F00A8F6F1948F
SHA-256:	AC69EE30064EB845886176352A94214F1E278B7890BE119FDEE7F05AA234F467
SHA-512:	BC0E797B52EDB9692007933A1FA9761D6E44DF40D38F40B7420F9176F4020C32E2906141E2E2879029EA722D9C35ECCF22961A365A43C68FCA805799F942F327
Malicious:	**true**
Reputation:	low
Preview:	....[.2.0.2.1./.0.4./.1.5. .2.1.:.3.7.:.5.0. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[. .R.u.n. .].....[. .P.r.o.g.r.a.m. .M.a.n.a.g.e.r. .].....[. .B.R.I.N.T.O.V.E.R.I.L. T.E.T.S. .].....[. .C.:.\.U.s.e.r.s.\.f.r.o.n.t.d.e.s.k.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.s.u.b.f.o.l.d.e.r.1.\.f.i.l.e.n.a.m.e.1...v.b.s. .].....[. .P.r.o.g.r.a.m. .M.a.n.a.g.e.r. .].....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.671059123248846
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	SBG-1100319PurchaseOrder.exe
File size:	204800
MD5:	2dd62d78b9f7e9c5529502e085b55756

General

SHA1:	151d4cd68958df35ae706cc232627a05e923307f
SHA256:	c63a3f86be406a11e8f7760403e407a97441753205f8cef432fd634856ca2992
SHA512:	9b7d8ee135dca77460b5e2d566c2b42f68d5b97918f6d9c2f4bdf6f89d6c46b80014821231380d46137a59ef04bec89498f728d018d4cc8fc57f56fbdfb705349
SSDEEP:	3072:hPLl4Y52bzb2z50FdSfZaa0e5+YghusL5PEqJ:hPLl4Y5s6ziKfx0eERV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....#J.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401780
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4A23B8BA [Mon Jun 1 11:17:14 2009 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:	e917dfcbe7bbc83f756c722d2ba3704e

Entrypoint Preview

Instruction
push 00402FE0h
call 00007F18808E3625h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add ah, al
jmp 00007F189111903Ch
jbe 00007F18808E3676h
mov bh, 51h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2f374	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x32000	0x98c	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
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	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x164	.text
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
.text	0x1000	0x2e8fc	0x2f000	False	0.304521276596	data	5.8539621073	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x30000	0x11d4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x32000	0x98c	0x1000	False	0.17919921875	data	2.09138345915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3285c	0x130	data		
RT_ICON	0x32574	0x2e8	data		
RT_ICON	0x3244c	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x3241c	0x30	data		
RT_VERSION	0x32150	0x2cc	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaLineInputStr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaStrCmp, __vbaAryConstruct2, __vbaI2I4, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaVarMul, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaErrorOverflow, __vbaFileOpen, __vbaNew2, __vbaVarInt, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarAdd, __vbaVarDup, __vbaFpI4, __vbaVarLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	Highness
InternalName	hippoglossus
FileVersion	4.00
CompanyName	Highness
LegalTrademarks	Highness
Comments	Highness
ProductName	INFILTRERER
ProductVersion	4.00
OriginalFilename	hippoglossus.exe

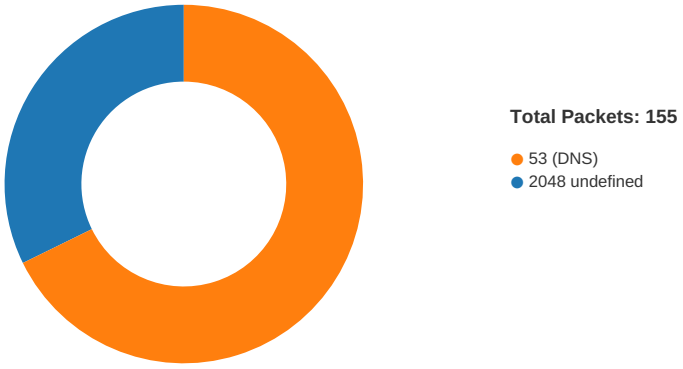
Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 21:37:50.658086061 CEST	49722	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:50.745105982 CEST	2048	49722	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:51.344219923 CEST	49722	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:51.431309938 CEST	2048	49722	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:51.937181950 CEST	49722	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:52.023936033 CEST	2048	49722	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:52.091919899 CEST	49725	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:52.176884890 CEST	2048	49725	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:52.687280893 CEST	49725	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:52.771493912 CEST	2048	49725	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:53.296722889 CEST	49725	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:53.381534100 CEST	2048	49725	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:54.446427107 CEST	49726	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:54.530323982 CEST	2048	49726	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:55.187752008 CEST	49726	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:55.271759033 CEST	2048	49726	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:55.796799898 CEST	49726	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:55.880161047 CEST	2048	49726	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:55.946604967 CEST	49727	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:56.032840014 CEST	2048	49727	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:56.640830040 CEST	49727	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:56.725261927 CEST	2048	49727	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:57.304725885 CEST	49727	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:57.387958050 CEST	2048	49727	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:58.510648966 CEST	49729	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:58.594577074 CEST	2048	49729	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:59.188102007 CEST	49729	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:59.271946907 CEST	2048	49729	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:59.797215939 CEST	49729	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:37:59.881184101 CEST	2048	49729	79.134.225.124	192.168.2.7
Apr 15, 2021 21:37:59.946696043 CEST	49730	2048	192.168.2.7	79.134.225.124

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 21:38:00.032313108 CEST	2048	49730	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:00.687903881 CEST	49730	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:00.772231102 CEST	2048	49730	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:01.297344923 CEST	49730	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:01.381195068 CEST	2048	49730	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:02.643265009 CEST	49731	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:02.730581999 CEST	2048	49731	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:03.344342947 CEST	49731	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:03.431385040 CEST	2048	49731	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:04.032040119 CEST	49731	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:04.119266987 CEST	2048	49731	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:05.151153088 CEST	49732	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:05.234556913 CEST	2048	49732	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:05.797668934 CEST	49732	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:05.881674051 CEST	2048	49732	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:06.500875950 CEST	49732	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:06.586385965 CEST	2048	49732	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:07.661844969 CEST	49733	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:07.745783091 CEST	2048	49733	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:08.344841957 CEST	49733	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:08.428081989 CEST	2048	49733	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:09.032380104 CEST	49733	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:09.116520882 CEST	2048	49733	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:09.183631897 CEST	49734	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:09.269610882 CEST	2048	49734	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:09.776696920 CEST	49734	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:09.859898090 CEST	2048	49734	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:10.438726902 CEST	49734	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:10.522753000 CEST	2048	49734	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:11.600717068 CEST	49735	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:11.683999062 CEST	2048	49735	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:12.188847065 CEST	49735	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:12.274252892 CEST	2048	49735	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:12.798233032 CEST	49735	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:12.884767056 CEST	2048	49735	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:12.954102039 CEST	49736	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:13.038309097 CEST	2048	49736	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:13.642090082 CEST	49736	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:13.725850105 CEST	2048	49736	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:14.309469938 CEST	49736	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:14.395292044 CEST	2048	49736	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:15.495146036 CEST	49737	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:15.581310987 CEST	2048	49737	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:16.189173937 CEST	49737	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:16.272660971 CEST	2048	49737	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:16.798619032 CEST	49737	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:16.881822109 CEST	2048	49737	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:16.946445942 CEST	49739	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:17.029719114 CEST	2048	49739	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:17.533021927 CEST	49739	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:17.616312027 CEST	2048	49739	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:18.142458916 CEST	49739	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:18.226792097 CEST	2048	49739	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:19.298131943 CEST	49747	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:19.382178068 CEST	2048	49747	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:20.001991034 CEST	49747	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:20.086201906 CEST	2048	49747	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:20.697515011 CEST	49747	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:20.781402111 CEST	2048	49747	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:21.023291111 CEST	49748	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:21.107357025 CEST	2048	49748	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:21.642724991 CEST	49748	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:21.726025105 CEST	2048	49748	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:22.345961094 CEST	49748	2048	192.168.2.7	79.134.225.124

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 21:38:22.431240082 CEST	2048	49748	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:23.527326107 CEST	49749	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:23.613301992 CEST	2048	49749	79.134.225.124	192.168.2.7
Apr 15, 2021 21:38:24.189809084 CEST	49749	2048	192.168.2.7	79.134.225.124
Apr 15, 2021 21:38:24.276510954 CEST	2048	49749	79.134.225.124	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 21:37:21.116890907 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:21.139518023 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:21.177566051 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:21.212950945 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:21.342756987 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:21.393239021 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:22.445159912 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:22.496710062 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:23.436460018 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:23.485205889 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:24.375103951 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:24.423715115 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:25.134414911 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:25.184573889 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:26.352135897 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:26.402460098 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:27.737003088 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:27.799365997 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:28.697981119 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:28.751064062 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:28.955796003 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:29.004618883 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:30.043492079 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:30.092012882 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:32.206346989 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:32.268373013 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:33.275363922 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:33.324043989 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:34.326977968 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:34.375830889 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:35.509403944 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:35.562067032 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:37.801271915 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:37.852930069 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:38.638372898 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:38.688057899 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:39.744858027 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:39.793553114 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:41.156838894 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:41.205507040 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:42.519402981 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:42.578747988 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:45.196619987 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:45.253675938 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:48.802593946 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:48.893234015 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:49.218544960 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:49.267182112 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:49.960247040 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:50.058324099 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:50.591296911 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:50.657018900 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:50.752192974 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:50.803999901 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:51.613775015 CEST	64296	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 21:37:51.662403107 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:52.027503014 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:52.090646982 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:54.396652937 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:54.445342064 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:55.883899927 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:55.945579052 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:58.407825947 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:58.464782953 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 15, 2021 21:37:59.886395931 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:37:59.943789959 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:02.496493101 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:02.556653976 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:05.063811064 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:05.121182919 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:07.598874092 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:07.660828114 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:09.121296883 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:09.182832956 CEST	53	58367	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:11.537194014 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:11.599572897 CEST	53	60599	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:12.891961098 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:12.952260017 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:15.411658049 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:15.475481033 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:16.332539082 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:16.392249107 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:16.885463953 CEST	60427	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:16.945600033 CEST	53	60427	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:17.518254995 CEST	56209	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:17.575056076 CEST	53	56209	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:17.929274082 CEST	59582	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:17.994009972 CEST	53	59582	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:18.128596067 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:18.180253983 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:18.573218107 CEST	58542	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:18.703882933 CEST	53	58542	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:19.239909887 CEST	59179	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:19.297369003 CEST	53	59179	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:20.951914072 CEST	60927	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:21.009164095 CEST	53	60927	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:23.464535952 CEST	57854	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:23.526545048 CEST	53	57854	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:24.889895916 CEST	62026	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:24.946687937 CEST	53	62026	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:27.407407999 CEST	59453	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:27.467569113 CEST	53	59453	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:27.503534079 CEST	62468	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:27.560568094 CEST	53	62468	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:28.856319904 CEST	52563	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:28.916944027 CEST	53	52563	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:31.242928028 CEST	54721	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:31.302731037 CEST	53	54721	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:32.736114979 CEST	62826	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:32.755860090 CEST	62046	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:32.793426991 CEST	53	62826	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:32.818896055 CEST	53	62046	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:35.085406065 CEST	51223	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:35.144741058 CEST	53	51223	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:36.452704906 CEST	63908	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:36.509987116 CEST	53	63908	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:38.883800030 CEST	49226	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:38.942790985 CEST	53	49226	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:40.288779974 CEST	60212	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 21:38:40.337698936 CEST	53	60212	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:42.617156982 CEST	58867	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:42.667422056 CEST	53	58867	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:43.935611963 CEST	50864	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:43.993396044 CEST	53	50864	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:46.276639938 CEST	61504	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:46.328351974 CEST	53	61504	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:47.609361887 CEST	60231	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:47.660983086 CEST	53	60231	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:49.947123051 CEST	50095	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:50.006330013 CEST	53	50095	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:51.309214115 CEST	59654	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:51.367562056 CEST	53	59654	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:53.654618025 CEST	58233	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:53.713327885 CEST	53	58233	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:55.002692938 CEST	56822	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:55.060154915 CEST	53	56822	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:57.364814997 CEST	62572	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:57.420237064 CEST	53	62572	8.8.8.8	192.168.2.7
Apr 15, 2021 21:38:58.721203089 CEST	57179	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:59.710292101 CEST	57179	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:38:59.772655010 CEST	53	57179	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:02.055828094 CEST	56124	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:02.116065025 CEST	53	56124	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:03.420850039 CEST	62287	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:03.469728947 CEST	53	62287	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:04.451302052 CEST	54644	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:04.500186920 CEST	53	54644	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:05.760915995 CEST	59159	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:05.818090916 CEST	53	59159	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:07.113179922 CEST	57924	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:07.170516968 CEST	53	57924	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:08.245248079 CEST	51712	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:08.305916071 CEST	53	51712	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:09.463030100 CEST	58865	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:09.512432098 CEST	53	58865	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:10.786021948 CEST	64337	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:10.844202042 CEST	53	64337	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:13.140233040 CEST	50407	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:13.189012051 CEST	53	50407	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:14.469330072 CEST	61075	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:14.526352882 CEST	53	61075	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:16.916650057 CEST	54952	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:16.980429888 CEST	53	54952	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:18.251857042 CEST	59186	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:18.312412977 CEST	53	59186	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:20.590785980 CEST	52280	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:20.650733948 CEST	53	52280	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:21.949884892 CEST	51794	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:22.009567022 CEST	53	51794	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:24.292645931 CEST	50815	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:24.358584881 CEST	53	50815	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:24.644330978 CEST	58498	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:24.696161032 CEST	53	58498	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:25.542690992 CEST	56862	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:25.602709055 CEST	53	56862	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:25.656965971 CEST	61807	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:25.716300964 CEST	53	61807	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:26.318164110 CEST	52009	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:26.375566959 CEST	53	52009	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:26.387872934 CEST	58648	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:26.455368042 CEST	53	58648	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:26.870881081 CEST	59337	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:26.988657951 CEST	53	59337	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 21:39:27.811736107 CEST	59269	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:27.871707916 CEST	53	59269	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:28.170053959 CEST	49802	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:28.230061054 CEST	53	49802	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:28.934828043 CEST	50706	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:29.039972067 CEST	53	50706	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:29.503515005 CEST	55153	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:29.565331936 CEST	53	55153	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:29.623873949 CEST	59744	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:29.681648970 CEST	53	59744	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:30.935522079 CEST	59987	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:30.984512091 CEST	53	59987	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:31.859147072 CEST	61272	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:31.922386885 CEST	53	61272	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:31.924108028 CEST	54352	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:31.984180927 CEST	53	54352	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:32.517014980 CEST	60696	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:32.625258923 CEST	53	60696	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:33.209800005 CEST	59139	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:33.271392107 CEST	53	59139	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:35.556883097 CEST	59565	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:35.614804029 CEST	53	59565	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:36.892472029 CEST	56397	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:36.951955080 CEST	53	56397	8.8.8.8	192.168.2.7
Apr 15, 2021 21:39:39.229773998 CEST	52818	53	192.168.2.7	8.8.8.8
Apr 15, 2021 21:39:39.291035891 CEST	53	52818	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 15, 2021 21:37:48.802593946 CEST	192.168.2.7	8.8.8.8	0x46d8	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:49.960247040 CEST	192.168.2.7	8.8.8.8	0x775d	Standard query (0)	vug8la.am.files.1drv.com	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:50.591296911 CEST	192.168.2.7	8.8.8.8	0x531e	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:52.027503014 CEST	192.168.2.7	8.8.8.8	0x6687	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:54.396652937 CEST	192.168.2.7	8.8.8.8	0x77b7	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:55.883899927 CEST	192.168.2.7	8.8.8.8	0xefcd	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:58.407825947 CEST	192.168.2.7	8.8.8.8	0xcd0e	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:59.886395931 CEST	192.168.2.7	8.8.8.8	0xebc3	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:02.496493101 CEST	192.168.2.7	8.8.8.8	0x71af	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:05.063811064 CEST	192.168.2.7	8.8.8.8	0x1ad9	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:07.598874092 CEST	192.168.2.7	8.8.8.8	0x6e9f	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:09.121296883 CEST	192.168.2.7	8.8.8.8	0xf87f	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:11.537194014 CEST	192.168.2.7	8.8.8.8	0x1eaa	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:12.891961098 CEST	192.168.2.7	8.8.8.8	0xa7cf	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:15.411658049 CEST	192.168.2.7	8.8.8.8	0x4e0d	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:16.885463953 CEST	192.168.2.7	8.8.8.8	0x3a5a	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:17.518254995 CEST	192.168.2.7	8.8.8.8	0x263a	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:18.573218107 CEST	192.168.2.7	8.8.8.8	0x7d41	Standard query (0)	vug8la.am.files.1drv.com	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:19.239909887 CEST	192.168.2.7	8.8.8.8	0x635c	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:20.951914072 CEST	192.168.2.7	8.8.8.8	0x2da5	Standard query (0)	micheal3m.hopto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 15, 2021 21:38:23.464535952 CEST	192.168.2.7	8.8.8.8	0xd9a0	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:24.889895916 CEST	192.168.2.7	8.8.8.8	0xe9a0	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:27.407407999 CEST	192.168.2.7	8.8.8.8	0x21ec	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:28.856319904 CEST	192.168.2.7	8.8.8.8	0xac6b	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:31.242928028 CEST	192.168.2.7	8.8.8.8	0xbbde	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:32.736114979 CEST	192.168.2.7	8.8.8.8	0x1485	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:35.085406065 CEST	192.168.2.7	8.8.8.8	0x8533	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:36.452704906 CEST	192.168.2.7	8.8.8.8	0x62a9	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:38.883800030 CEST	192.168.2.7	8.8.8.8	0xac9d	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:40.288779974 CEST	192.168.2.7	8.8.8.8	0x2a00	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:42.617156982 CEST	192.168.2.7	8.8.8.8	0xf1f	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:43.935611963 CEST	192.168.2.7	8.8.8.8	0x8ff1	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:46.276639938 CEST	192.168.2.7	8.8.8.8	0x8eba	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:47.609361887 CEST	192.168.2.7	8.8.8.8	0x63b2	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:49.947123051 CEST	192.168.2.7	8.8.8.8	0xefaf	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:51.309214115 CEST	192.168.2.7	8.8.8.8	0xc01c	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:53.654618025 CEST	192.168.2.7	8.8.8.8	0x54a5	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:55.002692938 CEST	192.168.2.7	8.8.8.8	0xe904	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:57.364814997 CEST	192.168.2.7	8.8.8.8	0x7315	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:58.721203089 CEST	192.168.2.7	8.8.8.8	0x24ab	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:59.710292101 CEST	192.168.2.7	8.8.8.8	0x24ab	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:02.055828094 CEST	192.168.2.7	8.8.8.8	0x7441	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:03.420850039 CEST	192.168.2.7	8.8.8.8	0x5bf	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:05.760915995 CEST	192.168.2.7	8.8.8.8	0x4f8f	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:07.113179922 CEST	192.168.2.7	8.8.8.8	0x2030	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:09.463030100 CEST	192.168.2.7	8.8.8.8	0x7ec7	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:10.786021948 CEST	192.168.2.7	8.8.8.8	0x3a2c	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:13.140233040 CEST	192.168.2.7	8.8.8.8	0xfb12	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:14.469330072 CEST	192.168.2.7	8.8.8.8	0x1bf5	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:16.916650057 CEST	192.168.2.7	8.8.8.8	0x95d4	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:18.251857042 CEST	192.168.2.7	8.8.8.8	0xe70b	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:20.590785980 CEST	192.168.2.7	8.8.8.8	0x480b	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:21.949884892 CEST	192.168.2.7	8.8.8.8	0xf35f	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:24.292645931 CEST	192.168.2.7	8.8.8.8	0x10c4	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:25.656965971 CEST	192.168.2.7	8.8.8.8	0x1111	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:28.170053959 CEST	192.168.2.7	8.8.8.8	0xa942	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:29.503515005 CEST	192.168.2.7	8.8.8.8	0x96b3	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 15, 2021 21:39:31.859147072 CEST	192.168.2.7	8.8.8.8	0xe0c1	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:33.209800005 CEST	192.168.2.7	8.8.8.8	0x3d8e	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:35.556883097 CEST	192.168.2.7	8.8.8.8	0x91ca	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:36.892472029 CEST	192.168.2.7	8.8.8.8	0xc874	Standard query (0)	micheal3m. hopto.org	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:39.229773998 CEST	192.168.2.7	8.8.8.8	0xdf46	Standard query (0)	sheilabelt agy4m.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 15, 2021 21:37:48.893234015 CEST	8.8.8.8	192.168.2.7	0x46d8	No error (0)	onedrive.l ive.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 15, 2021 21:37:50.058324099 CEST	8.8.8.8	192.168.2.7	0x775d	No error (0)	vug8la.am. files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 15, 2021 21:37:50.058324099 CEST	8.8.8.8	192.168.2.7	0x775d	No error (0)	dm-files.f e.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 15, 2021 21:37:50.657018900 CEST	8.8.8.8	192.168.2.7	0x531e	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:52.090646982 CEST	8.8.8.8	192.168.2.7	0x6687	No error (0)	micheal3m. hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:54.445342064 CEST	8.8.8.8	192.168.2.7	0x77b7	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:55.945579052 CEST	8.8.8.8	192.168.2.7	0xefcd	No error (0)	micheal3m. hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:58.464782953 CEST	8.8.8.8	192.168.2.7	0xcd0e	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:37:59.943789959 CEST	8.8.8.8	192.168.2.7	0xebc3	No error (0)	micheal3m. hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:02.556653976 CEST	8.8.8.8	192.168.2.7	0x71af	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:05.121182919 CEST	8.8.8.8	192.168.2.7	0x1ad9	No error (0)	micheal3m. hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:07.660828114 CEST	8.8.8.8	192.168.2.7	0x6e9f	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:09.182832956 CEST	8.8.8.8	192.168.2.7	0xf87f	No error (0)	micheal3m. hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:11.599572897 CEST	8.8.8.8	192.168.2.7	0x1eaa	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:12.952260017 CEST	8.8.8.8	192.168.2.7	0xa7cf	No error (0)	micheal3m. hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:15.475481033 CEST	8.8.8.8	192.168.2.7	0x4e0d	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:16.945600033 CEST	8.8.8.8	192.168.2.7	0x3a5a	No error (0)	micheal3m. hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:17.575056076 CEST	8.8.8.8	192.168.2.7	0x263a	No error (0)	onedrive.l ive.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 15, 2021 21:38:18.703882933 CEST	8.8.8.8	192.168.2.7	0x7d41	No error (0)	vug8la.am. files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 15, 2021 21:38:18.703882933 CEST	8.8.8.8	192.168.2.7	0x7d41	No error (0)	dm-files.f e.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 15, 2021 21:38:19.297369003 CEST	8.8.8.8	192.168.2.7	0x635c	No error (0)	sheilabelt agy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)

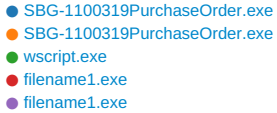
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 15, 2021 21:38:21.009164095 CEST	8.8.8.8	192.168.2.7	0x2da5	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:23.526545048 CEST	8.8.8.8	192.168.2.7	0xd9a0	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:24.946687937 CEST	8.8.8.8	192.168.2.7	0xe9a0	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:27.467569113 CEST	8.8.8.8	192.168.2.7	0x21ec	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:28.916944027 CEST	8.8.8.8	192.168.2.7	0xac6b	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:31.302731037 CEST	8.8.8.8	192.168.2.7	0xbbde	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:32.793426991 CEST	8.8.8.8	192.168.2.7	0x1485	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:35.144741058 CEST	8.8.8.8	192.168.2.7	0x8533	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:36.509987116 CEST	8.8.8.8	192.168.2.7	0x62a9	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:38.942790985 CEST	8.8.8.8	192.168.2.7	0xac9d	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:40.337698936 CEST	8.8.8.8	192.168.2.7	0x2a00	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:42.667422056 CEST	8.8.8.8	192.168.2.7	0xf1f	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:43.993396044 CEST	8.8.8.8	192.168.2.7	0x8ff1	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:46.328351974 CEST	8.8.8.8	192.168.2.7	0x8eba	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:47.660983086 CEST	8.8.8.8	192.168.2.7	0x63b2	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:50.006330013 CEST	8.8.8.8	192.168.2.7	0xefaf	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:51.367562056 CEST	8.8.8.8	192.168.2.7	0xc01c	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:53.713327885 CEST	8.8.8.8	192.168.2.7	0x54a5	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:55.060154915 CEST	8.8.8.8	192.168.2.7	0xe904	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:57.420237064 CEST	8.8.8.8	192.168.2.7	0x7315	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:38:59.772655010 CEST	8.8.8.8	192.168.2.7	0x24ab	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:02.116065025 CEST	8.8.8.8	192.168.2.7	0x7441	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:03.469728947 CEST	8.8.8.8	192.168.2.7	0x5bf	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:05.818090916 CEST	8.8.8.8	192.168.2.7	0x4f8f	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:07.170516968 CEST	8.8.8.8	192.168.2.7	0x2030	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:09.512432098 CEST	8.8.8.8	192.168.2.7	0x7ec7	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 15, 2021 21:39:10.844202042 CEST	8.8.8.8	192.168.2.7	0x3a2c	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:13.189012051 CEST	8.8.8.8	192.168.2.7	0xfb12	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:14.526352882 CEST	8.8.8.8	192.168.2.7	0x1bf5	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:16.980429888 CEST	8.8.8.8	192.168.2.7	0x95d4	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:18.312412977 CEST	8.8.8.8	192.168.2.7	0xe70b	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:20.650733948 CEST	8.8.8.8	192.168.2.7	0x480b	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:22.009567022 CEST	8.8.8.8	192.168.2.7	0xf35f	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:24.358584881 CEST	8.8.8.8	192.168.2.7	0x10c4	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:25.716300964 CEST	8.8.8.8	192.168.2.7	0x1111	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:28.230061054 CEST	8.8.8.8	192.168.2.7	0xa942	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:29.565331936 CEST	8.8.8.8	192.168.2.7	0x96b3	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:31.922386885 CEST	8.8.8.8	192.168.2.7	0xe0c1	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:33.271392107 CEST	8.8.8.8	192.168.2.7	0x3d8e	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:35.614804029 CEST	8.8.8.8	192.168.2.7	0x91ca	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:36.951955080 CEST	8.8.8.8	192.168.2.7	0xc874	No error (0)	micheal3m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)
Apr 15, 2021 21:39:39.291035891 CEST	8.8.8.8	192.168.2.7	0xdf46	No error (0)	sheilabeltagy4m.hopto.org		79.134.225.124	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SBG-1100319PurchaseOrder.exe PID: 6224 Parent PID: 5840

General

Start time:	21:37:29
Start date:	15/04/2021
Path:	C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe'
Imagebase:	0x400000
File size:	204800 bytes
MD5 hash:	2DD62D78B9F7E9C5529502E085B55756
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: SBG-1100319PurchaseOrder.exe PID: 6352 Parent PID: 6224

General

Start time:	21:37:37
Start date:	15/04/2021
Path:	C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe'
Imagebase:	0x400000

File size:	204800 bytes
MD5 hash:	2DD62D78B9F7E9C5529502E085B55756
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000002.00000002.501532840.0000000000562000.00000040.00000001.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\Temp\subfolder1\filename1.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	566545	CreateFileW
C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	566545	CreateFileW
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	563306	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	563306	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	563306	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	563306	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	563306	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	563306	InternetOpenUrlA
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	408CCE	CreateDirectoryW
C:\Users\user\AppData\Roaming\remcos\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	3	41715E	CreateFileW
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	408CCE	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe	unknown	204800	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 8b 23 c4 db cf 42 aa 88 cf 42 aa 88 cf 42 aa 88 4c 5e a4 88 ce 42 aa 88 80 60 a3 88 cd 42 aa 88 f9 64 a7 88 ce 42 aa 88 52 69 63 68 cf 42 aa 88 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ba b8 23 4a 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 f0 02 00 00 30 00 00 00 00 00 00 80 17 00 00 00 10 00 00 00 00 03 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 04 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........#...B...B...B..L^...B ...`...B...d...B..Rich.B...... ....PE..L.....#J............. ....0....................@.	success or wait	1	561663	WriteFile
C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs	unknown	120	53 65 74 20 57 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a 53 65 74 20 43 20 3d 20 57 2e 45 78 65 63 20 28 22 43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 73 75 62 66 6f 6c 64 65 72 31 5c 66 69 6c 65 6e 61 6d 65 31 2e 65 78 65 22 29	Set W = CreateObject("Wscr ipt.Shell")..Set C = W.Exec ("C:\Users\user \AppData\Local\Temp\subf older1\filename1.exe")	success or wait	1	561663	WriteFile
C:\Users\user\AppData\Roaming\remcos\logs.dat	unknown	170	0d 00 0a 00 5b 00 32 00 30 00 32 00 31 00 2f 00 30 00 34 00 2f 00 31 00 35 00 20 00 32 00 31 00 3a 00 33 00 37 00 3a 00 35 00 30 00 20 00 4f 00 66 00 66 00 6c 00 69 00 6e 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 53 00 74 00 61 00 72 00 74 00 65 00 64 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 20 00 52 00 75 00 6e 00 20 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 20 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 4d 00 61 00 6e 00 61 00 67 00 65 00 72 00 20 00 5d 00 0d 00 0a 00	....[.2.0.2.1./.0.4./.1.5. .2. 1.:.3.7.:.5.0. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r. t.e.d.]........[. .R.u.n. .]. ....[. .P.r.o.g.r.a.m. .M. a.n.a.g.e.r. .].....	success or wait	3	417198	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SBG-1100319PurchaseOrder.exe	unknown	204800	success or wait	1	566545	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\idll-WT08JM\	success or wait	1	410372	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\idll-WT08JM	exepath	binary	ED D2 BF 48 AC 16 45 E5 06 83 C4 8A E6 2C 0B D1 73 94 E8 09 01 FB 76 A0 CA EC 45 99 E3 19 B8 DA 20 FD 2C 5A 6E D0 85 07 7E ED 66 94 78 5F D3 33 8A FA F2 D7 43 52 AB 19 22 9B 92 12 4C B6 E1 79 3E CD AE BD F8 E9 4C 58 53 D9 DE 7F 9B 1D E5 98 88 99 1D C4 07 93 6E A2 82 3F C9 BA B4 B7 16 15 B0 4F 4B 34 EC C2 3E 7B D4 10 12 A1 D9 44 90 3F	success or wait	1	41039A	RegSetValueExA
HKEY_CURRENT_USER\Software\idll-WT08JM	licence	unicode	F980DA39CAEF5CA7DEBAF7FC1AAA23B5	success or wait	1	41039A	RegSetValueExA

Analysis Process: wscript.exe PID: 7152 Parent PID: 3292

General

Start time:	21:37:56
Start date:	15/04/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\subfolder1\filename1.vbs'
Imagebase:	0x7ff667170000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: filename1.exe PID: 5936 Parent PID: 7152

General

Start time:	21:37:57
Start date:	15/04/2021
Path:	C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe
Imagebase:	0x400000
File size:	204800 bytes
MD5 hash:	2DD62D78B9F7E9C5529502E085B55756
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: filename1.exe PID: 5516 Parent PID: 5936

General

Start time:	21:38:09
Start date:	15/04/2021
Path:	C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\subfolder1\filename1.exe
Imagebase:	0x400000
File size:	204800 bytes
MD5 hash:	2DD62D78B9F7E9C5529502E085B55756
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000D.00000002.341786606.0000000000560000.00000040.00000001.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	563306	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	563306	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	563306	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	563306	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	563306	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	563306	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis