ID: 882711
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:22:07
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

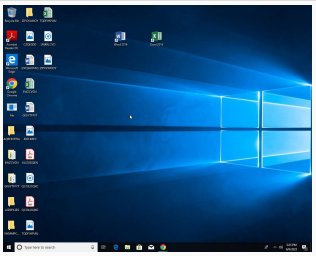
Windows Analysis Report

file.exe

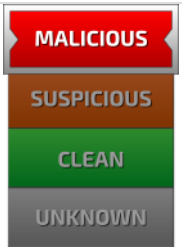
Overview

General Information

Sample Name:	file.exe
Analysis ID:	882711
MD5:	66108176e22e…
SHA1:	a05e217104b3…
SHA256:	e1eb3fe18ad66..
Tags:	NET exe MSIL RemcosRAT x64
Infos:	



Detection



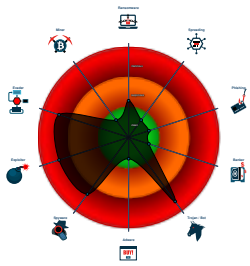
Remcos

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

Signatures

- Found malware configuration
- Yara detected UAC Bypass using C…
- Contains functionality to bypass UA…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Remcos RAT
- Sigma detected: Remcos
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Writes to foreign memory regions
- Contains functionality to steal Firefo…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6804 cmdline: C:\Users\user\Desktop\file.exe MD5: 66108176E22E6F9513A62C76F2185468)
  - aspnet_compiler.exe (PID: 6588 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Remcos, RemcosRAT	Remcos (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers.Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes, but has been used in numerous hacking campaigns.Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user.Remcos is developed by the cybersecurity company BreakingSecurity.	• APT33 • The Gorgon Group	http://malware-traffic-analysis.net/2017/12/22/index.htmlhttps://asec.ahnlab.com/en/32376/https://asec.ahnlab.com/ko/25837/https://asec.ahnlab.com/ko/32101/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "pekonomia.duckdns.org:30861:1",
  "Assigned name": "RemoteHost",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Mutex": "Rmc-B0VP4N",
  "Keylog file": "logs.dat",
  "Screenshot file": "Screenshots",
  "Audio folder": "MicRecords",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "100000"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.550296982.0000018F9283E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000001.00000002.550296982.0000018F9283E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000002.550296982.0000018F9283E000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x6ed58:$a1: Remcos restarted by watchdog! • 0x6f2bc:$a3: %02i:%02i:%02i:%03i
00000002.00000002.813061315.00000000013F7000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000002.00000002.812919702.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.file.exe.18f92636a68.1.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
1.2.file.exe.18f92636a68.1.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
1.2.file.exe.18f92636a68.1.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM	Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003)	ditekSHen	• 0x623b8:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x6234c:$s1: CoGetObject • 0x62360:$s1: CoGetObject • 0x6237c:$s1: CoGetObject • 0x6c15e:$s1: CoGetObject • 0x6230c:$s2: Elevation:Administrator!new:
1.2.file.exe.18f92636a68.1.unpack	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x68470:$a1: Remcos restarted by watchdog! • 0x689d4:$a3: %02i:%02i:%02i:%03i

Source	Rule	Description	Author	Strings
1.2.file.exe.18f92636a68.1.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x624c4:$str_a1: C:\Windows\System32\cmd.exe • 0x62440:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x62440:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x62938:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x63168:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x62534:$str_b2: Executing file: • 0x635b4:$str_b3: GetDirectListeningPort • 0x62f58:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x630d8:$str_b7: \update.vbs • 0x6255c:$str_b9: Downloaded file: • 0x62548:$str_b10: Downloading file: • 0x625ec:$str_b12: Failed to upload file: • 0x6357c:$str_b13: StartForward • 0x6359c:$str_b14: StopForward • 0x63030:$str_b15: fso.DeleteFile " • 0x62fc4:$str_b16: On Error Resume Next • 0x63060:$str_b17: fso.DeleteFolder " • 0x625dc:$str_b18: Uploaded file: • 0x6259c:$str_b19: Unable to delete: • 0x62ff8:$str_b20: while fso.FileExists(" • 0x62a71:$str_c0: [Firefox StoredLogins not found]
Click to see the 14 entries				

Sigma Signatures

Stealing of Sensitive Information

Sigma detected: Remcos

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Exploits

Yara detected UAC Bypass using CMSTP

Privilege Escalation

Contains functionality to bypass UAC (CMSTPLUA)

Networking

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to modify clipboard data

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Delayed program exit found

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Remcos RAT

Contains functionality to steal Firefox passwords or cookies

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality

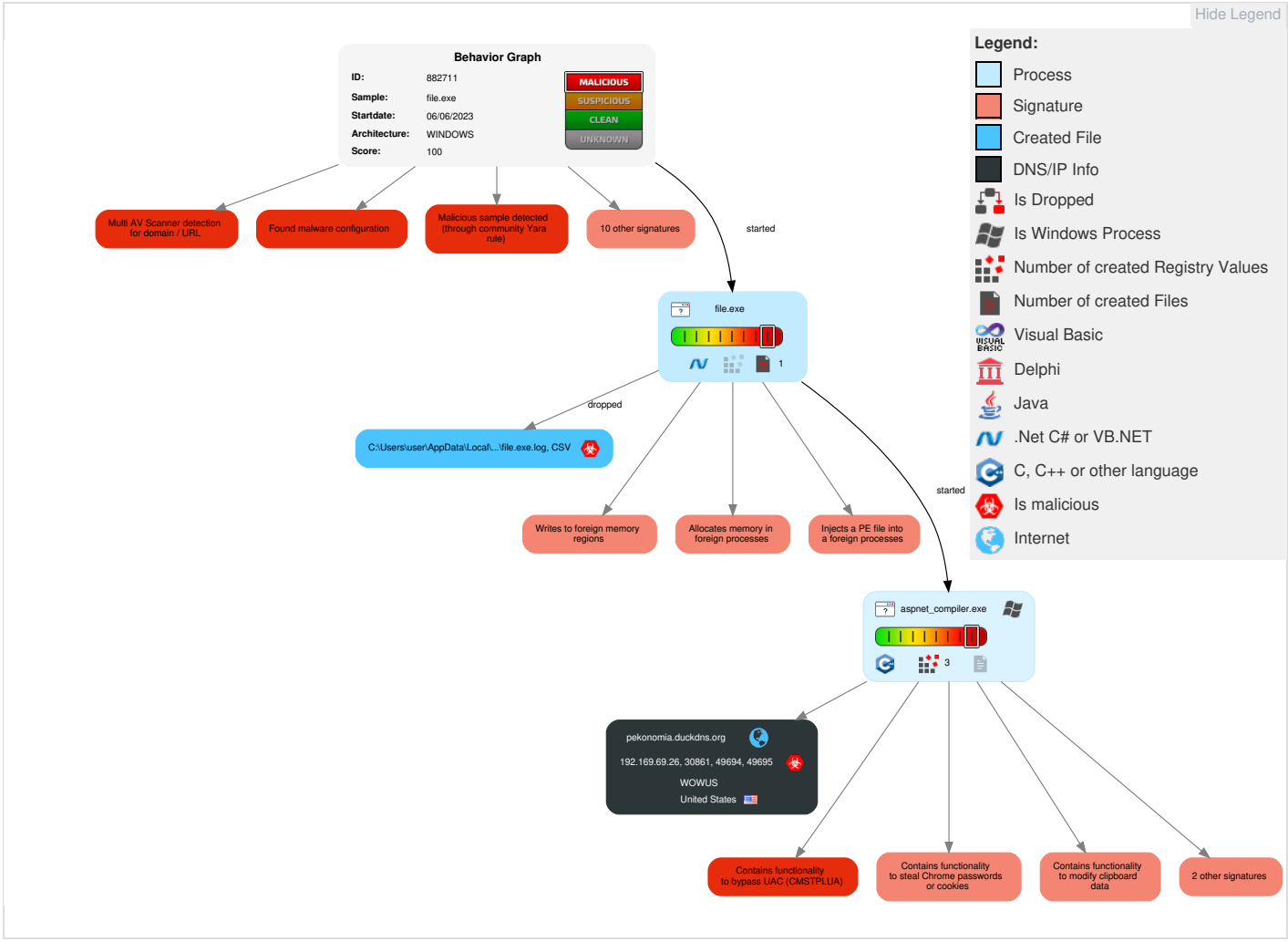
Yara detected Remcos RAT

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 Native API	1 Windows Service	1 Bypass User Access Control	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Service Execution	Logon Script (Windows)	1 Windows Service	3 Obfuscated Files or Information	2 Credentials In Files	1 System Service Discovery	SMB/Windows Admin Shares	1 2 Clipboard Data	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	3 2 1 Process Injection	1 2 Software Packing	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Bypass User Access Control	LSA Secrets	3 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	2 1 Security Software 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 1 Virtualization/Sandbox Evasion	DCSync	2 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Access Token Manipulation	Proc Filesystem	1 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	3 2 1 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
file.exe	32%	Virustotal		Browse
file.exe	100%	Avira	HEUR/AGEN.1326434	
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
pekonomia.duckdns.org	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gp	0%	URL Reputation	safe	
http://geoplugin.net/json.gp	0%	URL Reputation	safe	
http://geoplugin.net/json.gp/C	0%	URL Reputation	safe	
pekonomia.duckdns.org	7%	Virustotal		Browse
pekonomia.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pekonomia.duckdns.org	192.169.69.26	true	true	• 7%, Virustotal, Browse	unknown

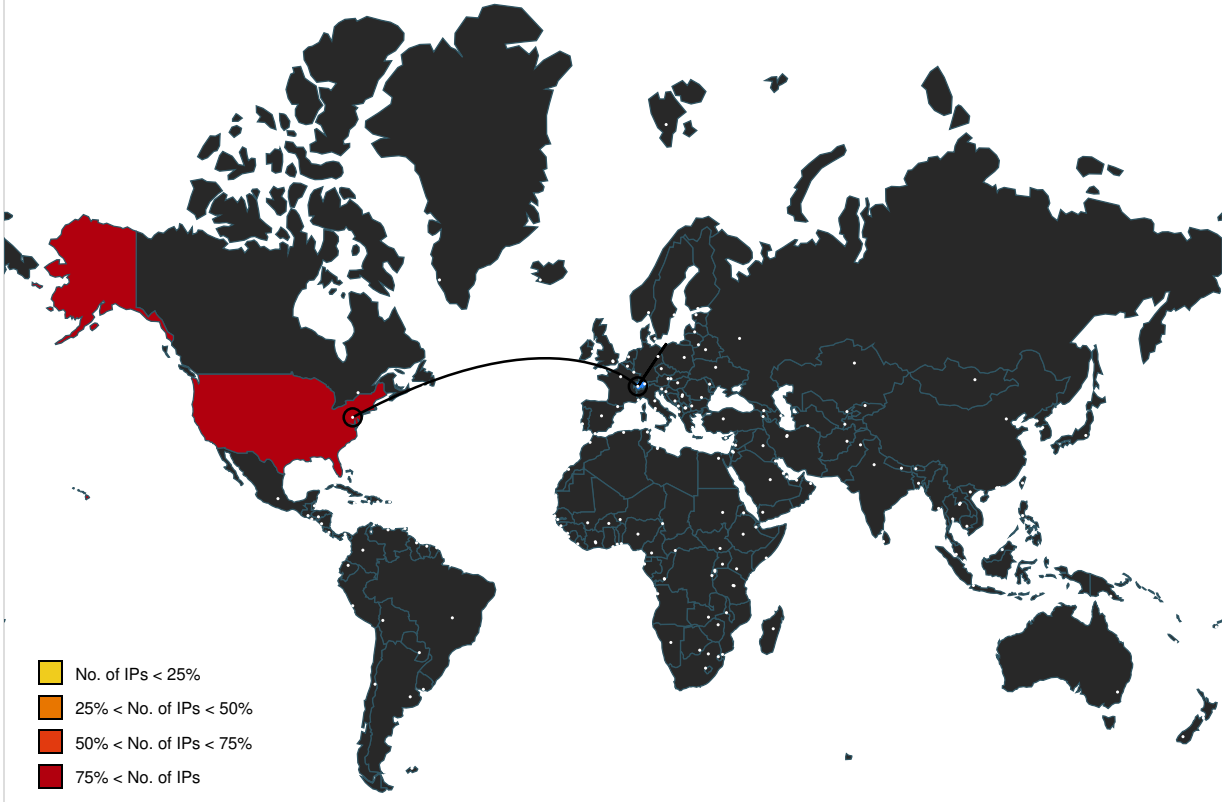
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
pekonomia.duckdns.org	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://geoplugin.net/json.gp	aspnet_compiler.exe	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://geoplugin.net/json.gp/C	file.exe, 00000001.00000002.550296982.00 00018F9283E000.00000004.00000800.0002000 0.00000000.sdmp, aspnet_compiler.exe, 00 000002.00000002.812919702.00000000004000 00.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.169.69.26	pekonomia.duckdns.org	United States		23033	WOWUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882711
Start date and time:	2023-06-06 17:22:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	3
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
Sample file name:	file.exe
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winEXE@3/1@68/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 87.2% (good quality ratio 82.6%) • Quality average: 83.5% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

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\file.exe.log

Process:	C:\Users\user\Desktop\file.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZiIv:Q3La/KDLI4MWuPTxAlv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	**true**
Reputation:	high, 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..

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.962338247780781
TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	file.exe
File size:	500224
MD5:	66108176e22e6f9513a62c76f2185468
SHA1:	a05e217104b39485fbb4ce3cda9cb65b20960ccb
SHA256:	e1eb3fe18ad660415f59eaac2c768afa1b20e07f107dfc207da8b0880a888aaf
SHA512:	646233ba810efba1ab506041d44d698590e30c88ce22f258fcb7eb8ef4435866fb9d7ca1f8d1067c7805c0275c63c690ca98a4b1efbf635fc7b3df8f8f9ca243
SSDEEP:	12288:oeV56CrxH8gnW6yhQNmPLXWu38n4RQgsAlVF+LpnN7TihIHVQMfT:deCrxsvh/Wusn4RHZvF+lnd/
TLSH:	F7B4129CBB1079CFC897D630AA880C28AA94B437970BC343B497255E9A1D2CFCF555E7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....d.....0..... ....@..... .....`...@.....@..... .....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x647F07F4 [Tue Jun 6 10:18:28 2023 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:	

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7c000	0x596	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x7b7c4	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	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	0x79803	0x79a00	False	0.9617564876670093	data	7.966829562881022	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x7c000	0x596	0x600	False	0.416015625	data	4.0776365849895475	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x7c0a0	0x30c	data		
RT_MANIFEST	0x7c3ac	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:23:10.020539045 CEST	49694	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:10.239814043 CEST	30861	49694	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:10.248241901 CEST	49694	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:10.261132956 CEST	49694	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:10.739983082 CEST	30861	49694	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:11.874109983 CEST	49695	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:12.320915937 CEST	30861	49695	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:12.321114063 CEST	49695	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:12.330519915 CEST	49695	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:12.815340042 CEST	30861	49695	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:13.847930908 CEST	49696	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:14.151731968 CEST	30861	49696	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:14.152007103 CEST	49696	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:14.163101912 CEST	49696	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:14.464538097 CEST	30861	49696	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:15.611469030 CEST	49697	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:18.011476994 CEST	30861	49697	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:18.011765957 CEST	49697	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:18.021563053 CEST	49697	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:18.598541975 CEST	30861	49697	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:19.833255053 CEST	49698	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:20.497962952 CEST	30861	49698	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:20.498182058 CEST	49698	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:20.507790089 CEST	49698	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:20.711457968 CEST	30861	49698	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:21.749228001 CEST	49699	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:22.073091030 CEST	30861	49699	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:22.073292971 CEST	49699	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:22.468920946 CEST	49699	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:22.811598063 CEST	30861	49699	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:23.864869118 CEST	49700	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:24.345674992 CEST	30861	49700	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:24.345782042 CEST	49700	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:24.351846933 CEST	49700	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:24.563781023 CEST	30861	49700	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:25.605225086 CEST	49701	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:25.980650902 CEST	30861	49701	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:25.980848074 CEST	49701	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:25.988635063 CEST	49701	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:26.297305107 CEST	30861	49701	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:29.397516966 CEST	49702	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:29.828934908 CEST	30861	49702	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:29.829189062 CEST	49702	30861	192.168.2.4	192.169.69.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:23:29.838835001 CEST	49702	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:30.092890024 CEST	30861	49702	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:31.220876932 CEST	49703	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:31.435878992 CEST	30861	49703	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:31.436007977 CEST	49703	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:31.442682981 CEST	49703	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:31.757859945 CEST	30861	49703	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:32.807379961 CEST	49704	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:33.099116087 CEST	30861	49704	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:33.099446058 CEST	49704	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:33.108616114 CEST	49704	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:33.503370047 CEST	30861	49704	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:34.553211927 CEST	49705	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:34.864063978 CEST	30861	49705	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:34.864389896 CEST	49705	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:34.877161980 CEST	49705	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:35.090729952 CEST	30861	49705	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:36.128022909 CEST	49706	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:36.440148115 CEST	30861	49706	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:36.440316916 CEST	49706	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:36.446348906 CEST	49706	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:36.637808084 CEST	30861	49706	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:37.672673941 CEST	49707	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:37.987435102 CEST	30861	49707	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:37.987632036 CEST	49707	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:38.043175936 CEST	49707	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:38.333920956 CEST	30861	49707	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:39.645679951 CEST	49708	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:40.000320911 CEST	30861	49708	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:40.000567913 CEST	49708	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:40.444880962 CEST	49708	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:40.715411901 CEST	30861	49708	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:41.754580021 CEST	49709	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:41.954874992 CEST	30861	49709	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:41.956939936 CEST	49709	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:41.965553999 CEST	49709	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:42.352693081 CEST	30861	49709	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:43.387157917 CEST	49710	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:43.693973064 CEST	30861	49710	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:43.694065094 CEST	49710	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:43.700570107 CEST	49710	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:44.025559902 CEST	30861	49710	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:45.074491978 CEST	49714	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:45.292243004 CEST	30861	49714	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:45.292365074 CEST	49714	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:45.300174952 CEST	49714	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:45.514847994 CEST	30861	49714	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:46.565622091 CEST	49715	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:46.830353975 CEST	30861	49715	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:46.830677986 CEST	49715	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:46.837193012 CEST	49715	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:47.192370892 CEST	30861	49715	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:48.331861973 CEST	49716	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:48.544203997 CEST	30861	49716	192.169.69.26	192.168.2.4
Jun 6, 2023 17:23:48.544301987 CEST	49716	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:48.553767920 CEST	49716	30861	192.168.2.4	192.169.69.26
Jun 6, 2023 17:23:48.844855070 CEST	30861	49716	192.169.69.26	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:23:07.842909098 CEST	59683	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:08.868144035 CEST	59683	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:09.872961998 CEST	59683	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:10.011384964 CEST	53	59683	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:11.757905006 CEST	64167	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:11.872504950 CEST	53	64167	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:13.824974060 CEST	58565	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:13.844806910 CEST	53	58565	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:15.479593039 CEST	52239	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:15.609191895 CEST	53	52239	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:19.760226965 CEST	56807	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:19.779814005 CEST	53	56807	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:21.727471113 CEST	61007	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:21.747344971 CEST	53	61007	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:23.843090057 CEST	60686	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:23.862986088 CEST	53	60686	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:25.571588039 CEST	61124	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:25.599648952 CEST	53	61124	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:27.315334082 CEST	59444	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:28.370309114 CEST	59444	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:29.366127968 CEST	59444	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:29.394942999 CEST	53	59444	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:31.104743958 CEST	55570	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:31.218715906 CEST	53	55570	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:32.776896000 CEST	64906	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:32.805476904 CEST	53	64906	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:34.520683050 CEST	59446	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:34.549218893 CEST	53	59446	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:36.103789091 CEST	50861	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:36.123658895 CEST	53	50861	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:37.650890112 CEST	61088	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:37.670564890 CEST	53	61088	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:39.491831064 CEST	58729	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:39.644150972 CEST	53	58729	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:41.729126930 CEST	64700	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:41.752347946 CEST	53	64700	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:43.371170998 CEST	56022	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:43.385559082 CEST	53	56022	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:45.041933060 CEST	54851	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:45.069904089 CEST	53	54851	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:46.535536051 CEST	57300	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:46.563900948 CEST	53	57300	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:48.199925900 CEST	54521	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:48.329842091 CEST	53	54521	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:49.855040073 CEST	58914	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:49.874944925 CEST	53	58914	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:53.465065956 CEST	51419	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:53.485065937 CEST	53	51419	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:55.499727011 CEST	51054	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:55.528429985 CEST	53	51054	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:57.402059078 CEST	55673	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:57.421524048 CEST	53	55673	8.8.8.8	192.168.2.4
Jun 6, 2023 17:23:59.402724028 CEST	49735	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:23:59.431236982 CEST	53	49735	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:01.121879101 CEST	52437	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:01.141323090 CEST	53	52437	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:02.886992931 CEST	52825	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:24:02.915380001 CEST	53	52825	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:04.623007059 CEST	58530	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:04.649470091 CEST	53	58530	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:08.423386097 CEST	64959	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:08.438074112 CEST	53	64959	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:10.349967003 CEST	63093	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:10.369967937 CEST	53	63093	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:12.185261965 CEST	50433	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:12.213613033 CEST	53	50433	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:14.093641043 CEST	53498	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:14.108341932 CEST	53	53498	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:16.310941935 CEST	61460	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:16.442303896 CEST	53	61460	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:18.202089071 CEST	63001	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:18.340361118 CEST	53	63001	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:20.404315948 CEST	65133	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:20.526863098 CEST	53	65133	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:22.068470955 CEST	60998	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:22.098330021 CEST	53	60998	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:23.530201912 CEST	61733	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:23.549674034 CEST	53	61733	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:25.286185980 CEST	53370	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:25.314686060 CEST	53	53370	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:26.952038050 CEST	63746	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:27.984253883 CEST	63746	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:28.996661901 CEST	63746	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:29.134788036 CEST	53	63746	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:30.779999971 CEST	50622	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:30.799817085 CEST	53	50622	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:32.452723980 CEST	64773	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:32.472512960 CEST	53	64773	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:34.280824900 CEST	59818	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:34.303818941 CEST	53	59818	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:36.203314066 CEST	49684	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:36.231791019 CEST	53	49684	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:38.046365023 CEST	63229	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:38.069847107 CEST	53	63229	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:39.687596083 CEST	58576	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:39.715939045 CEST	53	58576	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:41.369954109 CEST	54044	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:41.397990942 CEST	53	54044	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:43.000757933 CEST	52259	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:43.029664993 CEST	53	52259	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:44.534632921 CEST	53887	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:44.672501087 CEST	53	53887	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:46.503317118 CEST	56218	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:46.522917032 CEST	53	56218	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:48.273422956 CEST	50094	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:48.292912006 CEST	53	50094	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:50.250770092 CEST	51766	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:50.273751974 CEST	53	51766	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:52.222918987 CEST	61522	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:52.245238066 CEST	53	61522	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:54.251509905 CEST	57349	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:54.279695988 CEST	53	57349	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:55.971133947 CEST	53963	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:55.990896940 CEST	53	53963	8.8.8.8	192.168.2.4
Jun 6, 2023 17:24:57.762820959 CEST	53622	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:57.783139944 CEST	53	53622	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:24:59.581954956 CEST	49600	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:24:59.601772070 CEST	53	49600	8.8.8.8	192.168.2.4
Jun 6, 2023 17:25:01.598633051 CEST	58355	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:25:01.621582031 CEST	53	58355	8.8.8.8	192.168.2.4
Jun 6, 2023 17:25:03.282915115 CEST	57601	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:25:03.311701059 CEST	53	57601	8.8.8.8	192.168.2.4
Jun 6, 2023 17:25:04.892241955 CEST	64159	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:25:04.906692028 CEST	53	64159	8.8.8.8	192.168.2.4
Jun 6, 2023 17:25:06.580219984 CEST	59926	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:25:06.607954979 CEST	53	59926	8.8.8.8	192.168.2.4
Jun 6, 2023 17:25:08.251962900 CEST	61709	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:25:08.266287088 CEST	53	61709	8.8.8.8	192.168.2.4
Jun 6, 2023 17:25:10.254165888 CEST	59182	53	192.168.2.4	8.8.8.8
Jun 6, 2023 17:25:10.273897886 CEST	53	59182	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:23:07.842909098 CEST	192.168.2.4	8.8.8.8	0xc728	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:08.868144035 CEST	192.168.2.4	8.8.8.8	0xc728	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:09.872961998 CEST	192.168.2.4	8.8.8.8	0xc728	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:11.757905006 CEST	192.168.2.4	8.8.8.8	0xa0dd	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:13.824974060 CEST	192.168.2.4	8.8.8.8	0x351c	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:15.479593039 CEST	192.168.2.4	8.8.8.8	0x3285	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:19.760226965 CEST	192.168.2.4	8.8.8.8	0x8664	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:21.727471113 CEST	192.168.2.4	8.8.8.8	0xb42c	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:23.843090057 CEST	192.168.2.4	8.8.8.8	0x9c55	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:25.571588039 CEST	192.168.2.4	8.8.8.8	0xee2a	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:27.315334082 CEST	192.168.2.4	8.8.8.8	0x6115	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:28.370309114 CEST	192.168.2.4	8.8.8.8	0x6115	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:29.366127968 CEST	192.168.2.4	8.8.8.8	0x6115	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:31.104743958 CEST	192.168.2.4	8.8.8.8	0x7b8a	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:32.776896000 CEST	192.168.2.4	8.8.8.8	0x26d9	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:34.520683050 CEST	192.168.2.4	8.8.8.8	0xb5bb	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:36.103789091 CEST	192.168.2.4	8.8.8.8	0x3bab	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:37.650890112 CEST	192.168.2.4	8.8.8.8	0x7d9b	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:39.491831064 CEST	192.168.2.4	8.8.8.8	0x636f	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:41.729126930 CEST	192.168.2.4	8.8.8.8	0x4052	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:43.371170998 CEST	192.168.2.4	8.8.8.8	0x7272	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:45.041933060 CEST	192.168.2.4	8.8.8.8	0x2741	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:46.535536051 CEST	192.168.2.4	8.8.8.8	0xb4a1	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:48.199925900 CEST	192.168.2.4	8.8.8.8	0xad87	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:23:49.855040073 CEST	192.168.2.4	8.8.8.8	0x70fc	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:53.465065956 CEST	192.168.2.4	8.8.8.8	0xc5a1	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:55.499727011 CEST	192.168.2.4	8.8.8.8	0xe4f4	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:57.402059078 CEST	192.168.2.4	8.8.8.8	0xcb52	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:59.402724028 CEST	192.168.2.4	8.8.8.8	0x8c91	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:01.121879101 CEST	192.168.2.4	8.8.8.8	0x1d7b	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:02.886992931 CEST	192.168.2.4	8.8.8.8	0xcf14	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:04.623007059 CEST	192.168.2.4	8.8.8.8	0x1f5e	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:08.423386097 CEST	192.168.2.4	8.8.8.8	0x361c	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:10.349967003 CEST	192.168.2.4	8.8.8.8	0x5ef9	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:12.185261965 CEST	192.168.2.4	8.8.8.8	0xc983	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:14.093641043 CEST	192.168.2.4	8.8.8.8	0x950d	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:16.310941935 CEST	192.168.2.4	8.8.8.8	0x52b5	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:18.202089071 CEST	192.168.2.4	8.8.8.8	0xed56	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:20.404315948 CEST	192.168.2.4	8.8.8.8	0x204e	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:22.068470955 CEST	192.168.2.4	8.8.8.8	0x2055	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:23.530201912 CEST	192.168.2.4	8.8.8.8	0x7c82	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:25.286185980 CEST	192.168.2.4	8.8.8.8	0x16bf	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:26.952038050 CEST	192.168.2.4	8.8.8.8	0xcae8	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:27.984253883 CEST	192.168.2.4	8.8.8.8	0xcae8	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:28.996661901 CEST	192.168.2.4	8.8.8.8	0xcae8	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:30.779999971 CEST	192.168.2.4	8.8.8.8	0x414f	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:32.452723980 CEST	192.168.2.4	8.8.8.8	0x1cc5	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:34.280824900 CEST	192.168.2.4	8.8.8.8	0x1385	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:36.203314066 CEST	192.168.2.4	8.8.8.8	0x5c3c	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:38.046365023 CEST	192.168.2.4	8.8.8.8	0x625a	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:39.687596083 CEST	192.168.2.4	8.8.8.8	0x6d9b	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:41.369954109 CEST	192.168.2.4	8.8.8.8	0x947b	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:43.000757933 CEST	192.168.2.4	8.8.8.8	0x7d50	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:44.534632921 CEST	192.168.2.4	8.8.8.8	0xdd7	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:46.503317118 CEST	192.168.2.4	8.8.8.8	0xeec7	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:48.273422956 CEST	192.168.2.4	8.8.8.8	0x5b	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:50.250770092 CEST	192.168.2.4	8.8.8.8	0x460a	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:52.222918987 CEST	192.168.2.4	8.8.8.8	0xf2aa	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:54.251509905 CEST	192.168.2.4	8.8.8.8	0xccbd	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:24:55.971133947 CEST	192.168.2.4	8.8.8.8	0xed15	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:57.762820959 CEST	192.168.2.4	8.8.8.8	0x81b3	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:59.581954956 CEST	192.168.2.4	8.8.8.8	0xfba9	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:01.598633051 CEST	192.168.2.4	8.8.8.8	0x85f4	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:03.282915115 CEST	192.168.2.4	8.8.8.8	0x7a4d	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:04.892241955 CEST	192.168.2.4	8.8.8.8	0xe585	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:06.580219984 CEST	192.168.2.4	8.8.8.8	0x8514	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:08.251962900 CEST	192.168.2.4	8.8.8.8	0x57d7	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:10.254165888 CEST	192.168.2.4	8.8.8.8	0xb90f	Standard query (0)	pekonomia.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

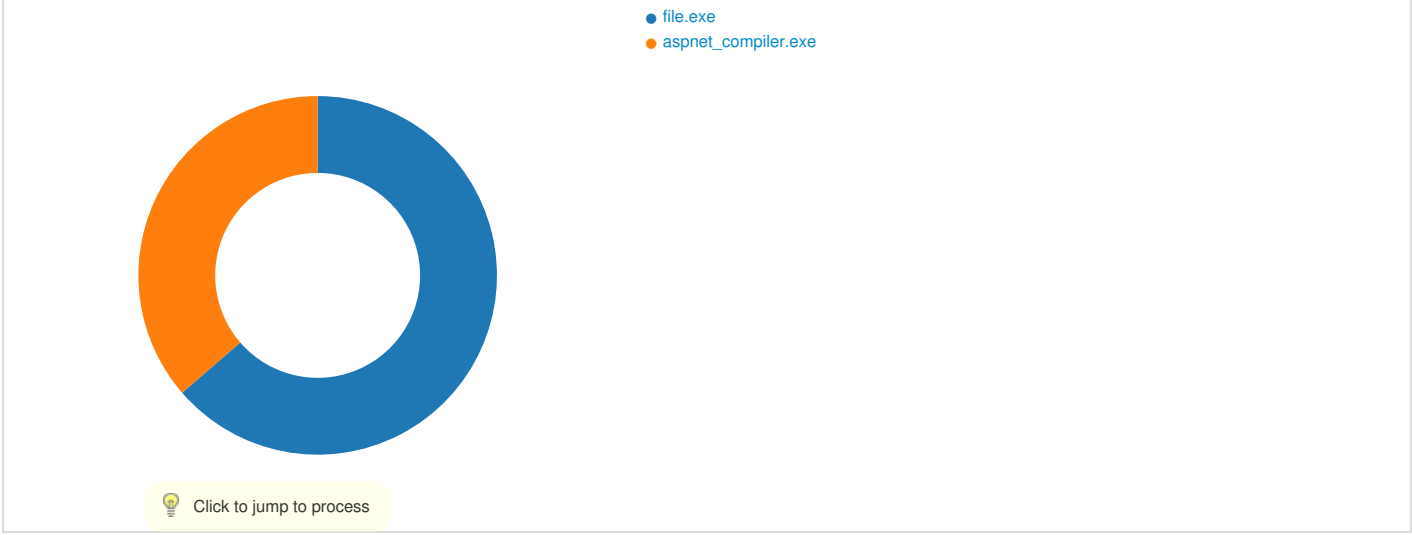
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 17:23:10.011384964 CEST	8.8.8.8	192.168.2.4	0xc728	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:11.872504950 CEST	8.8.8.8	192.168.2.4	0xa0dd	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:13.844806910 CEST	8.8.8.8	192.168.2.4	0x351c	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:15.609191895 CEST	8.8.8.8	192.168.2.4	0x3285	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:19.779814005 CEST	8.8.8.8	192.168.2.4	0x8664	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:21.747344971 CEST	8.8.8.8	192.168.2.4	0xb42c	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:23.862986088 CEST	8.8.8.8	192.168.2.4	0x9c55	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:25.599648952 CEST	8.8.8.8	192.168.2.4	0xee2a	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:29.394942999 CEST	8.8.8.8	192.168.2.4	0x6115	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:31.218715906 CEST	8.8.8.8	192.168.2.4	0x7b8a	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:32.805476904 CEST	8.8.8.8	192.168.2.4	0x26d9	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:34.549218893 CEST	8.8.8.8	192.168.2.4	0xb5bb	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:36.123658895 CEST	8.8.8.8	192.168.2.4	0x3bab	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:37.670564890 CEST	8.8.8.8	192.168.2.4	0x7d9b	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:39.644150972 CEST	8.8.8.8	192.168.2.4	0x636f	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:41.752347946 CEST	8.8.8.8	192.168.2.4	0x4052	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 17:23:43.385559082 CEST	8.8.8.8	192.168.2.4	0x7272	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:45.069904089 CEST	8.8.8.8	192.168.2.4	0x2741	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:46.563900948 CEST	8.8.8.8	192.168.2.4	0xb4a1	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:48.329842091 CEST	8.8.8.8	192.168.2.4	0xad87	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:49.874944925 CEST	8.8.8.8	192.168.2.4	0x70fc	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:53.485065937 CEST	8.8.8.8	192.168.2.4	0xc5a1	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:55.528429985 CEST	8.8.8.8	192.168.2.4	0xe4f4	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:57.421524048 CEST	8.8.8.8	192.168.2.4	0xcb52	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:23:59.431236982 CEST	8.8.8.8	192.168.2.4	0x8c91	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:01.141323090 CEST	8.8.8.8	192.168.2.4	0x1d7b	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:02.915380001 CEST	8.8.8.8	192.168.2.4	0xcf14	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:04.649470091 CEST	8.8.8.8	192.168.2.4	0x1f5e	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:08.438074112 CEST	8.8.8.8	192.168.2.4	0x361c	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:10.369967937 CEST	8.8.8.8	192.168.2.4	0x5ef9	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:12.213613033 CEST	8.8.8.8	192.168.2.4	0xc983	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:14.108341932 CEST	8.8.8.8	192.168.2.4	0x950d	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:16.442303896 CEST	8.8.8.8	192.168.2.4	0x52b5	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:18.340361118 CEST	8.8.8.8	192.168.2.4	0xed56	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:20.526863098 CEST	8.8.8.8	192.168.2.4	0x204e	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:22.098330021 CEST	8.8.8.8	192.168.2.4	0x2055	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:23.549674034 CEST	8.8.8.8	192.168.2.4	0x7c82	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:25.314686060 CEST	8.8.8.8	192.168.2.4	0x16bf	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:29.134788036 CEST	8.8.8.8	192.168.2.4	0xcae8	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:30.799817085 CEST	8.8.8.8	192.168.2.4	0x414f	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:32.472512960 CEST	8.8.8.8	192.168.2.4	0x1cc5	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 17:24:34.303818941 CEST	8.8.8.8	192.168.2.4	0x1385	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:36.231791019 CEST	8.8.8.8	192.168.2.4	0x5c3c	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:38.069847107 CEST	8.8.8.8	192.168.2.4	0x625a	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:39.715939045 CEST	8.8.8.8	192.168.2.4	0x6d9b	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:41.397990942 CEST	8.8.8.8	192.168.2.4	0x947b	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:43.029664993 CEST	8.8.8.8	192.168.2.4	0x7d50	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:44.672501087 CEST	8.8.8.8	192.168.2.4	0xdd7	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:46.522917032 CEST	8.8.8.8	192.168.2.4	0xeec7	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:48.292912006 CEST	8.8.8.8	192.168.2.4	0x5b	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:50.273751974 CEST	8.8.8.8	192.168.2.4	0x460a	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:52.245238066 CEST	8.8.8.8	192.168.2.4	0xf2aa	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:54.279695988 CEST	8.8.8.8	192.168.2.4	0xccbd	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:55.990896940 CEST	8.8.8.8	192.168.2.4	0xed15	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:57.783139944 CEST	8.8.8.8	192.168.2.4	0x81b3	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:24:59.601772070 CEST	8.8.8.8	192.168.2.4	0xfba9	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:01.621582031 CEST	8.8.8.8	192.168.2.4	0x85f4	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:03.311701059 CEST	8.8.8.8	192.168.2.4	0x7a4d	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:04.906692028 CEST	8.8.8.8	192.168.2.4	0xe585	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:06.607954979 CEST	8.8.8.8	192.168.2.4	0x8514	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:08.266287088 CEST	8.8.8.8	192.168.2.4	0x57d7	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:25:10.273897886 CEST	8.8.8.8	192.168.2.4	0xb90f	No error (0)	pekonomia.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 6804, Parent PID: 3528

General

Target ID:	1
Start time:	17:23:04
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x18ff8920000
File size:	500224 bytes
MD5 hash:	66108176E22E6F9513A62C76F2185468
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.550296982.0000018F9283E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.550296982.0000018F9283E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000001.00000002.550296982.0000018F9283E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.550296982.0000018F91E43000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.550296982.0000018F91E43000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000001.00000002.550296982.0000018F91E43000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: aspnet_compiler.exe PID: 6588, Parent PID: 6804

General

Target ID:	2
Start time:	17:23:06
Start date:	06/06/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0xec0000
File size:	55400 bytes

MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000002.813061315.00000000013F7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000002.00000002.812919702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000002.812919702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM, Description: Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003), Source: 00000002.00000002.812919702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000002.00000002.812919702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000002.00000002.812919702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Rmc-B0VP4N\	success or wait	1	412A6C	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Rmc-B0VP4N	exepath	binary	C5 5F 2B 55 33 A4 98 37 6E 69 93 D0 FA C8 DF 1D 85 5A D2 A3 F4 69 F6 E6 9F 19 FD F0 A7 EC 01 F5 46 63 8F BB B9 69 85 00 DF F9 DF 1C 35 87 19 0C 66 74 E5 C1 40 C8 B2 56 52 3A 39 AF 6E 7B A2 4B C2 F9 6C 0B 27 18 35 EF DA 6D 77 A7 1C D9 6A C4 7E 5E C3 0D 05 AF AE 03 2A 5D 9D 85 53 DA 1C 55 9B 15 A7 B6 55 99 F2 C6 6A EF 6C 66 0F F0 CB 98 42 F9 5B 20 60 89 F5 83 86 03 C5 66 7C 2A FB E5 39 FA 4B 6E	success or wait	1	412A94	RegSetValueExA
HKEY_CURRENT_USER\Software\Rmc-B0VP4N	licence	unicode	49255DCB2A8EDE90D2BF0B84970D8636	success or wait	1	412A94	RegSetValueExA
HKEY_CURRENT_USER\Software\Rmc-B0VP4N	time	dword	1686069412	success or wait	1	412B8E	RegSetValueExA

Disassembly

No disassembly